No. 164 Julio - Septiembre 2022 DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

La cadena de suministro digital

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

ISACA®
Bogotá Chapter

CISM Certified Information Security Manager®
An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT®
An ISACA® Certification

CET Certified in Emerging Technology
An ISACA® Certification

CSX CYBERSECURITY
FUNDAMENTALS CERTIFICATE

COBIT® 2019

Mayor Información
www.isaca.org/credentialing

Los miembros de ISACA pueden beneficiarse del acceso, ahorros y conocimiento para impulsar su éxito en auditoría, control, seguridad, ciberseguridad y gobernanza de SI / TI en una multitud de industrias. Member Advantage abarca el conjunto de beneficios que los miembros de ISACA reciben para avanzar profesionalmente y ser recompensados personalmente a lo largo de toda su carrera.

¡Sé parte de **ISACA Bogotá**!

www.isacabogota.org | Teléfono 3007498689

ISACA® Bogotá Chapter

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Julio - Septiembre 2022
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

XXXVI MARATÓN NACIONAL DE PROGRAMACIÓN POR ACIS/REDIS

Resultados:

- phiUN - UNal Bog
- Fast and Fourier - EAFIT
- Newtons Flaming Laser Sword - Uniandes

Los primeros 40 equipos representarán a Colombia en la **Maratón Latinoamericana 2022** por un cupo a mundial.

Más información en:
www.acis.org.co/maraton/

REDIS
RED COLOMBIANA DE PROGRAMAS DE INGENIERIA DE SISTEMAS Y AFINES

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

2022
acm
icpc International Collegiate Programming Contest

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 inesperados. 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 sabiendo 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 convocados 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 conceptuales 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–.*

El XIII Encuentro Nacional de Programas de Ingeniería de Sistemas y Afines

El Encuentro Nacional de programas de Ingeniería de Sistemas y Afines - REDIS, se desarrollará en el corazón verde de Colombia, en el departamento del Quindío.

Su tema central será:

"Oportunidades, retos y desafíos de la formación de ingenieros de sistemas y programas afines".

Fecha: Se realizará del 2 al 5 de noviembre del 2022

Lugar: Hotel Campestre Café Café, Armenia - Quindio

Para más Información:
- 3015530540
- 3043463413

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

REDIS
RED COLOMBIANA DE PROGRAMAS DE INGENIERÍA DE SISTEMAS Y AFINES

Protección de la cadena de suministro

DOI: 10.29236/sistemas.n164a2

A medida que las cadenas de suministros lineales tradicionales son más flexibles, digitales y conectadas, el número de enlaces externos que una organización tiene con otras, como el volumen y las fuentes de datos que fluyen a través de esas conexiones, crecen exponencialmente.
Así también lo hace el número de riesgos potenciales y vulnerabilidades.

Juan Mario Posada D.

En este mundo digital estamos tan seguros como el más débil de los eslabones en la cadena de suministros (Olson, 2020). Esto ha hecho que la protección de la cadena de suministro se convierta en uno de las preocupaciones con mayor crecimiento en los negocios modernos.

La pandemia impulsó las tendencias de aumento en la interoperabilidad, interconexión, eliminación de fronteras, aumento de volúmenes

de los datos y fuentes de información. Además, las organizaciones están redoblando la apuesta por la digitalización para su agilidad y capacidad de respuesta y estar mejor preparadas para hacer frente a los impactos de la crisis y sus consecuencias.

Para gestionar las crecientes amenazas que son inherentes al entorno de negocios, las organizaciones necesitan integrar los principios de seguridad en toda la red de la cadena de suministro. Esto incluye hacer de la ciberseguridad una prioridad no sólo dentro de la empresa, sino también a través de todas las organizaciones asociadas conectadas. También incluye el desarrollo de soluciones de trazabilidad para mejorar la visibilidad de la red. Estas deben ser consideraciones centrales en el diseño de cualquier cadena de suministro inteligente. Es acá donde toman gran relevancia esos factores que influencian la dinámica del entorno de seguridad digital, identificados por Accenture Cyber Threat Intelligence en su reporte anual (Accenture, 2020):

1. Entorno geopolítico comprometedor.
2. Los ciberdelincuentes se adaptan, apresuran y diversifican.
3. Aumento de motivos para el *ransomware.*
4. La mejora de la higiene del ecosistema está empujando las amenazas hacia arriba en la cadena de suministro.
5. Las vulnerabilidades en la infraestructura de la nube exigen soluciones costosas.

¿Cuál es la solución?

Como en muchos otros desafíos de la transformación digital de los negocios, la solución empieza por pensar en la seguridad desde el diseño como elemento fundamental de los procesos de la cadena de suministro.

Para reforzar la ciberseguridad de las cadenas de suministro, las empresas deben construir herramientas de soluciones de seguridad para cubrir las posibles vulnerabilidades. Para la mayoría, esto debería incluir una combinación de gestión de activos; supervisión de la seguridad; revisión y gestión de contratos legales; evaluación de la postura de seguridad del vendedor/proveedor; y la autenticación para el acceso al sistema.

Las empresas deben avanzar hoy hacia una base de datos central que recoja y compruebe la data. Hoy blockchain es una gran oportunidad en ese sentido, ya que integra eventos logísticos en la cadena de suministro y, a través de códigos QR únicos en los productos, pueden, por ejemplo, comprobar la autenticidad y obtener el detalle de la ruta del producto.

Las organizaciones deben buscar ahora ampliar sus estrategias y procesos de seguridad. Para esto, deben trabajar en conjunto con sus

proveedores para aumentar la visibilidad, comprender las amenazas y su potencial aplicabilidad e impacto en su organización. De esa forma se podrá avanzar hacia una estrategia que mitigue los riesgos. Para esto, National Institute of Standars and Technology (NIST) (s.f.) sugiere contemplar algunos principios guía:

- Desarrollar las iniciativas bajo el supuesto de que los sistemas serán vulnerados que permite responder no sólo a la pregunta de cómo prevenir sino también cómo recuperarse.
- La ciberseguridad nunca es un problema exclusivo de tecnología pues contempla a las personas, los procesos y el conocimiento empresarial. Cada vez son menos las infracciones originadas en fallas tecnológicas y más las derivadas de errores humanos.
- Seguridad es Seguridad, los adversarios aprovechan las brechas de la seguridad física para lanzar los ciberataques y viceversa.

Referencias

Accenture. (2020). Securing the supply chain. https://www.accenture.com/cr-en/insights/consulting/securing-the-supply-chain

National Institute of Standards and Technology (NIST). (s.f.). Best Practices in Cyber Supply Chain Risk Management. Supply Chain Best Practices (p. 3). National Institute of Standards and Technology (NIST).

Olson, E. (2020). Why you need to urgently rethink supply chain security. Accenture Business Functions Blog. https://www.accenture.com/us-en/blogs/business-functions-blog/why-you-need-to-urgently-rethink-supply-chain-security

Thomas, A. R. (2010). Supply Chain Security, International Practices and Innovations in Moving Goods Safely and Efficiently. Praeger.

Juan Mario Posada Daza: *Líder de los servicios de ciberseguridad en Accenture Colombia. Con más de 15 años de experiencia en áreas relacionadas con Ciberseguridad, Auditoría de TI y Gestión de Riesgos en empresas del sector financiero, energía, consumo masivo y telecomunicaciones. Ha trabajado anteriormente en firmas de consultoría como Deloitte e EY, donde estructuró y fortaleció las prácticas de servicios de consultoría en Ciberseguridad, seguridad de la información y privacidad.*

ACIS TIC 2022

Analítica + Negocio + Resiliencia = Éxito organizacional

Jornada académica, con invitados destacados representantes de la academia, la industria y el gobierno quienes compartirán sus conocimientos y experiencias en el uso de la analítica para solucionar los cambiantes retos organizacionales.

28 de noviembre al 2 de diciembre

Modalidad Virtual

Más Información en:

www.acis.org.co

ACIS

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Riesgos y retos

DOI: 10.29236/sistemas.n164a3

En Colombia es necesario impulsar una cultura de ciberseguridad.

Sara Gallardo M.

La experiencia como oficial de seguridad de la información en Servientrega, empresa especializada en el transporte, entrega y logística física o digital, proporciona a Carlos Enrique Bermúdez Suárez las herramientas necesarias para pronunciarse sobre todos los aspectos que contempla la cadena de suministro.

En esa compañía, el ingeniero de sistemas, especialista en seguridad de la información y magíster en ciberseguridad y ciberdefensa, lidera la estrategia de ciberseguridad empresarial, después de haber sido consultor de seguridad de la información en otras firmas muy importantes del sector.

En medio de sus responsabilidades laborales, reserva tiempo para practicar el tiro con arco y sumergirse en lecturas de temas distintos a la tecnología, como las relacionadas con la mente de los seres humanos.

"El reto actual más importante es estructurar el país hacia una cultura de ciberseguridad que involucre todos los sectores, aquellos que potencialmente pueden ser estructuras críticas, al ciudadano, a la empresa privada y a las fuerzas militares en un esquema de cooperación y colaboración", sostiene con firmeza.

Revista Sistemas: ¿Qué podemos entender por una cadena de suministro digital? ¿En qué cambia con la cadena de suministro tradicional?

Carlos Enrique Bermúdez Suárez: Entender el contexto digital es de por sí bastante complejo. Cuan-

do lo alineamos a la cadena de suministro y a su constante evolución, podemos definirla como un grupo de procesos interconectados cuya vía de productividad, rendimiento, eficiencia y eficacia es la web, en donde el elemento principal es tener una visibilidad logística inteligente de todas las actividades que forman parte de la cadena de suministro, apoyada en tecnologías como el machine learning e inteligencia artificial para recolectar y procesar información acerca del comportamiento de las actividades en tiempo real, con el propósito de anticiparse a las situaciones que comprometan la operación de la cadena de suministro.

En relación con la cadena de suministro tradicional, el cambio se cen-

tra en la forma como cada empresa enfoca sus sistemas de producción frente al ciclo logístico, enfocados hoy en tecnologías inteligentes, interconectadas y digitales, enmarcados en procesos y cadenas de valor.

***RS:** ¿Cómo se reconocen o entienden los riesgos cibernéticos en la cadena de suministro ahora en un contexto digital?*

CEBS: Durante el día a día de operación de una cadena de suministro, cada segundo sucede eventos que pueden desencadenar en un ciberataque, lo cual demanda un monitoreo constante de los comportamientos. El riesgo cibernético dentro de la cadena se puede visualizar como una serie de eventos que pueden ir mutando en comportamientos de ataques materializados que dejan a la cadena en un tipo de operación bastante volátil en un contexto digital, dado que al involucrar nuevas tecnologías el dinamismo de las funciones cambia al igual que el riesgo cibernético al que está expuesta.

***RS:** ¿Cómo afecta el tema digital la cadena logística de Servientrega?*

CEBS: Bajo la filosofía de "Mundo de Soluciones" evolucionamos para hacer entregas en otras dimensiones, nos lleva a romper paradigmas y a evolucionar para satisfacer las necesidades actuales de mercado. Esto significa adoptar nuevas tecnologías dentro de la cadena logística, cuya afectación principal en el contexto Servientrega, es que introduce nuevos riesgos cibernéticos de forma más rápida y continua, difíciles de identificar para anticiparse en el corto tiempo. Al materializarse puede generar un impacto frente a la marca y las operaciones. Así que estos nuevos contextos digitales dentro de la cadena logística demandan ser identificados y contextualizados en el impacto que su materialización pueda traer a la cadena logística, de manera de anticiparse a su potencial impacto positivo o negativo, además de definir los esfuerzos para que las soluciones que ofrece Servientrega al mercado tengan un componente de seguridad que brinde a los clientes la confianza en el uso de las mismas.

***RS:** ¿Cómo entienden el riesgo cibernético en la dinámica de las operaciones de Servientrega?*

CEBS: En el contexto estratégico la gestión del riesgo es uno de los pilares fundamentales de nuestra compañía; dicha gestión se encuentra definida en la acrópolis empresarial interna.

Teniendo en cuenta que las operaciones logísticas y de transporte en Servientrega son operaciones volátiles y complejas, que involucran factores técnicos y tecnológicos, sumados a los requisitos pactados con los clientes que se convierten en los modelos de operación logística, la gestión del riesgo cibernético se entiende como un habilitador de operación, para poder anticiparnos a una interrupción causada

por un ciberataque, cumpliendo la oferta de servicios y nuestra filosofía actual de entregar en otras dimensiones.

***RS:** ¿El gremio logístico y de transporte en Colombia es consciente de los impactos del riesgo cibernético en el desarrollo de sus operaciones?*
CEBS: A raíz de los ciberataques diarios sobre grandes empresas a nivel mundial, se ha generado cierta preocupación e interés en los temas de ciberseguridad en las empresas del sector en Colombia; sin embargo, los avances en esta gestión han sido mínimos.

En los últimos dos años me he dedicado a revisar informes, investigaciones, reportes de gestión oficiales de entidades públicas en Colombia relacionadas con el sector logístico y de transporte y es muy escaso lo que se identifica en términos de ciberseguridad. Eso sumado a que en la normatividad del sector transporte en el país, tampoco se identifican avances.

Dicho esto, es necesario que los principales entes reguladores, así como las agremiaciones o asociaciones públicas y privadas unan esfuerzos para lograr que se realicen trabajos significativos en procura de construir un entorno normativo y operativo focalizado en el ciclo logístico, orientado a hacerle frente a los ciberataques, mediante la adopción de modelos o estrategias de ciberseguridad, así como la preparación y desarrollo de competencias del capital humano que gira en torno a este sector.

***RS:** Como responsable de ciberseguridad, ¿usted ha sabido o conoce de eventos cibernéticos que hayan afectado las operaciones en el gremio logístico y de transporte en Colombia?*
CEBS: Según el informe de la Comisión Económica para América latina y el Caribe (CEPAL), denominado “Estado de la ciberseguridad en la logística de América Latina y el Caribe”, se identificaron aproximadamente seis ciberataques relacionados con *ransomware* y *malware* como los tipos de ataques de mayor frecuencia en este sector colombiano. Es posible que este número sea mayor, considerando que a través de herramientas de monitoreo, las empresas detectan miles de elementos o comportamientos sospechosos, provenientes de diferentes partes del mundo, que pueden desencadenar un ciberataque lo que hace pensar que van en aumento y que este sector se está convirtiendo en algo atractivo para los ciberdelincuentes.

***RS:** ¿El sector logístico y de transporte en Colombia está preparado para atender y recuperarse ante un ataque cibernético? ¿Cuenta con prácticas de seguridad y control aplicadas y aseguradas?*
CEBS: Considero que el país va en camino hacia esa preparación, porque ya se reconoce como un sector que puede ser vulnerado, que los

ciberataques son una realidad que nos puede sorprender en cualquier momento.

No obstante, recuperarse de un ciberataque es todavía un proceso lento y hasta desorganizado, dado que no se cuenta con la preparación suficiente ni con los elementos ni la sensibilización alrededor de este tipo de escenarios.

Tampoco se identifican fuertes espacios de simulación para adoptar una posición resiliente cuando se presenta un ataque cibernético.

RS: *¿Cómo se puede avanzar en la resiliencia digital del sector logístico en Colombia?*

CEBS: Actualmente, estoy en proceso de terminar una investigación cuyo resultado es una propuesta de un modelo de ciberseguridad, en la búsqueda de un camino hacia esa resiliencia cibernética para las empresas del sector logístico y transporte.

Este trabajo maneja un concepto de resiliencia importante con base en dos elementos claves como son los potenciadores y los reductores de resiliencia, que son como las variables de todo el contexto del ciclo logístico, las cuales nos van marcando el estado y el nivel de madurez y cuya meta es mantener los potenciadores en niveles altos y los reductores muy controlados, para que la compañía se vuelva resiliente, cibernéticamente hablando.

Un potenciador de resiliencia se pude entender como un elemento que ayuda a identificar, anticipar, a estar preparado y adquirir competencias para responder frente a un ataque cibernético y en reductor de resiliencia como un elemento que reduce las capacidades, además de marcar un punto de vulnerabilidad y sensibilidad frente a un contexto resiliente.

Para avanzar es importante entender el ciclo logístico, sus actividades y sus habilitadores (tecnológicos o físicos) de operación; esto nos permite establecer un contexto de riesgo cibernético que vaya más allá de los esquemas tradicionales, que sumado a una adecuada gestión de potenciadores y reductores, nos permita avanzar hacia una organización ciberresiliente.

Es importante que siempre existan mediciones periódicas de estos ni-

veles de resiliencia (riesgo cibernético, potenciadores y reductores de resiliencia) dada la adopción de nuevas tecnologías en todo el contexto de las cadenas de suministro digitales.

RS: *¿El sector logístico y de transporte en Colombia cuenta con el talento humano necesario y suficiente para atender el reto del riesgo cibernético?*

CEBS: Cuando hablamos de riesgo cibernético nos enfrentamos a un contexto más allá de la forma tradicional en la que hoy día se realiza la evaluación de riesgo en las organizaciones. Un autor como (Cano, 2017) en su contexto de la ventana de AREM[1], nos lleva a pensar en los riesgos más allá de los riesgos conocidos por la organización, para trascender a aquellos focalizados, latentes y emergentes. Bajo este esquema metodológico requerido para profundizar, considero que el talento humano sigue siendo mínimo para atender este reto con un talento humano competente y de una visión amplia dirigida a trascender los esquemas tradicionales hacia un panorama real de los contextos cibernéticos que demandan la logística y el transporte.

Por otro lado, debe existir un convencimiento pleno de las organizaciones del sector en la gestión de riesgos cibernéticos, como pilar fundamental de sus operaciones diarias, teniendo en cuenta la exposición y el intercambio de información que se realiza a través del ciberespacio.

RS: *¿Puede considerarse el sector logístico y transporte en Colombia, una infraestructura crítica cibernética? ¿Cómo ve el futuro del sector en la gestión del riesgo cibernético?*

CEBS: El sector logístico y de transporte en Colombia ha venido ganando y generando espacios significativos para considerarse una infraestructura critica cibernética.

Primero, la logística es considerada como el sexto dominio de la guerra sumado a la tierra, mar, aire, espacio y ciberespacio, sin considerar que existen otras posibilidades.

Segundo, el marco del Covid 19 exigió a la logística y el transporte ser una línea vital, fuente transportadora de vida. En tal sentido, fue uno de los principales sectores que durante la pandemia movía la economía del país.

Tercero, algunos autores definen el mercado como un escenario multidimensional que los Estados buscan controlar y es por eso que las guerras futuras que se puedan de-

[1] Cano, J. (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. ISACA Journal. 5. https://www.isaca.org/es-es/resources/isaca-journal/issues/2017/volume-5/the-arem-window-a-strategy-to-anticipate-risk-and-threats-to-enterprise-cyber-security

sarrollar en este contexto estarían encaminadas a ejercer el control y la soberanía de un territorio.

Cuarto, el contexto de las guerras híbridas (capacidad militar y cibernética) que puede afectar cualquier sector de un país, demanda la atención en procura de mantener el control de la soberanía.

Con base en el contexto descrito, el sector logístico y de transporte sí debe ser considerado como una infraestructura crítica cibernética, toda vez que las amenazas o ciberataques hoy en día pueden materializarse sobre este sector y desestabilizar e incluso poner en riesgo la propia vida de los habitantes dentro del país.

Sobre el futuro del sector en la gestión del riesgo cibernético considero que se deben realizar investigaciones más profundas y la implementación de herramientas y modelos de análisis y evaluación de riesgo que involucren y tengan una conexión directa del ciclo logístico y de transporte al riesgo cibernético.

Hoy se utilizan esquemas tradicionales que no permiten identificar riesgos cibernéticos latentes y emergentes lo que hace que puedan tener aproximaciones un poco limitadas al contexto real del panorama de las empresas de este sector frente a escenarios y amenazas, como lo es un ciberataque.

Por otro lado, estas investigaciones deben apalancar un contexto ciberresiliente, debido a que el sector logístico y de transporte involucra actividades de todos los días del año, lo que significa que un ataque cibernético que ponga en riesgo estas operaciones sería de gran impacto, situación que existe una gran preparación.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; En la actualidad es asesora y editora en escritura y producción de libros. Es editora de esta revista.*

GEODATOS
2022

SERVICIOS PÚBLICOS Y TRANSFORMACIÓN ENERGÉTICA ALINEADOS CON LAS TIC Y LOS SIG

MODALIDAD PRESENCIAL
21 AL 23 DE NOVIEMBRE

LUGAR:UNIANDINOS
CL. 92 # 16-11, BOGOTÁ,
CUNDINAMARCA

MÁS INFORMACIÓN EN:
WWW.ACIS.ORG.CO

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Cadenas de suministro

Un desafío de las organizaciones modernas.

DOI: 10.29236/sistemas.n164a4

Andrés R. Almanza J.

Jeimy J. Cano M.

Resumen

El presente artículo es un compendio relacionado con informes recientes alrededor de las cadenas de suministro y sus impactos en las organizaciones. El primero y más representativo de ellos es el informe titulado *Cadena de Suministro 4.0*, del Banco Interamericano de Desarrollo. Los otros informes usados en este resumen están relacionados con reportes de empresas como BSI Institute, Accenture, entre otros. En ellos se revelan los retos que asumen en la actualidad y cómo las organizaciones se deben ajustar para superar los desafíos encaminados a mantener, proteger y desarrollar sus negocios con terceros en el marco de la confianza.

Palabras clave

Cadena de suministro, resiliencia, robustez, proveedores, ciberseguridad

Introducción

Las tecnologías de la información han producido cambios no solo acelerados, sino profundos en la forma en cómo las organizaciones hacen negocios y se desenvuelven en el entorno actual. De la misma manera, la pandemia del COVID-19 también ha mostrado efectos relevantes sobre cómo las organizaciones producen, transportan, exportan, importan y comercializan todo lo que hacen; en otras palabras, ha cambiado de manera drástica la forma de operación de las empresas.

En este contexto, la cadena de suministro se ha revelado como una pieza fundamental del proceso de desarrollo de las organizaciones, haciendo evidente su sensibilidad y necesidad de todos los tipos, tamaños, sectores, industrias y/o verticales, como parte articuladora de la promesa de valor de las compañías y soporte fundamental para contar con sus productos y servicios.

La transformación digital es un proceso que viven las empresas de hoy el cual implica, no sólo tener capacidades tecnológicas, sino financieras, humanas y conceptuales (BID, 2019) para que puedan adaptarse a las nuevas economías de los datos, de la inteligencia artificial y de las exposiciones significativas a la disrupción y los riesgos.

En consecuencia, serán estas empresas las que, procurando una adaptación sistémica a la disrupción, se encuentren mejor preparadas para avanzar en medio del ecosistema digital empresarial disponible a la fecha.

Por tanto, este documento pretende visualizar, los retos y mejores prácticas que pueden experimentar las organizaciones en relación con las cadenas de suministro y cómo dichos retos y oportunidades pueden ser abordados.

Cadenas de suministro, un desafío de las organizaciones

Hoy por hoy, las cadenas de suministro son una pieza angular de todo negocio. A medida que pasa el tiempo, el aumento y la evolución del contexto de los ecosistemas empresariales incrementa su complejidad y su gestión, lo cual acrecienta el espacio para la disrupción como uno de los riesgos claves para las organizaciones actuales.

Las tecnologías modernas que surgen en el marco de la llamada Cuarta Revolución Industrial, forman parte del entramado de complejidad en las organizaciones y en todos los actores de un ecosistema empresarial que hace a las cadenas de suministro parte esencial.

Esta articulación no sólo crea capacidades con mayor agilidad y menor costo, sino escenarios de riesgo pocos conocidos.

Como parte de las tendencias indispensables en las cadenas de su-

ministro, la firma Gartner ha publicado cinco tendencias que reflejan la forma sobre cómo en el futuro, las cadenas de suministro necesitarán elementos estratégicos para mantener sus operaciones (ver figura 1) (Gartner, 2022).

Señala Gartner que los ecosistemas organizacionales son la pieza clave de la competitividad, puesto que es posible aprovechar la capacidad de todas las partes involucradas. Entre más cooperación, más integración y mayor trabajo conjunto, se acrecentará el potencial de competitividad en entornos digitales cada vez más complejos.

El segundo factor está relacionado con un trabajo de estos ecosistemas por educar a los consumidores en el ejercicio de la sostenibilidad. No sólo es reconocer las necesidades locales, sino los retos internacionales que implica hacer sostenible la organización.

El tercer factor está relacionado con lo modular, con el fin de incrementar la innovación, disminuir tiempos y hacer que las cargas operacionales sean menores y más eficientes. La modularidad enfrenta el reto de la integración y la articulación para concretar sus beneficios.

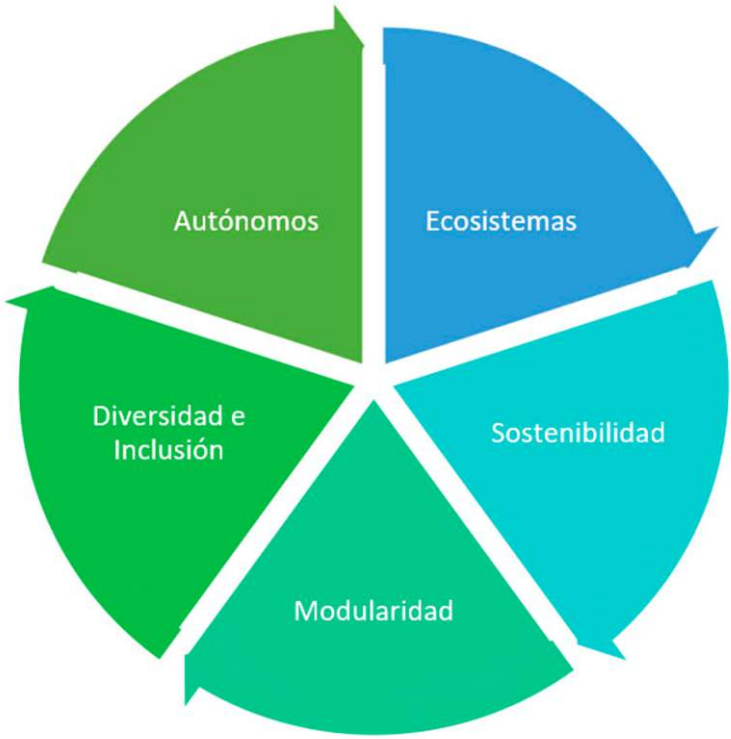


Figura 1. Tendencias de las cadenas de suministro. Elaboración propia

El cuarto elemento la diversidad e inclusión. Mejorar el rendimiento de las cadenas de suministro pasa por la inclusión, diversidad y equidad, y es por ello, que según los datos, es una tendencia de trabajo marcada que mostrará resultados claves en el corto plazo. A mayor diversidad e inclusión, diferentes oportunidades para repensar la dinámica de la cadena en sí misma.

El quinto factor, el uso de la inteligencia artificial y las máquinas de aprendizaje que harán más ágiles los procesos repetitivos y operacionales de las cadenas de suministro para mejorar la toma de decisiones y su expansión, en un escenario cada vez más interconectado y automatizado.

Cadenas de Suministro:
Las cadenas de suministro están definidas como el conjunto de actividades que contemplan desde el diseño, hasta la puesta en marcha de un producto bien o servicio. En las economías modernas las cadenas de suministro hacen parte esencial de la producción y, en consecuencia, son parte fundamental de la dinámica empresarial.

Una cadena de suministro y su desempeño está organizada por proveedores, facilitadores, logística, fabricación y canales de distribu-

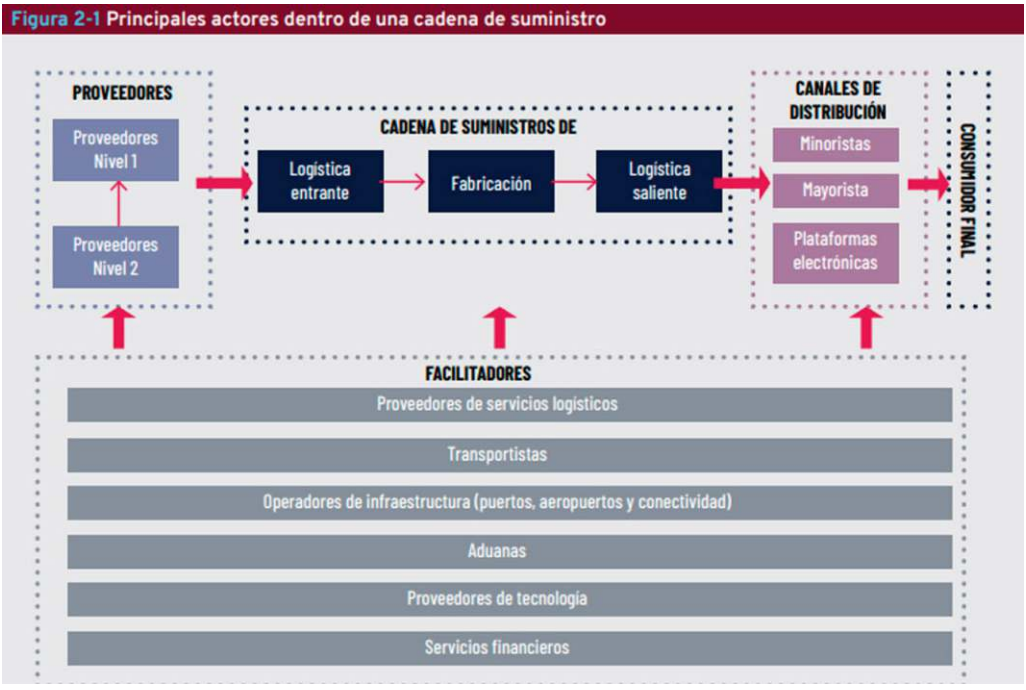


Figura 2. Componentes de una cadena de suministro. Fuente: BID, 2019

ción, la figura 2 ilustra cómo puede estar compuesta una cadena de suministro.

Los principales participantes de una cadena son: (BID, 2019)

Proveedores de primer y segundo nivel: Aquellos que proveen al productor (primer nivel) de los insumos y los de segundo nivel, los que soportan al proveedor de primer nivel.

Empresa creadora (manufacturera): Es la empresa que produce el bien o servicio, que pueden ser de gran tamaño, pertenecientes a múltiples verticales, y que usa los insumos de sus proveedores de primer y segundo nivel para transformarlos y producir un bien o servicio.

Organismos de control: Entes o entidades que pueden intervenir para validar el cumplimiento de las regulaciones respectivas en relación con la importación y exportación de las materias primas en caso de que se requieran.

Proveedores de tecnología: Aquellas empresas que proporcionan energía como apoyo a la organización.

Proveedores de servicios financieros: Toda aquella entidad de este orden que participa de manera directa o indirecta en el proceso de transformación.

Distribuidores (Mayoristas/Minoristas): Empresas que se encargan de la comercialización del producto fabricado.

Proveedores de logística: Todos aquellos que intervienen en el transporte físico de los materiales o productos transformados.

En la medida en se incrementa el nivel de complejidad en la transformación de materias primas en productos terminados, es necesario incrementar la visibilidad, coordinación, cooperación, seguimiento y monitoreo de todas las partes que intervienen en el proceso. En esa misma línea la complejidad se puede ver manifiesta en distritos niveles, descrita en la tabla 1.

Tecnologías y transformación digital:
La tecnología sin lugar a dudas es un factor determinante en las cadenas de suministro, es por esto, que son también esenciales, especialmente por las tecnologías que han acelerado su dinámica como el Internet de las cosas (IoT), el Big Data, la Inteligencia Artificial, el Metaverso, la robótica, por mencionar algunas, que han incrementado la necesidad de contar con cadenas más ágiles y sintonizadas en un contexto digital que cada vez tiene mayor presencia.

Las cadenas de suministros del futuro:
Definitivamente el futuro estará permeado de cadenas de suministro mucho más robustecidas y con mucha presencia de las

Complejidad en:	Descripción
La red	Mayor cantidad de actores participantes
Los procesos	Por una mayor cantidad de ellos para realizar el proceso
En el producto	Por requerir mayores elementos para su elaboración
En la demanda	Por el incremento de la volatilidad, fragmentación y especificidad
Organizacional	Por el mayor número de involucrados y la tendencia a trabajar de manera aislada e independiente

Tabla 1. Niveles de complejidad en las cadenas de suministro.
Basado en Informe del BID, 2019

tecnologías disruptivas actuales y en desarrollo. Para el caso del presente y del futuro, el documento propone definir a las cadenas de suministro, como cadenas 4.0, las cuales se caracterizan por:

1. Alto grado de complejidad por sus niveles de interconexiones entre los contextos físicos y digitales. Dependen en alta medida de sensores del IoT que recolectan datos y mediante el Big Data esta información es analizada para acelerar la toma de decisiones; en la misma línea la inteligencia artificial y la nube se convierten en elementos claves para estas cadenas de suministro complejas y digitales.

2. Una amplia dependencia de la automatización y robotización que facilitarán los procesos y la toma de decisiones, así como concentrar esfuerzos en la toma de decisiones, su cobertura y el trabajo avanzado que las personas puedan hacer en el ecosistema digital.

3. Incrementos de productividad, riesgos y gestión, por una mayor conectividad y complejidad del ambiente de operaciones, que si bien mejora la productividad, también advierte un incremento de los riesgos en un ecosistema cibernético que requerirá de un elevado nivel de gobierno y gestión.

Al mirar el futuro se puede observar que las cadenas de suministro serán más autónomas, más independientes y con mayor capacidad, toda vez que la convergencia digital, la automatización y la misma transformación digital imprimen en las cadenas de suministros estas características que hacen elevar el nivel de digitalización. Se estima que las cadenas de suministro pasen de una autonomía a una forma automática de pensamiento "*self-thinking supply chains*", cadenas que

Figura 3. Cadena de suministro rígida. Elaboración propia

piensan y actúan por sí misma (BID, 2019).

La alta conectividad, la presencia masiva de sensores, la capacidad de gestión de grandes volúmenes de datos, más una capacidad algorítmica inteligente y avanzada hacen de las cadenas de suministro del futuro un elemento esencial de la competitividad de los ecosistemas organizacionales, que requerirán de una robustez organizacional para seguir manteniéndose en el contexto digital (Xie et al. 2022).

Por lo tanto, el monitoreo continuo y la gestión temprana serán elementos claves para poder anticipar posibles anomalías en las cadenas de suministro, así como una optimización constante de las operaciones y procesos de manera inmediata, buscando mejorar el desempeño y creando mayores niveles de flexibilidad frente a las fallas en las operaciones.

En estos modelos se pasa de estándares rígidos y lineales (figura 3), a modelos flexibles y modelos sistémicos (figura 4), flexibles, ágiles y multidireccionales; esto hará que la competencia no sea de un elemento particular de la empresa (producto), sino de toda la cadena (ecosistema) lo que hará la diferencia. Los grandes sectores competirán basados en la agilidad, flexibilidad, capacidad y desempeño de todos sus socios y no solo de ellos mismos.

Adoptar la transformación digital no sólo es una moda, es una necesidad imperante en un ambiente que se mueve más hacia lo digital. La necesidad de ello está centrada en la idea de que, mientras estas cadenas de suministro sean más densas, habrá más fragmentación y por ende mayor posibilidad de fallas en alguno de sus elementos. En consecuencia, la transformación digital requiere un acelerado desarrollo para que todas estas tecnologías empiecen a articular las nuevas cadenas que crecen de manera acelerada.

Es por eso que estas cadenas de suministro 4.0 caracterizadas por adoptar las nuevas tecnologías en todos los actores, procesos e interacciones (proveedores de primer y segundo nivel, procesos, infraestructuras físicas y tecnológicas, logística, comercialización, así como en los entes regulatorios), necesitan incluir procesos de transforma-

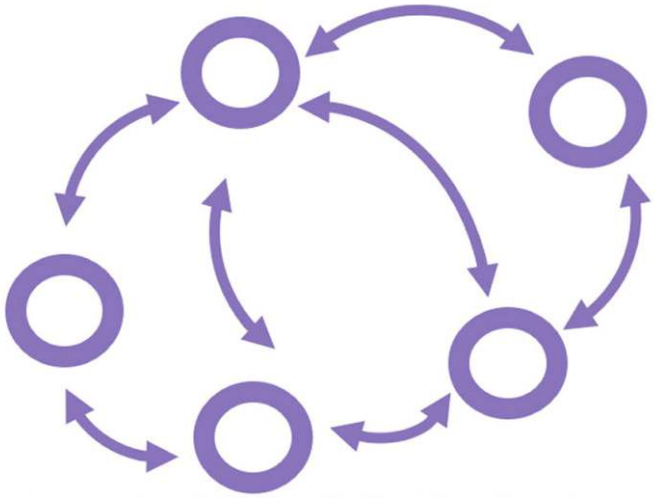


Figura 4. Cadena de suministro flexible. Elaboración propia

ción digital, lo que implica colaboración, cooperación, coordinación entre todas las partes que intervienen para asegurar la interoperabilidad de todos los sistemas involucrados, de tal forma que los beneficios sean visibles en estos nuevos ecosistemas empresariales.

En definitiva, la coordinación es uno de los factores claves para que una cadena de suministro funcione de la mejor forma. Existen fallas de coordinación en los actores privados, fallas de coordinación en la adopción de tecnologías y fallas de coordinación en el sector público, elementos que se convierten en grandes desafíos de las cadenas de suministro.

Incentivos y retos de las cadenas de suministro:
Las buenas prácticas en esta materia son variadas y jalonadas precisamente por la competitividad, no sólo en sí misma, sino en el contexto globalizado de la economía; como ocurre también con las tecnologías disruptivas y las nuevas empresas que continuamente entran a jugar un papel en todo este entramado.

Dentro del conjunto de buenas prácticas y desafíos para tener cadenas de suministro de alto nivel o denominadas 4.0, están: (BID, 2019)

Proveedores de primer nivel: Incentivos que favorecen la buena práctica como la colocación de sistemas y transferencia de tecnología por parte de fabricantes. Barreras: Acceso limitado al capital humano y recursos.

Proveedores de segundo nivel y pymes: Prácticas como descuen-

tos de proveedores tecnológicos y programas de incentivos gubernamentales juegan un papel importante. Entre los desafíos están los enfoques de las tecnologías sólo para proveedores de primer nivel con más capacidad para invertir, con acceso limitado a capital humano y recursos en los niveles gerenciales.

Grandes fabricantes: Enfrentan la presión competitiva, la integración vertical y la internacionalización, las nuevas tecnologías como la nube, la inteligencia artificial y la web 3.0. Como desafíos están la multiplicidad de tecnologías y su compatibilidad, las barreras organizacionales propias y la inmadurez en la adopción de las tecnologías.

Proveedores de servicios logísticos y gestores de infraestructura: La presión del mercado es un gran habilitador y el codesarrollo con fabricantes se convierte en una práctica necesaria. Por su parte la dependencia de otros transportadores (pequeños), la estructura del mercado que puede ser informal, la tecnología y la inmadurez en la adopción de estas se convierten en grandes retos para este actor de la cadena.

Transportistas: La presión como práctica para la adopción y desarrollo de las cadenas, la poca disponibilidad de la tecnología en el sector, el acceso limitado a capital humano y recursos, la poca o baja transparencia del sector y los desafíos en la interoperabilidad de sistemas, son grandes retos.

Conjunto de buenas prácticas para el desarrollo de cadenas de suministro

Están divididas en cuatro grandes frentes:

- Estrategias y planes de orden nacional para apoyar el desarrollo de las cadenas de suministro. Con base en agendas de trabajo y hojas de ruta para la adopción de la transformación digital en las cadenas de suministro, buscando que la digitalización llegue a la pequeña y mediana industria, los planes de logística son otro frente dentro de este conjunto de estrategias de alto nivel. Y, por último, las agendas digitales de las partes interesadas, de tal manera que la adopción de la tecnología esté en la agenda de la transformación de las cadenas de suministro.

- Apoyo a la pequeña y mediana empresa, el despliegue de centros tecnológicos que promocionen la adopción de prácticas digitales en los procesos industriales, el incentivo financiero en empresas que empiecen sus procesos de transformación, y la difusión de conocimiento relacionadas con la expansión de mercados, mejora de procesos son buenas prácticas usadas en apoyo a las empresas.

- Desarrollo de estándares de comunicación interorganizacional; dentro del desarrollo de estándares está el propósito para que los sectores privados y públicos tengan ambientes adecuados y sólidos para poder interoperar entre sí, de manera más ágil, transparente y natural.

- Programas para incentivar la cooperación público–privada; en este sentido la definición de roles, responsabilidades y funciones es pieza clave de la práctica para que todos los actores puedan intercambiar experiencia, tiempo y recursos, de manera de acelerar la forma en que sus cadenas de suministro evolucionan hacia unas cadenas 4.0. Así mismo, el establecimiento de centros o hubs de transformación digital de las cadenas de suministro, el desarrollo de hojas de ruta o guías de transformación digital y la documentación de casos de uso exitosos en el ejercicio, serán elementos indispensables.

América Latina, un camino por recorrer

El mundo y los grandes países industrializados han avanzado bastante en el desarrollo de cadenas de suministro de gran envergadura; aunque América Latina no se queda atrás, tiene frente a las grandes potencias mucho camino por recorrer. Existen para la región dos tipos de crecimiento en la materia, por un lado las empresas de gran tamaño que, junto con sus proveedores de primer y hasta segundo nivel han logrado hacer una evolución significativa acercándose a cadenas de suministro 4.0. Así mismo, las empresas pymes tienen bajos niveles de conocimiento, escaso acceso y uso de la tecnología, además de escasos recursos financieros y de gestión para estar a la par con la demanda actual, sin perjuicio de las asimetrías en los distintos sectores de la industria latinoamericana, frente a las buenas prácticas internacionales.

En esa línea, para la región pueden existir tres grandes factores para determinar el grado de preparación encaminado a afrontar las transformaciones digitales necesarias en las cadenas de suministro en las empresas de la región de las Américas. Los factores están asociados al grado de inserción de las cadenas de suministro en el contexto global, al grado de integración vertical y al nivel de intensidad competitiva del ecosistema.

En la misma línea existen algunas barreras importantes para que las cadenas de suministro de la región de América Latina muestren un atraso. Los entornos económicos de los países, los niveles de incertidumbre política y las condiciones de inversión son barreras estructurales que afectan la zona. De igual forma, los costos laborales, la disponibilidad local limitada de la tecnología, la reducida disponibilidad de servicios de implementación de

nuevas tecnologías, el desconocimiento de los niveles directivos y ejecutivos, la resistencia cultural, el talento humano entrenado, se advierten entre los factores enfrenta la región.

Las capacidades de las pymes en el ámbito de la región de las Américas es otro gran punto para considerar. Por un lado, aunque este sector reconoce la necesidad de innovar como fuente de crecimiento, tiene poco acceso a las tecnologías necesarias para que eso suceda.

No sólo son los actores principales los que poseen grandes retos, también los facilitadores de las cadenas de suministro en la región tienen una tarea por hacer. El acceso de las telecomunicaciones a nivel regional es tal vez el factor más predominante y común en todos, lo que se convierte en un gran reto a trabajar, para que dichas transformaciones en la operación sucedan de una mejor manera. Sin dejar de lado que la falta de coordinación multisectorial es otra pieza importante para considerar en el desarrollo de las cadenas de suministro de las Américas.

La figura 5, resalta las iniciativas del sector público de Latinoamérica con impacto en las cadenas de suministro.

Tabla 5-5. Iniciativas del Sector Público de América Latina con impacto en ciertas áreas de la cadena de suministro

Iniciativas	Argentina	Brasil	Colombia	México	Paraguay
Industria 4.0	• Plan de Innovación Digital 4.0 • Clústeres de Innovación I+D	• Estrategia Nacional de Industria 4.0 • Estrategia Brasileña de Transformación Digital	• Programa de Transformación Productiva	• Industria 4.0 • Prosoft 4.0	• Visión Paraguay 2030
Logística		• Plan Nacional de Logística y Transporte	• Política Nacional Logística	• Plan Nacional de Transporte y Logística 2014-2018	• Plan Nacional Logístico
Transporte	• Plan Belgrano • APPs de Infraestructura		• Plan Maestro de Transporte 2010-2032	• Programa de Inversión en Transporte 2013-18	• Plan Maestro de Transporte
Telecomunicaciones	• Red Federal de Fibra Óptica	• Plan Nacional de Banda Ancha • Plan Nacional IoT	• Vive Digital	• Estrategia Nacional de Digitalización	• Plan Nacional de Telecomunicaciones
Aduanas	• Ventanilla Única de Comercio Exterior • Secretaria de Simplificación Productiva		• Plan Estratégico de Aduanas	• Plan de Modernización Aduanera	• Plan Estratégico de Aduanas

Fuente: Compilación de los autores

Figura 5. Iniciativas del sector público en cadenas de suministro.
Fuente BID, 2019

Riesgos de las cadenas de suministro

Los riesgos están a la orden del día, no hay cadena de suministro en el contexto global que esté exenta de ellos. Uno de cada cuatro manifiesta haber tenido una afectación en las cadenas de suministro, considerando la acelerada transformación digital del sector (ISACA, 2022).

Dentro de los principales riesgos que las cadenas de suministro pueden enfrentar tenemos (BSI, 2021).

Riesgos regulatorios, ambientales, impactos por el COVID-19, laborales, de seguridad física, inequidad y pobreza, geopolítica y crimen organizado, de continuidad de negocio y de ciberseguridad. La figura 6, muestra el panorama. Dada la complejidad de las cadenas de suministro y su creciente dependencia en los ecosistemas organizacionales los riesgos han aumentado, los años de pandemia promovieron tales riesgos y desafíos. (BSI, 2021).

En el contexto digital los riesgos son cada vez más permanentes, más globales y de mayor impacto, frente a otras situaciones. Existe en la actualidad una variedad amplia de reportes que vienen estudiando el fenómeno de los riesgos de ciberseguridad en las cadenas de suministro y muestran una complejidad importante que requiere ser atendida de manera inmediata. El reciente informe titulado *Supply Chain Security GAPS* producido por ISACA 2022, organización global líder para los profesionales del gobierno, el control, la seguridad y la auditoría de las tecnologías de la

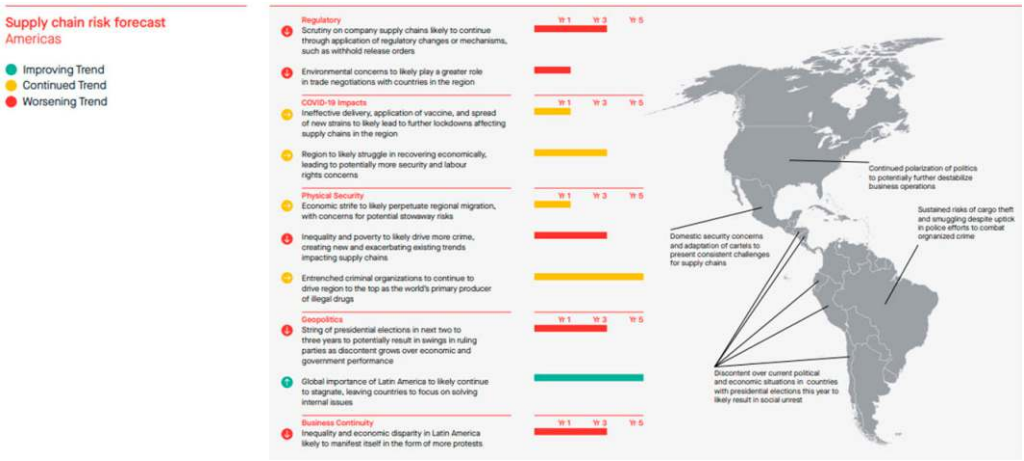


Figura 6. Pronósticos de Riesgos de la Cadena de Suministro.
Fuente BSI, 2021

información, menciona que es el ransomware (73%) lo que más afecta a las cadenas de suministro.

La figura 7, resalta el top de posibles situaciones de riesgos en el contexto digital.

Para enfrentar estos riesgos, Gartner (2021) ha propuesto capacidades que son necesarias para que toda cadena de suministro pueda tener instrumentos que le ayuden a solventar la disrupción. Aquellos que trabajan en la visibilidad, en la resiliencia y la agilidad, podrán tener mayores oportunidades para enfrentar los riesgos que las cadenas de suministro presentan, ver figura 8.

La resiliencia asegura que la cadena de suministro tenga los insumos suficientes y las opciones para responder activamente ante los riesgos. La visibilidad le permite a la cadena de suministro y a todo su ecosistema monitorear los riesgos y dar respuestas tempranas o anticipatorias a los mismo. La agilidad asegura la flexibilidad necesaria para usar todos los insumos y con ello generar respuestas claves y claras frente a los riesgos existentes.

Para ello Gartner (2021), propone adelantar acciones claves para desarrollar estas capacidades, tales como:

1. Conciencia de toda la cadena suministro para considerar la sensibilización en la estrategia de gestión de las cadenas de suministro. Aquellos que la involucran en toda la cadena de suministro, ponderan de la misma manera la calidad del producto, su costo y la velocidad para responder a la demanda; en esa medida no se crean desbalan-

Figura 7. Top de riesgos de seguridad en cadenas de suministro.
Fuente ISACA. 2022

Figura 8. Capacidades de las cadenas de suministro. Elaboración Propia

ces y se reducen posibles riesgos.

2. Reducir la superficie de la cadena de suministro, en este aspecto la simplificación de los procesos, su automatización, la reducción de los movimientos entre los distintos componentes y el diseño de toda la red de interconexiones de la misma cadena, pueden disminuir los riesgos en las cadenas de los ecosistemas organizacionales.

En la misma línea para atender los desafíos y riesgos de las organizaciones y los ecosistemas, existen ejercicios claves que pueden reconfigurar las cadenas de suministro y mejorar su exposición a los riesgos (Sáenz & Revilla 2014), entre las cuales están:

1. Identificar las prioridades estratégicas de toda la cadena de suministro, identificar los elementos claves, desarrollar y mantener un inventario completo (ISACA, 2022).

2. Hacer un mapa de las vulnerabilidades identificadas en toda la cadena de suministro y sus elementos.

3. Integrar a los riesgos de manera sistémica dentro del ciclo de producción del producto y la cadena de suministro. Diseñar las cade-

nas de suministro desde el inicio de manera resiliente en su operación.

4. Monitorear, lo cual implica poder observar a través de herramientas tecnológicas y procesos todo el comportamiento de la cadena de suministro. Confiar, pero revisar (ISACA, 2022) o aplicar el principio de "confianza cero" es relevante para estar en relación con todos los actores como proveedores o terceros que ofrecen algo a la organización.

5. Observar los eventos, incidentes, problemas, involucrando una adecuada gestión, una acertada continuidad de negocio, un manejo resiliente de los eventos y con ello producir ecosistemas organizacionales robustecidos (Xie et al., 2022).

Conclusiones

Las cadenas de suministro son parte esencial de las economías digitales y modernas que existen en las que participan diferentes actores. Las interacciones generadas entre ellos y lo que se produce de los mismos se convierten en elementos esenciales de la productividad de las empresas, organizaciones y naciones (BID, 2019).

Las tecnologías de información y las comunicaciones forman parte esencial del proceso de las cadenas de suministro y su adopción acelera el desarrollo, no sólo de las empresas, sino de todos los que en ella intervienen. Sin embargo, tener adopciones limitadas de la tecnología en la cadena de suministro puede afectar significativamente la competitividad de las empresas y específicamente de una región como la latinoamericana.

Como lo menciona el informe del Banco Interamericano de Desarrollo (BID, 2019), es necesario que las agendas de los países latinoamericanos den prioridad al desarrollo y fortalecimiento de las cadenas de suministro. Por tanto, el informe resalta cinco ejes de acción que deben ser considerados para fortalecer dichas cadenas y dar un impulso a las economías en ascenso.

1. Implementar las mejores prácticas de los líderes, los países con mayor avance han aprendido y creado experiencia que puede ser de utilidad para el mejoramiento en América Latina. Abordaje integral o manejo sistémico al desarrollo de las cadenas de suministro, tener hojas de ruta y planes de trabajo bien definidos, así como una postura de cautela y observación a los cambios del entorno y contexto global, son claves para el desarrollo de cadenas de suministro enriquecidas y sólidas.

2. Visión regional: es necesario que la región de américa latina enfrente sus propios retos basados en los trabajos de cooperación, la asimetría de capacida-

des con otras regiones y países hace necesario un enfoque de tales dimensiones que ayude a apalancar los desafíos propios de la agenda latinoamericana. Tecnología y costos laborales, así como conocimiento y talento; y, por último, las relaciones del sector público y privado, son los frentes que como región se deben enfrentar para superar estos retos.

3. Apoyo de las pymes, en la región las empresas medianas y pequeñas, representan una gran proporción del empresariado, por tanto, fortalecerlas es el camino más adecuado, de cara al robustecimiento de las cadenas de suministro que soportan las economías emergentes, desde centros de gestión tecnológica hasta políticas públicas para minimizar los costos de producción pueden ser elementos que ayuden en esta materia.

4. Digitalizar a los actores secundarios: no son sólo los proveedores de primer o segundo nivel a quienes debe llegar la tecnología, la idea es que debe llegar a todos los elementos que intervienen en una cadena de suministro que dé lugar a instancias encaminadas a articular la llegada de todas estas tendencias a los actores claves dentro de un ecosistema complejo.

5. Política pública. Los Estados necesitan de estándares y política pública para apoyar a las cadenas de suministro, especialmente en regiones como la latinoamericana, que permitan fomentar el desarrollo de cadenas de suministro 4.0.

El futuro de los ecosistemas organizacionales no solo pasa por las cadenas de suministro, sino por la robustez de estas. Los riesgos, y en mayor medida los digitales, son una fuente clara de inestabilidad y disrupción que estarán presentes y deben ser atendidos. Fenómenos globales como el COVID-19 o el conflicto entre Rusia y Ucrania hacen que las cadenas de suministro estén cada vez más expuestas a eventos inciertos, no sólo a nivel de un ecosistema aislado, sino de todo un país, una región o incluso el mundo (BSI, 2021).

Estrategias que permitan a las organizaciones mantener una exposición controlada a los riesgos cibernéticos son pieza fundamental del trabajo de gestionar los riesgos a los que las cadenas de suministro son expuestas (CEPAL, 2021).

Pero no son los únicos riesgos que deben visualizarse, los riesgos deben ser vistos de manera sistémica (BSI, 2021), permitiendo así crear ecosistemas robustecidos (Xie et Al., 2022) capaces de superar la continuidad de los eventos adversos, cada vez más frecuentes y que afectarán el flujo normal de operación de las empresas, organizaciones y naciones.

La gestión de riesgos de la cadena de suministro no debe verse como una isla independiente de la operación de la organización; por el contrario, en el futuro no muy lejano debe ser una gestión integral de riesgo, en la que esos elementos que no eran considerados parte del sistema lo sean y sean visualizados como un todo, pasando de una práctica estática y llena de relatividad, a una práctica más dinámica basada en red y ambientes sistémicos (Sáenz & Revilla, 2014).

Visibilidad, agilidad, flexibilidad, visión holística, resiliencia, responsabilidad y debida diligencia son elementos claves a la hora de gestionar las cadenas de suministro (Accenture, 2020). El continuo desarrollo de estas capacidades hará de las cadenas de suministro un factor clave, que requiere de esfuerzos, personas, procesos, regulaciones y tecnología que, de hacerse de la manera correcta, creará ambientes altamente competitivos y claves para el desarrollo de las empresas y las naciones (Alicke et al. 2021).

Referencias

Accenture (2020). *Securing the supply chain. Understanding and mitigating the security risks of modern enterprise supply networks.* https://www.accenture.com/_acnmedia/PDF-134/Accenture-Securing-The-Supply-Chain.pdf

Alicke. K., Barriball. E. & Trautwein. V. (2022). *Cómo la COVID-19 está remodelando las cadenas de suministro*. https://www.mckinsey.com/featured-insights/destacados/como-la-covid-19-esta-remodelando-las-cadenas-de-suministro/es

BID (2019). *Cadena de suministro 4.0*. https://publications.iadb.org/publications/spanish/document/Cadena_de_suministro_4.0_Mejores_pr%C3%A1cticas_internacionales_y_hoja_de_ruta_para_Am%C3%A9rica_Latina_es.pdf

BSI (2021). *BSI Supply Chain Risk Insights Report 2021*. https://www.bsigroup.com/globalassets/localfiles/en-gb/supply-chain-solutions/resources/bsi-supply-chain-risk-insights-report-2021.pdf

CEPAL (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

Gartner (2021). *Adopt a New Supply Chain Strategy to Minimize Risk Impacts*. https://www.gartner.com/en/supply-chain/insights/supply-chain-risk-management

Gartner (2022). *The Rise of the Ecosystem — and 4 More Supply Chain Predictions*. https://www.gartner.com/en/articles/the-rise-of-the-ecosystem-and-4-more-supply-chain-predictions

ISACA (2022). *Supply Chain Security Gaps: A 2022 Global Research Report*. https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/reports/supply-chain-security-gaps-a-2022-global-research-report_202205.pdf

Sáenz. M. & Revilla. E. (2014). Creating More Resilient Supply Chains. *Sloan Management Review*. https://sloanreview.mit.edu/article/creating-more-resilient-supply-chains/

Xie, Y., Desouza, K. C., & Jabbari, M. (2022). On organizational robustness: A conceptual framework. *Journal of Contingencies and Crisis Management, 1–16*. https://doi.org/10.1111/1468-5973.12423

Andres R. Almanza J., Ms.C, CISM. *Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo, Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador y miembro del comité editorial de la revista sistemas de ACIS. Executive Certificate en Cybersecurity Leadership & Strategy en FIU University, Profesional en Ingeniería de Sistemas y especialista en seguridad en redes y máster en seguridad de la información, Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager de PECB, CISM, ITILv3, LPIC1, Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation. Ha creado espacios de aprendizaje como la Comunidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin).*

Jeimy J. Cano M., PhD, CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D en Business Administration de Newport University, CA. USA. y Ph.D en Educación de la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) en 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–.*

Cadena de suministro

DOI: 10.29236/sistemas.n164a5

¿Ahora digital?

Los aspectos más relevantes fueron analizados en la mesa de debate.

Sara Gallardo M.

Diferentes aspectos fueron tratados en torno a la cadena de suministro y su alcance digital en la reunión moderada por Jeimy J. Cano Martínez, director de esta revista.

A la cita acudieron Liliana Patricia Quiñonez García, secretaria general de la Federación Colombiana de Agentes Logísticos en Comercio Internacional, FITAC; Juan Mario Posada Daza, líder de Ciberseguridad de Accenture, Colombia y Emilio Alberto Oropeza Zurita, Security Engineer Manager.

Jeimy J. Cano M.
¿Qué podemos entender por una cadena de suministro digital? ¿En qué cambia con la cadena de suministro tradicional?

Liliana P. Quiñonez García
Secretaria General
Federación Colombiana de Agentes Logísticos en Comercio Internacional, FITAC
Con la declaratoria de la emergencia sanitaria y "pandemia" el sector logístico se vio obligado a implementar sí o sí la cadena de suministro o plataformas digitales para que la prestación del servicio, propia de la actividad de comercio exterior, estuviese armonizada con los sistemas informáticos de las diferentes entidades de vigilancia, inspección y control. Integrando así

a todos los actores de la cadena tales como importador, fabricante, operador logístico, exportador, transportador en el exterior y nacional.

Emilio Alberto Oropeza Zurita
Security Engineer Manager
A partir de la pandemia todo el tema logístico empezó a incrementar y hay que entender dos puntos, la parte de e-commerce y la de cadena de suministro. Lo importante del canal de suministro digital es emplear nuevas tecnologías, impulso que se ha dado desde hace varios años y que empieza a crear distintos riesgos. La cadena de suministro digital contempla el proceso completo desde que estamos en bodega a los terceros utilizados hasta llegar al punto de la última milla, en donde se manejan más datos personales.

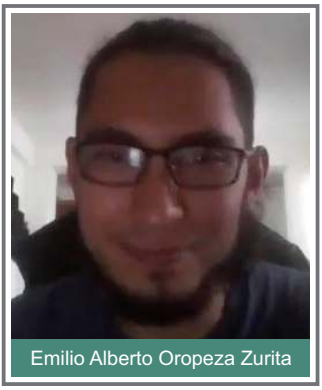
Juan Mario Posada Daza
Líder de Ciberseguridad
Accenture Colombia
A lo ya planteado podría agregar que en la cadena de suministro digital hay otros elementos como la adopción de nuevas tecnologías, la interoperabilidad y la interacción digital de los diferentes actores de la cadena, quienes, al automatizarse y hacer uso de tecnologías como la nube, internet de las cosas y la inteligencia artificial, enfrentan unos retos orientados en la seguridad.

Jeimy J. Cano M.
¿Cómo se reconocen o entienden los riesgos cibernéticos en la cadena de suministro, ahora en un contexto digital?

Juan Mario Posada D.
Se trata fundamentalmente de entender cuáles son los diferentes nodos dentro de la cadena, por eso nos referíamos al involucramiento de tecnologías emergentes y a la interacción que empiezan a tener los diferentes actores de la cadena de suministro. Esta situación trae consigo un cambio en los flujos de información lo que, a su vez, desencadena cambios en los puntos

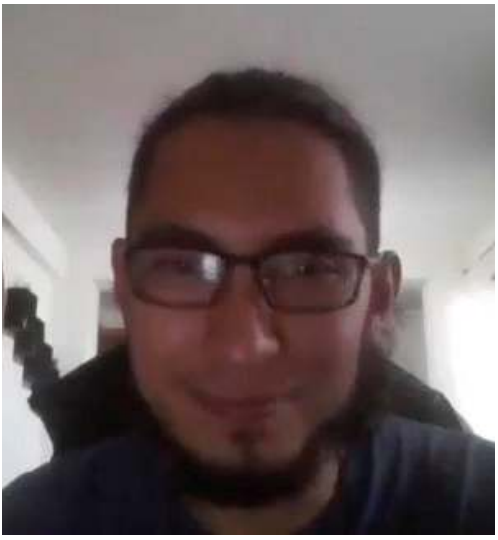

Liliana Patricia Quiñonez García


Juan Mario Posada Daza


Emilio Alberto Oropeza Zurita

sujetos a riesgos, dependiendo el tipo de cadena de suministro.

Emilio Alberto Oropeza Z.



Y no hay que olvidar que mucho de la interacción en la parte de la cadena de suministro digital inicia por un tema físico o por la gente involucrada en el medio. De ahí la necesidad de entender el negocio, porque muchas veces la misma empresa se convierte en el primer riesgo por no saber implementar los controles, situación que impacta de manera negativa la operación. Así mismo, es necesario contemplar que, una vez se tiene todo el flujo de la cadena de suministro, puede haber una consecuencia física derivada de un ataque cibernético, es cuando se requiere una ciberseguridad prospectiva.

A través de las nuevas tecnologías los riesgos aumentan, dando pie al robo de datos de los flujos de la cadena de suministro, estos datos pueden contener información personal que derivan a un riesgo en temas de regulaciones y leyes como GDPR, LGPD, la Ley Federal de Protección de Datos Personales; comúnmente estos datos que suelen utilizarse en la última milla.

Son varios puntos y riesgos los que debemos contemplar no solo en el mundo digital, sino también en el físico como consecuencia de la materialización de un ataque cibernético. Debemos considerar que varios riesgos del mundo digital se pueden trasladar al mundo físico como consecuencia de la materialización de un ciberataque, por eso es muy importante entender el negocio y poder implementar los controles con base en las necesidades de la operación.

Jeimy J. Cano M.

¿Eso significa que se van a mezclar los riesgos en algún punto? Es decir, ¿vamos a tener esa convergencia y ahí cómo distinguimos los asuntos? Porque esto se vuelve un reto precisamente en esos puntos donde todo converge.

Emilio A. Oropeza Z.

Así es, de ahí la necesidad de entender muy bien los flujos de la operación. Los responsables de la seguridad debemos tener ese entendimiento para saber en qué punto los controles digitales pueden afectar un tema físico o viceversa. Por ejemplo, si un control digital en al-

gún computador de operación no se activa de manera correcta, puede terminar en un ataque que afecte todo el sistema físico. Es muy importante que los responsables de la creación de los controles tengan en cuenta tales aspectos para determinar la diferencia entre los controles físicos y los digitales.

Liliana P. Quiñonez G.

Desde mi óptica jurídica con la Ley 599 de 2000 (Código Penal), se da una tipificación puntual a los delitos informáticos que terminan vulnerando los derechos de los usuarios de plataformas digitales, que afectan no solo a la persona natural, sino a la sociedad. Por ello con la evolución normativa, hoy tenemos la Ley de protección de datos (1581 de 2012), que no tiene un fin diferente a la salvaguarda de los datos personales, la carga, los temas de competencia, las invenciones (fórmulas) versus las garantías que esta misma ley ofrece, sin que éstos se vean afectados o estén en riesgo. En otras palabras, no solo se trata de tener sistemas que protejan los datos, sino de la seguridad en la recepción, almacenamiento, reproducción y transmisión de la información; tener implementado un sistema de riesgo y conocimiento del cliente final.

Emilio A. Oropeza Z.

También es importante validar y gestionar quiénes son todos nuestros terceros (TPRM), porque muchas veces la fuga de información es a través de ellos y eso se convierte en un tema complejo. La otra parte en la que coincido con Liliana, es saber cómo vamos a responder ante algún incidente cibernético; muchas veces nos enfocamos solamente en proteger y demostrar cuáles activos estamos protegiendo, pero no tenemos una respuesta a incidentes o a crisis, para saber en cuánto tiempo tenemos que dar un alcance, y claro, si estás cotizando en bolsa, por ejemplo, tienes 72 horas por mucho para notificar el alcance del ataque. No hay que enfocarnos solamente en los controles de protección que muchas veces nos solicitan los reguladores, también debemos tener todo un plan de respuesta a incidentes, a crisis para notificarlos de manera correcta a los terceros y a las entidades. Ninguna empresa está exenta de ser atacada, es importante madurar la respuesta ante este tipo de eventos.

Juan Mario Posada D.
Somos tan seguros como lo sea el eslabón más débil de la cadena de suministro, lo que quiere decir que, si éste está completamente expuesto en la cadena digital nos lleva a un efecto dominó.

Accenture lideró un estudio reciente de seguridad en el que plantea cinco pasos prácticos para iniciar el fortalecimiento de la cadena de suministro; el primero se refiere a tener la claridad de lo que el estudio llama el centro de gravedad con un programa o una oficina dedicada o una función dedicada a gestionar estos riesgos de la cadena de suministro que requieren, no solo conocimiento de ciberseguridad, sino también conocimiento específico de los sectores de industria y los procesos de negocio. El segundo paso es cómo obtener los mecanismos de visibilidad a través de toda la cadena. En tercera instancia el entendimiento de las amenazas y las debilidades de una manera holística; como cuarto paso la creación de esa caja de herramientas de soluciones a las que se pueda acceder en cualquier momento para asegurar la cadena de suministro, siempre que haya un nuevo actor o un cambio. Y, por último, mantenimiento y mejora para entrar en el ciclo virtuoso de planear, hacer, verificar, actuar y mejorar en forma continua.

Jeimy J. Cano M.
¿El sector logístico y de transporte en Colombia está preparado para atender y recuperarse ante un ataque cibernético? ¿Cuenta con prácticas de seguridad y control aplicadas y aseguradas?

Liliana P. Quiñonez G.
Por más esfuerzos y procedimientos, por más sistemas de gestión del riesgo implementados, jamás serán suficientes, toda vez que día a día aparecerán otros riesgos y el sector del transporte deberá estar preparado para asumirlos y contra atacarlos.

Hoy en sus procedimientos, las empresas de transporte terrestre de carga han venido adelantando los llamados “planes de continuidad”, lo cual permite dar mayor seguridad a la prestación de servicio de transporte; adicionalmente, la seguridad que brinda el sector logístico es el mantenimiento de requisitos ante las entidades competentes.

Juan Mario Posada D.
Sin el ánimo de desconocer los esfuerzos que se han hecho por parte de los actores logísticos para fortalecer la seguridad en la cadena, sí quiero mencionar el caso de malware de 2017, que se inició como un conflicto geopolítico por ataques a operaciones de negocios de Ucrania y terminó afectando a empresas globales grandes, con presupuestos bien importantes en temas de fortalecimiento de la ciberresiliencia de sus negocios, como los casos Maersk, Merck, y Mondelēz. Si me remito a los hechos

para analizar lo que ha sucedido en geografías y organizaciones probablemente mucho más maduras de lo que estamos en Colombia, flaco favor le hacemos a los actores de la cadena logística, haciéndoles pensar que ya están preparados para un ciberataque de alto impacto, porque, aunque se vienen haciendo importantes esfuerzos, retomando la dependencia de todos los eslabones de la cadena de suministro, los esfuerzos de seguridad deben ser coordinados y cooperativos. En los últimos años hemos visto muchos casos que demuestran la capacidad financiera y tecnológica más sofisticada de los adversarios. Bien decía Liliana que es necesario protegerse proactivamente para no estar un paso atrás.

Anticiparnos al entorno de amenazas comienza a cobrar relevancia. Quedarnos esperando, no nos permitirá visualizar hacia dónde están avanzando los cibercriminales ni como resultado una protección más eficaz.

Emilio Alberto Oropeza Z.
Elaboraré mi comentario en el sector logístico y de transporte para México.

A pesar de que en Colombia tienen más leyes orientadas al tema de ciberseguridad en comparación con México, aquí actualmente se está trabajando en elaborar una nueva ley en el tema de ciberseguridad. En el sector de transporte conozco a gente del ámbito de ciberseguridad y sé que implementan controles, pero no dejemos de lado que siempre va a existir un vector de ataque; como bien menciona Juan Mario, el eslabón más débil de la cadena de seguridad es el usuario, y muchas veces no es consciente del impacto que puede tener solo hacer un clic a una URL maliciosa; también contamos con los famosos insiders los cuales son vectores de ataque que a veces no se contemplan en los análisis de riesgos.

México apenas se está preparando, muy a pesar de esto, hay mucha tecnología que actualmente se emplea para ser proactivos en el tema de la ciberseguridad y así poder disminuir ciertos riesgos.

Para el tema logístico creo que lo vamos a dividir en dos grupos; existen las grandes empresas que pueden invertir millones de dólares en temas de ciberseguridad, y que fomentan una cultura de automatizar y crear sus propias herramientas, y existen las otras empresas, como las start-up's, pymes o empresas medianas, las cuales están entrando a este mundo del sector logístico y realmente no tienen contemplada una inversión en seguridad, este último grupo son los que considero como punto de falla, no solo para Colombia y México, sino a nivel LATAM, toda vez que no existe una cultura de seguridad hasta que tienen algún incidente.

Lo que deberíamos estar trabajando, como bien mencionaron todos,

es el tema de simulaciones de ataque, emplear análisis de riesgos prospectivo, como la matriz de riesgos VICA (Volátil, Incierto, Complejo, Ambiguo), la cual nos ayuda a crear escenarios prospectivos y de esta manera disminuir el riesgo de posibles ataques de día cero o de Supply-Chain (enfocado a DevOps); hago mención a este tipo de ataques debido a que muchas empresas grandes y medianas, así como Start-Up's, dependen del nivel de desarrollo de packages de terceros, ejemplo el suceso de Log4J; este tipo de ataques puede impactar de manera negativa en los desarrollos que se utilizan en el sector logístico.

Jeimy J. Cano M.

¿Cuenta el sector logístico y de transporte en Colombia con el talento humano necesario y suficiente para atender el reto del riesgo cibernético en su sector? Detalle su respuesta.

Emilio Alberto Oropeza Z.

La pregunta es un tanto compleja y la abordaré desde la perspectiva de México y con un poco de conocimiento que tengo por compañeros de Colombia en el sector logístico y de transporte. Creo que sí hay talento humano muy técnico y aquí cabe destacar lo siguiente, la persona técnica que va a administrar el equipo de ciberseguridad, debe conocer los procesos del negocio, toda vez que, si no conoce los flujos de la operación, lo más probable es que el control de seguridad que se implemente impacte de manera negativa una operación 24/7, sea del sector de transporte o logístico.

En México en todo el sector de transporte se podría decir que hay muchos recursos humanos, sin embargo, en el tema logístico como termina siendo un poco más compleja la operación, se complica encontrar recursos técnicos que decidan involucrarse para entender el negocio. Con base en mi experiencia les puedo comentar que la otra parte importante a tener en cuenta, es el famoso equipo en la logística que se llama *loss prevention*, porque ellos son los que ven un poco más el tema humano, sobre cómo se mueven los usuarios internos en la operación, una combinación entre la parte cibernética y de *loss prevention* pueden generar un tema de Threat Intelligence muy completo lo cual deriva en una vi-

sión prospectiva; concluyendo, si existen recursos pero no los suficientes o como la demanda laboral está exigiendo, falta involucrarlos más a nivel negocio dependiendo en qué sector estén.

Juan Mario Posada D.

Disiento un poco del planteamiento anterior, no porque no exista el talento, seguramente hay personas muy preparadas, tanto en México como en Colombia y el resto de Hispanoamérica, pero la realidad y lo que se está viviendo hoy en el mundo es que hay más demanda del talento en materia de protección, ciberdefensa, y ciberseguridad que la oferta que existe en el mercado y ese es un desafío grande a resolver. En firmas como la nuestra lo vivimos a diario, hay demanda de los clientes y tenemos que salir a buscar talento especializado, tarea que no es simple, es un asunto que implica trabajo. Se encuentran personas preparadas, pero no son las suficientes para la atención de la demanda y es en ese punto en donde me queda la duda.

Otro asunto que me parece importante tratar es el rompimiento del paradigma de la seguridad de las cuatro paredes, porque ya estamos en un entorno absolutamente sin fronteras, desde la perspectiva del ciberespacio, en donde la seguridad perimetral dejó de ser suficiente hace mucho tiempo y en el que se debe trascender los esfuerzos para la protección de la cadena de abastecimiento. En resumen, hay talento, pero no el suficiente.

Liliana P. Quiñonez G.

En mi opinión, el sector logístico colombiano cuenta con un gran talento humano en todas las áreas. Sin embargo, considero que jamás será suficiente la capacitación para apoyar el tema de riesgo detrás de un ciberataque o en la vulneración de los canales digitales.

Jeimy J. Cano M.

Sería interesante realizar una encuesta en el sector y observar si las empresas tienen un oficial de ciberseguridad. En FITAC podrían adelantar ese tipo de iniciativas para fortalecer la cadena de suministro.

Liliana Patricia Quiñonez G.

Por ahora lo que tenemos son los oficiales de cumplimiento, encargados de minimizar el riesgo, tema

que no se encuentra contemplado en nuestros afiliados, siendo ésta una buena propuesta.

Emilio Alberto Oropeza Z.
Aunque contamos con gente preparada, no es el talento suficiente y nunca lo habrá, es un patrón general en el tema tecnológico, porque las empresas van evolucionando y adaptándose a los nuevos desarrollos. El punto es cómo podemos tener esa visión para responder de una manera más ágil sin necesidad de que nos gane el atacante.

Jeimy J. Cano M.
¿Puede considerarse el sector logístico y transporte en Colombia una infraestructura crítica cibernética? ¿Cómo ve el futuro del sector en la gestión del riesgo cibernético?

Juan Mario Posada D.
Mi opinión es un rotundo sí, es parte de la infraestructura critica cibernética del país, porque no es sino mirar el impacto que podría tener una interrupción de los principales actores logísticos en las diferentes industrias; imaginemos lo que significaría una interrupción en la cadena de suministro de las farmacéuticas, el sector de energía, las empresas de gas o la industria de alimentos, para citar algunas. El sector logístico es clave para que todos los negocios operen de forma normal y atiendan las necesidades de las personas y en especial con la dinámica de los últimos dos años en la que el volumen de envíos y transporte de mercancías ha aumentado significativamente.

Emilio Alberto Oropeza Z.
Quizás en cinco años podría tener un rotundo sí. Considero que el tema logístico y de transporte debe ser una infraestructura crítica cibernética dependiente del sector. No va a ser el mismo impacto en la operación de una e-commerce en comparación con un transporte marítimo que lleva medicamentos, este último puede afectar de manera negativa a todo un país.

Existen varias empresas que están abordando el tema logístico y de transporte y ampliando su gama de recursos; por ejemplo, transportar medicamentos con drones. Por lo tanto, yo sí considero que en tres o cinco años todo este sector se convertirá en una infraestructura crítica cibernética, y por lo tanto deberíamos empezar a implementar ciertas regulaciones no solamente en Colombia o México, sino también en Latinoamérica. Será necesario pedir apoyo a distintas personas involucradas en este sector, no solo del área de ciberseguridad, para entender cuál puede ser el impacto y cómo podemos proteger sin afectar desde temas de regulaciones, las operaciones 24/7.

Liliana Patricia Quiñonez G.
El sector logístico y de transporte es considerado un sector atractivo, toda vez que no solo se podrían ver afectados los datos de los actores de este sector, sino también las

mercancías. Es cierto que se han implementado varios procedimientos para proteger las operaciones y los datos de los usuarios; sin embargo, jamás serán suficientes los esfuerzos para proteger y amparar el riesgo. Si bien el comercio es cambiante, también lo es el riesgo; es conocido que los delincuentes intentan estar un paso más adelante que el de los actores; no se trata de eliminar el riesgo, pero sí de minimizarlo.

Hoy el sector logístico tiene, además del procedimiento de continuidad de carga, la implementación de sellos satelitales, para la seguridad en la carga, además de los programas tecnológicos para los mismos fines. Este sector se viene preparando y formando arduamente para que el futuro no sea incierto.

Juan Mario Posada D.
Me devuelvo a lo que significa infraestructura crítica cibernética. La entiendo como los elementos de la infraestructura de una nación que, en caso de ser interrumpidos por un ciberataque de alto impacto, afectan el producto interno bruto, la economía y la salud, entre otros asuntos.

Analizando el caso del buque que quedó atravesado como consecuencia de la pérdida de control del capitán por un ataque cibernético, pues el impacto que eso tuvo en la logística global fue tan grande que hubo desabastecimiento de alimentos, medicamentos, de fuentes de energía y tantas otras cosas. Todo esto puede surgir en una situación de tal naturaleza.

Emilio Alberto Oropeza Z.
Totalmente de acuerdo con Juan Mario, al final todo ese tema derivado del significado de infraestructura crítica cibernética, es lo que terminaría afectando no solamente a nivel de gobierno, sino un impacto económico a nivel nacional o internacional, como lo vimos con el tema del gasoducto en Estados Unidos, Colonial Pipeline, que terminó afectando a varios países. Con base en este ejemplo, considero que sí es necesario dividir cuál es ese sector logístico tal vez más enfocado a un impacto global que pueda repercutir a nivel económico, medicinas, desabasto, a comparación de una infraestructura logística de e-commerce, toda vez que ésta sí puede impactar a cierta minoría o a ciertas personas dentro del aforo que están solicitando temas de compras, pero no es el mismo impacto que una infraestructura crítica cibernética. Por eso mencionaba el tema de tres a cinco años, lo hemos visto con Amazon que ya te llevan con un dron todas las cosas a tu casa, seguramente varias empresas van a utilizar distintos recursos tecnológicos para hacer la entrega o delivery de activos más críticos como medicinas, convirtiéndose en su momento en una infraestructura crítica cibernética.

Jeimy J. Cano M.
Les pido plantear algunas reflexiones finales.

Emilio Alberto Oropeza Z.
Con la definición que tenemos de infraestructura crítica cibernética para la cadena de suministro digital, detectamos que existen dos puntos a los que debemos prestar atención: mapear los flujos para entender los procesos internos de cada cadena de suministro e implementar controles para la capa 8, el usuario, sin perder de vista que en los próximos años con el uso de las nuevas y actuales tendencias tecnológicas surgirán nuevos riesgos de seguridad. Nosotros como expertos de la materia, debemos emplear una visión prospectiva, no solo implementar controles de detección y protección, sino también tecnologías que nos ayuden contrarrestar el impacto que pueden tener los ciberataques y reforzar la respuesta a incidentes, manteniendo siempre la mejora continua de nuestra estrategia.

Juan Mario Posada D.
En un mundo hiperconectado y con los efectos evidentes de la pandemia, la agilidad logística se hace más necesaria. Esto, en conjunto con un aumento significativo de los nodos, la superficie de ataque y los puntos de vulnerabilidad, nos debe llevar a reflexionar acerca de la suficiencia de los controles, las medidas de protección y el esfuerzo destinado al fortalecimiento de la seguridad en la cadena de suministro. Acá reitero que debemos comprender que la falla de uno puede tener impacto en muchos de los actores de la cadena.

Liliana Patricia Quiñonez G.
El sector logístico siempre debe estar a la vanguardia de los servicios requeridos y dar continuidad a la cadena logística; debe procurar que los actores de la cadena tengan una integración de la prestación de servicios y su continuidad, con ello se evitarían algunos impactos no solo en las cargas, sino posibles infracciones que conduzcan inclusive al cierre de las compañías. Así mismo, es necesario que las plataformas utilizadas para estos fines tengan seguridad en la transmisión y conservación de los datos; con ello se le brindaría seguridad, protección y tranquilidad al beneficiario final.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; En la actualidad es asesora y editora en escritura y producción de libros. Es editora de esta revista.*

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

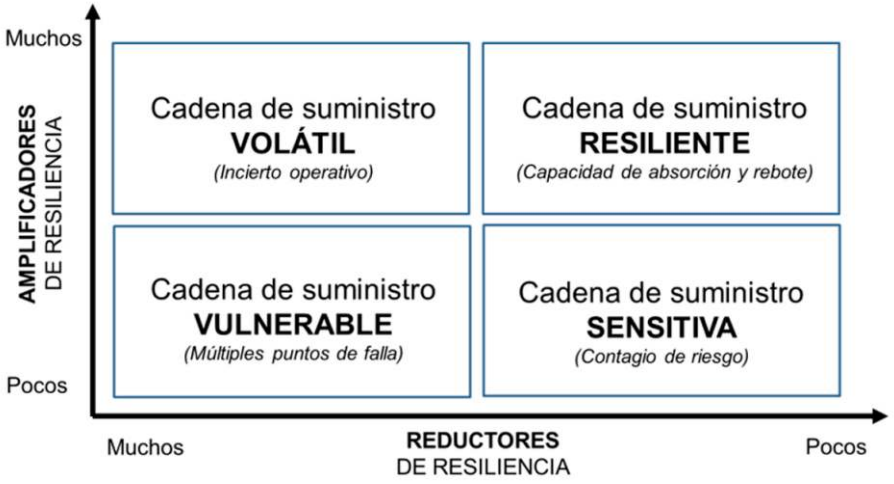


Figura 1. Matriz de resiliencia de la cadena de suministro digital
(Traducción libre de: Blackhurst et al., 2011)

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–.*

Sector comercio en Colombia

DOI: 10.29236/sistemas.n164a7

Gestión de redes de suministro digitales, sostenibles e inclusivas.

Resumen

En febrero de 2022 el CIATI-JFK presentó el resultado de una investigación en la cual se evidenció que la gestión de las redes de suministro en Colombia se acerca a las buenas prácticas en gestión de redes de suministro digitales, sostenibles e inclusivas, propuestas en este nuevo paradigma de gestión en un 49%, es decir, que el Gap con respecto a las buenas prácticas, es del 51%. Mientras que el reporte de investigación presentó agregados de los tres sectores de la economía colombiana, este artículo se centra en el análisis de los resultados obtenidos exclusivamente en el Sector Comercio, el cual se acerca a las Buenas Prácticas en *Gestión de Redes de Suministro Digitales, Sostenibles e Inclusivas* en un 46%; es decir, que el Gap con respecto a las Buenas Prácticas, es del 54%. El Análisis de los resultados se aborda desde 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. Resignificar estructuras mentales y evolucionar hacia Redes de Suministro Digitales es una necesidad empresarial.

Palabras clave

Cadenas de Suministro, Redes de Suministro, Redes de Suministro Digitales, Transformación Digital, Sostenibilidad

Introducción

Desde 1982 cuando Keith Oliver acuña los vocablos Supply Chain, su concepto evolucionó significativamente, desde la administración fragmentada de múltiples actividades (pronóstico de la demanda, compras, planeación de la producción, almacenamiento, empaque, transporte, marketing, ventas y otras más) hasta el concepto de Logística Integrada, claro está que pasando por una etapa de consolidación. En los años 90s el esfuerzo de una integración funcional se orienta hacia una total integración interna, y las actividades asociadas con el flujo de materiales se organizan bajo el concepto "sombrilla" de "Logística Integrada" (CIATI-JFK, 2022)

En la primera década del 2000 emerge un paradigma de gestión denominado Gestión de las Cadenas de Suministro que hace énfasis en un enfoque lineal y en la creación de valor. Para apoyar dicha gestión surgen y se popularizan dos modelos: el primero, denominado "Global Supply Chain Forum" (GSCF) que propone una gestión por procesos (estratégicos y operacionales): administrar las relaciones con el cliente, administrar la demanda, administrar el servicio al cliente, administrar el flujo de manufactura, administrar la orden, administrar las relaciones con el proveedor, administrar el desarrollo y comercialización de productos / servicios y administrar el retorno, dándole la máxima importancia al concepto de red y al relacionamiento entre sus nodos (Lambert, 2014); y el segundo, Supply Chain Operations Reference Model (SCOR Model) desarrollado en 1996 por el Supply Chain Council (SCC), y promovido y actualizado de manera permanente por la Association for Operations Management (APICS), modelo que igual se fundamenta en la gestión por procesos: planeación (plan), aprovisionamiento (source), manufactura (make), distribución (deliver), retorno (return) y habilitar (enable). Estos modelos siguen vigentes, solo que hoy se administran de otra manera y en otros entornos.

En la segunda década 2010, se consolida la "Gestión de las Redes de Suministro" poniendo en práctica un enfoque no lineal, que enfatiza en redes (Sinha & Wuestm, 2021). ¡Las convencionales Supply Chain o Cadenas de Suministro agonizan! ¡La creación de valor económico, social y ambiental mediante el enfoque de Redes de Valor toma fuerza en las organizaciones! ¡Supply Chain y Logística no son sinónimos!

Si bien la transformación digital empresarial se venía desarrollando como resultado de los avances tecnológicos, es en 2020 que bajo la presión de la Pandemia COVID-19 se hizo realidad para superar las

rupturas generadas en las Cadenas de Suministro domésticas y globales. La transformación digital se acelera de forma nunca imaginada y desde luego impacta la gestión de las Redes de Suministro resignificándolas en Redes de Suministro inteligentes, siempre On, siempre conectadas, en tiempo real y dinámicamente adaptativas: Digital Supply Networks o Redes de Suministro Digitales (Sinha & Wuestm, 2021).

De acuerdo con Leinwand y Matt Mani (2022) las empresas deben decidir creativamente para alcanzar nuevas ventajas competitivas en vez de sólo digitalizar lo que hacen hoy. Esto significa que los gerentes deben sepultar las creencias, mitos, principios y valores del pasado con respecto a las "Cadenas de Suministros", de hecho, ya colapsadas, y emprender alternativas audaces como por ejemplo la *creación de valor* de manera colaborativa con socios, en redes y ecosistemas, para producir más valor del que produciría una empresa individualmente. Se trata entonces de evolucionar de Cadenas a Redes de Suministro y de éstas a Redes de Suministro Digitales, Sostenibles e Inclusivas. Las Figuras 1, 2, 3, y 4 esquematizan estos estados evolutivos.

Estas Cadenas de Suministro lineales tradicionales que desafortunadamente aún operan en Colombia y en el mundo no están estrechamente integradas mediante procesos de coordinación, colaboración y cooperación (enfoque C^3), en tanto funcionan bajo el criterio de silos y están fragmentadas estructural y sistemáticamente; de ahí la ineficiencia y la incompetencia. Cadena de Suministro no es sinó-

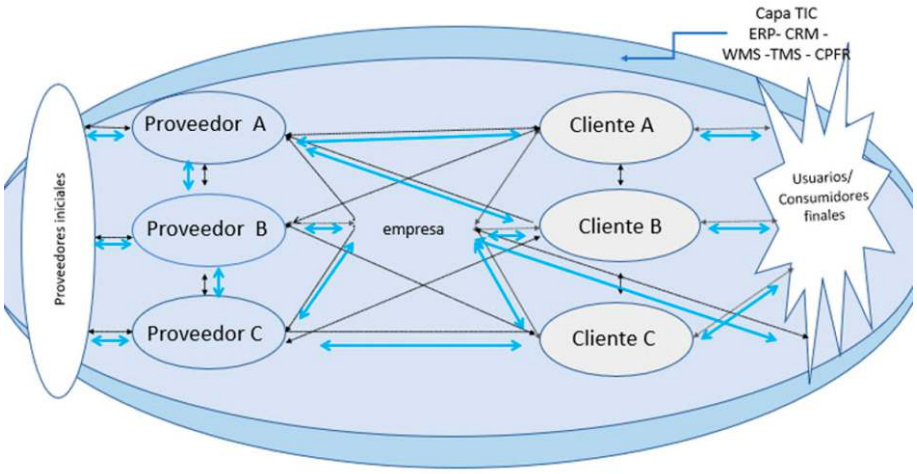
Figura 1.
Cadena de Suministro tradicional.

Nota: Tomado de: Deloitte. Kilpatrick & Barter (2020).

nimo de Logística… la Logística es una parte de aquella.

Estas Redes de Suministro son el resultado de la evolución de las Cadenas de Suministro lineales tradicionales, evidenciándose la disciplina como una entidad histórica en permanente evolución. Desde la perspectiva de Redes el enfoque C^3 se hace realidad a partir de la gestión de las relaciones con clientes y proveedores que se construyen cuando se activan los procesos los procesos estratégicos antes mencionados. Bajo este paradigma de gestión el relacionamiento juega un papel definitivo en la construcción de la estrategia en Gestión de Redes de Suministro centrada en el cliente, y debidamente alineada a la estrategia de la empresa que asuma el liderazgo, generalmente definida como empresa foco (Lambert, 2014). La gestión de las Redes de Suministro está soportada por una capa de Tecnología de Información y Comunicaciones (Capa TIC), mediante el uso de soluciones, como por ejemplo ERP, CRM, WMS, y otras más, optimizando las capacidades de todos los nodos de la Red y caracterizándose por ser más eficientes y competentes. Se hace énfasis en que Redes de Suministro no es sinónimo de Logística… las Redes Logísticas son una parte de aquellas. Una

Figura 2
Red de Suministro



Nota 1. En el mundo real ésta hipo-tética Red de Suministro podría formar parte de otras Redes de Suministro, y en ese orden de ideas surgirían las Redes de Redes. La competencia ahora no es empresa-empresa, sino entre Redes de Suministro.
Fuente. Sahid & Pinzón (2021).

empresa puede tener múltiples Redes de Suministros y por lo tanto múltiples Redes Logísticas.

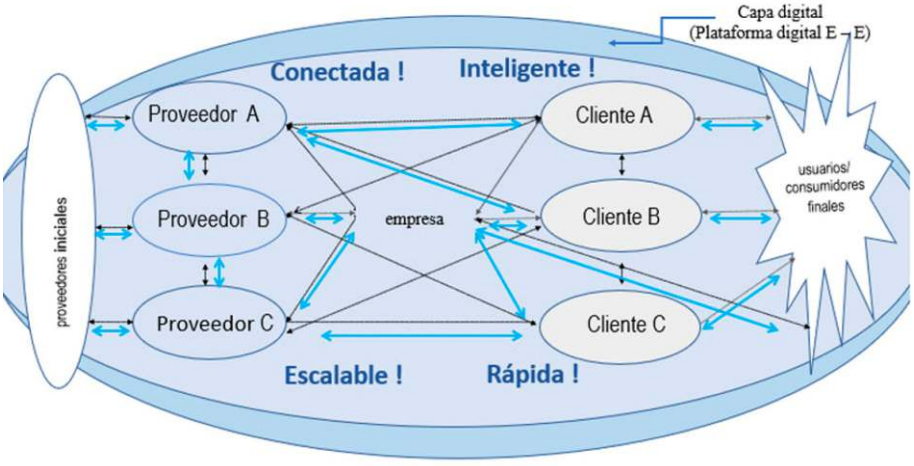
Estas Redes de Suministro Digitales son el resultado de la evolución de las Redes de Suministro. Una Red de Suministro Digital (DSN) puede definirse ampliamente como un conjunto integrado de capacidades que están habilitadas digitalmente e impulsadas por un flujo de información interconectado. En el centro de una DSN debe haber un núcleo digital que organiza simultáneamente las seis capacidades de Red de Suministro: planeación sincronizada, conectividad con clientes, manufactura inteligente, aprovisionamiento inteligente, desarrollo digital, y *fulfillment* dinámico (Sinha, 2021). Los datos e información que generan las capacidades convergen en el Digital Core para ser almacenados, distribuidos y analizados.

Según Temmen (2020) los beneficios de evolucionar de Cadenas a Redes de Suministro y de éstas a Redes de Suministro Digitales, son los siguientes:

Flexibilidad para personalizar las diferentes configuraciones de las Redes de Suministro a fin de satisfacer las demandas específicas del mercado.

Interconexión digital entre los nodos de la Red y con otras Redes de Suministro, para propiciar transparencia, fomentar la colaboración y mejorar la excelencia en todos los ámbitos.

Figura 3
Red de suministro digital



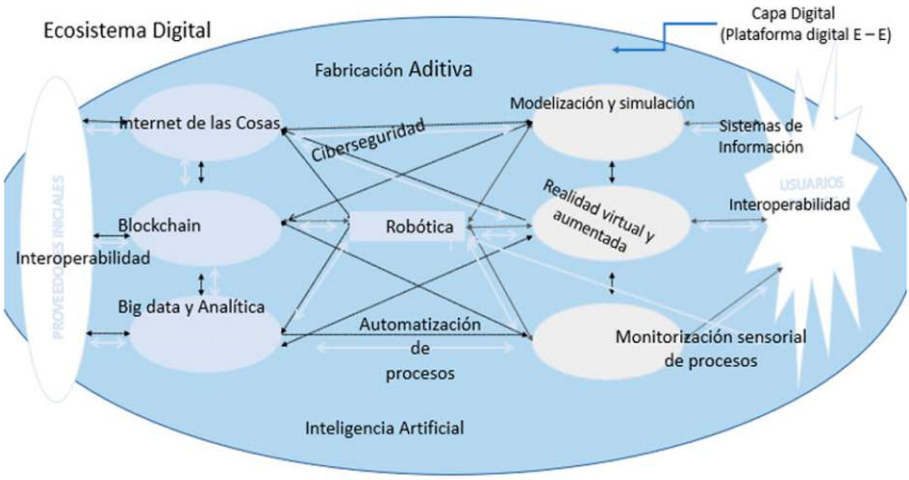
Nota: Tomado de Sahid & Pinzón (2021).

Eliminación de brechas y de la fragmentación en las Cadenas de Suministro.

Integración y transformación de procesos en ecosistemas de redes colaborativas dinámicas, resilientes, flexibles y efectivas para responder a señales de oferta y demanda cada vez más erráticas.

Respeto y valoración de las relaciones a largo plazo.

Figura 4
Ecosistema Digital

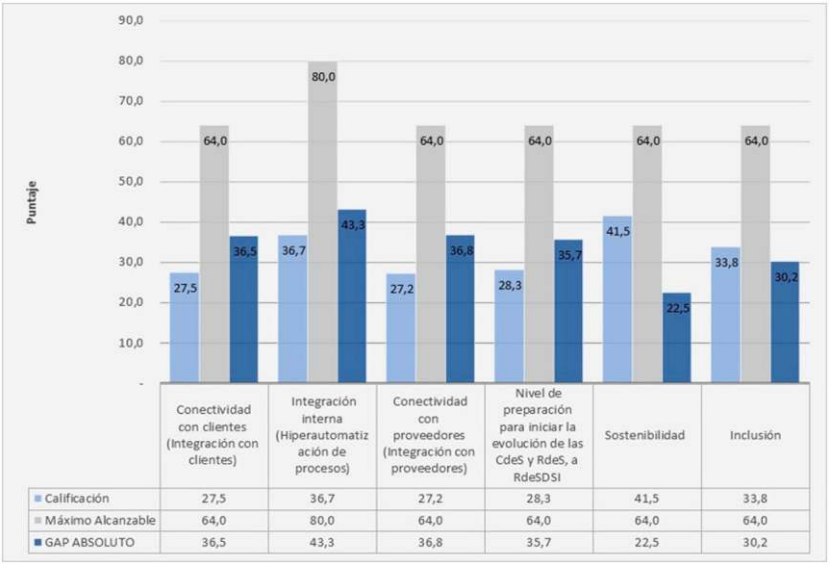


Nota 1. Estas Redes de Suministro Digitales establecen un hilo digital mediante canales físicos y digitales conectando información, productos y servicios de manera poderosa. Desde lo físico a lo digital: capturando señales y datos del mundo físico para crear un registro digital. *Desde lo digital a lo digital*: intercambiando y enriqueciendo la información utilizando análisis avanzados, inteligencia artificial, aprendizaje automático y otras tecnologías emergentes para generar información valiosa. *Desde lo digital a lo físico*: entrega información de manera automatizada y más efectiva para intervenir (producir acciones, decisiones y cambios) el mundo físico.

Nota 2. A diferencia de un modelo de *Cadena de Suministro* tradicional, las Redes de Suministro Digitales (DSN) son dinámicas, integradas y se caracterizan por un flujo continuo y de alta velocidad de información y análisis. La gestión de la Red de Suministro Digital ahora incluye la recopilación de información de datos distribuidos, sensores y activos conectados para impulsar mejoras viables a través de soluciones analíticas y digitales avanzadas. La propuesta de Deloitte Digital Supply Networks ayuda a las empresas y líderes empresariales a aprovechar esta oportunidad, crear una ventaja competitiva y competir para ganar.
Fuente. Sahid & Pinzón (2021).

A comienzos de 2021 el CIATI-JFK como integrante del Consejo Ejecutivo de la Mesa Sectorial de Logística, propone ante dicho Consejo el desarrollo de una investigación que permitiera develar en qué medida se acerca la gestión de las Redes de Suministro y las Redes Logísticas a las Buenas Prácticas en Gestión de Redes de Suministro Digitales, Sostenibles e Inclusivas, propuestas en el Modelo de Gestión, Procesos, Relaciones, Sostenibilidad e Inclusión (GPRDSI) para este nuevo paradigma de gestión, en Colombia. El Modelo GPRDSI permite apoyar investigaciones cualitativas y cuantitativas que utilicen categorías de análisis, y está soportado por una plataforma que admite **n** supracategorías de análisis, **n** categorías, **n** subcategorías y **n** buenas o mejores prácticas, y facilita el análisis de las

Figura 5
Resultados obtenidos en cada una de las categorías de análisis (capacidades). Sectores Industria, Comercio y Servicios



	Conectividad con clientes (Integración con clientes)	Integración interna (Hiperautomatización de procesos)	Conectividad con proveedores (Integración con proveedores)	Nivel de preparación para iniciar la evolución de las CdeS y RdeS, a RdeSDSI	Sostenibilidad	Inclusión
Calificación	27,5	36,7	27,2	28,3	41,5	33,8
Máximo Alcanzable	64,0	80,0	64,0	64,0	64,0	64,0
GAP ABSOLUTO	36,5	43,3	36,8	35,7	22,5	30,2

Nota 1. La figura muestra la calificación obtenida en cada una de las categorías de análisis, lo que explica el resultado de la medida en que la gestión de las *Redes de Suministro* se acerca a las Buenas Prácticas en la gestión de las *Redes de Suministro Digitales, Sostenibles e Inclusivas,* en Colombia.

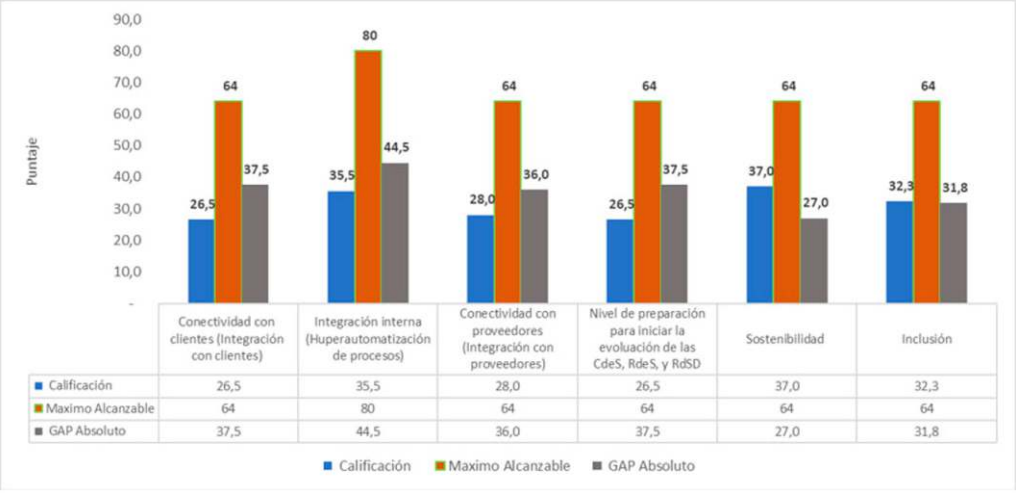
Nota 2. Los GAPs relativos más significativos corresponden a las categorías Conectividad con clientes (integración con clientes) con el 57%, Conectividad con proveedores (Integración con proveedores) con el 57%, y Nivel de preparación para iniciar la evolución de las CdeS y RdeS a RdeSDSeI) con el 56%.
Fuente. Sahid, Pinzón, Rodríguez, Pinzón & Florez (2022)

brechas identificadas. El Modelo GPRDSI está implícito en al reporte de investigación definitivo y en él se describe cada una de las categorías de análisis, relativas a esta investigación específicamente (Sahid, Pinzón, Rodríguez, Pinzón & Florez, 2022).

En febrero de 2022 el CIATI-JFK presentó el resultado final de la investigación en la cual se evidenció que la gestión de las Redes de Suministro en Colombia se acerca a las Buenas Prácticas (propuestas en dicha investigación) en *Gestión de Redes de Suministro Digitales, Sostenibles e Inclusivas* en este nuevo paradigma de gestión en un 49%, es decir, que el GAP con respecto a las Buenas Prácticas, es del 51%. La Figura 5 presenta los resultados, por categoría de análisis.

En consideración a que los resultados que se presentan en el reporte de investigación están relacionados con valores agregados para todas las empresas, el propó-

Figura 6
Resultados obtenidos en cada una de las categorías de análisis (capacidades). Sector Comercio únicamente



Nota 1. La figura muestra la calificación obtenida en cada una de las categorías de análisis únicamente del Sector Comercial. Luego de contrastar los resultados con los obtenidos para los tres sectores de la economía Figura 2, la capacidad *Integración con proveedores (conectividad con proveedores)* del Sector Comercio obtuvo una mejor calificación (28.0 puntos) que la obtenida por todos los Sectores (27.3 puntos). Las demás capacidades obtuvieron un puntaje menor que el obtenido por todos los Sectores. Las habilidades y (subcategorías de análisis) relativas a cada una de las categorías de análisis que deben mejorar las empresas del Sector Comercio se tratan a continuación.
Fuente. Elaboración propia.

sito de esta artículo es, entonces, realizar un análisis de los resultados obtenidos únicamente en las empresas del Sector Comercio y solamente en lo relativo a la Gestión de Redes de Suministro (no Logística), desde las siguientes categorías: Conectividad con clientes (integración con clientes), Integración interna (Hiperautomatización de procesos), Conectividad con proveedores (Integración con proveedores), Nivel de preparación para iniciar la evolución de las Cadenas de Suministro (CS) y Redes de Suministro (RS) a Redes de Suministro Digitales, Sostenibles e Inclusivas (RdSDSeI), Sostenibilidad e Inclusión. El artículo describe a manera de síntesis en qué consiste cada una de estas categorías y las habilidades que las empresas del Sector Comercio deben desarrollar para eliminar o atenuar las brechas actuales.

Conectividad con clientes (Integración con clientes)

Según el Modelo GPRDSI en entornos de Redes de Suministro Digitales, esta categoría está relacionada con la capacidad que tiene la empresa para construir relaciones (vínculos) temporales o perdurables con sus clientes, clientes de clientes y consumidores/usuarios finales, mediante la utilización de *Plataformas de Integración o Plataformas Digitales Multiempresa Extremo a Extremo* que permiten la conexión de datos estructurados y no estructurados de sistemas dispares, con el fin de ofrecer una visión unificada de las operaciones de la Red de Suministro y responder en tiempo real (CIATI-JFK, 2022).

Para disminuir el GAP que presentan las empresas del Sector Comercio es necesario desarrollar las siguientes habilidades:

Conectividad de la Red de Distribución. Esta habilidad se evidencia cuando la Red de Distribución aprovecha las capacidades digitales con fin de mantener una amplia visibilidad extremo a extremo, influencia y altos niveles de control con clientes, clientes de clientes y consumidores/usuarios finales, pudiendo reaccionar, relacionarse y comunicarse de manera eficiente y eficaz con estos, en tiempo real, diagnosticando sus necesidades e inclusive involucrándolos en la planificación de productos, iniciativas de diseño, gestión del riesgo y alternativas de relacionamiento en contexto de Economía de Bajo Contacto (EBC).

Inteligencia de la Red de distribución. Esta habilidad se evidencia cuando la Red de Distribución aprovecha la conectividad con sus clientes, clientes de clientes y consumidores/usuarios finales, con el fin de lograr el acceso a datos y utilizar la tecnología digital con el fin de convertir esos datos en información valiosa, aprovechando la analítica, los equipos cognitivos y las aplicaciones inteligentes, proporcionando la información ade-

cuada para la toma de decisiones y orientar la empresa hacia una Red de Distribución Inteligente (RDI). Los flujos de trabajo inteligentes se hacen realidad y las operaciones de activos son ágiles y resilientes (CIATI-JFK, 2022).

Escalabilidad de Red de distribución. Esta habilidad se evidencia cuando la empresa escala sus Redes de Suministro hacia sus clientes, clientes de clientes y consumidores/usuarios finales, en razón a sus altos niveles de conectividad e inteligencia (habilitada digitalmente), con el fin de hacer menos compleja la optimización de sus procesos así como su replicación, detectar fácilmente fallas y anomalías, reducir o agregar clientes según sea necesario, y mejorar la eficacia para apuntar a mercados, segmentos y clientes especializados, cuando sea necesario.

Rapidez de la Red de distribución. Esta habilidad se evidencia cuando la empresa distribuye productos/servicios de manera rápida, eficiente y efectiva a sus clientes, clientes de clientes y consumidores/usuarios finales, en razón a sus altos niveles de conectividad e interoperabilidad con los mismos.

Integración interna (Hiperautomatización de procesos)

Según el Modelo GPRDSI en entornos de Redes de Suministro Digitales, esta categoría está relacionada con la capacidad que tiene la empresa para integrar sus procesos internos y escalarlos hacia sus clientes, clientes de clientes y consumidores/usuarios finales, así como, a sus proveedores y proveedores de sus proveedores y hacia otros *Stakeholders*, mediante la utilización de *Plataformas de Integración o Plataformas Digitales Multiempresa Extremo a Extremo* que permiten la conexión de datos estructurados y no estructurados de Sistemas Dispares, para ofrecer una visión unificada de las operaciones de la Red de Suministro y responder en Tiempo real (CIATI-JFK, 2022). Para disminuir el GAP que presentan las empresas del Sector Comercio es necesario desarrollar las siguientes habilidades:

Comunicación interna. Esta habilidad se evidencia cuando la empresa hace de la comunicación interna un puente hacia la transformación digital y convertirse en un agente eficaz con el fin de propiciar el cambio en la organización.

Cultura Business Process Management (BPM)**.** Esta habilidad se evidencia cuando la empresa propicia el cambio en la organización, mediante la incorporación de la disciplina de gestión BPM. BPM propicia la optimización, agilidad, rendimiento, administración y control de los procesos de una organización y la respuesta adecuada a la volatilidad del entorno exterior de acuerdo con sus objetivos y estrategias organizacionales.

Automatización inteligente de procesos (IPA). Esta habilidad se evidencia cuando la empresa automatiza los procesos mediante la incorporación de Plataformas BPM y la utilización de tecnologías emergentes.

Desarrollo de las Capacidades humanas. Esta habilidad se evidencia cuando la empresa aprovecha la oportunidad creciente que se crea al automatizar procesos, con el propósito de que los colaboradores vean y vayan más allá de las habilidades técnicas e impulsen la creación de valor a través de sus capacidades humanas, puestas en práctica al interior de la organización y en sus relaciones con proveedores *Upstream* y clientes *Downstream*, mediante la utilización de Plataformas de Integración o Plataformas Digitales Multiempresa Extremo a Extremo que permiten la conexión de datos estructurados y no estructurados de Sistemas Dispares, a fin de ofrecer una visión unificada de las operaciones de la Red de Suministro y responder en tiempo real.

Formación del talento humano. Esta habilidad se evidencia cuando la empresa aprovecha las fortalezas que se construyen a partir de la formación, capacitación y entrenamiento de sus colaboradores a fin de propiciar la creación de valor y la innovación como recurso estratégico, y utilizarlo al interior de la organización y/o en sus relaciones con proveedores *Upstream* y clientes *Downstream*, mediante la utilización de Plataformas de Integración o Plataformas Digitales Multiempresa Extremo a Extremo que permiten la conexión de datos estructurados y no estructurados de Sistemas Dispares, para ofrecer una visión unificada de las operaciones de la Red de Suministro y responder en tiempo real.

Conectividad con proveedores (Integración con proveedores)

Según el Modelo GPRDSI en entornos de Redes de Suministro Digitales esta categoría está relacionada con la capacidad que tiene la empresa para construir relaciones (vínculos) temporales o perdurables con sus proveedores, y proveedores de sus proveedores y proveedores iniciales, mediante la utilización de *Plataformas de Integración o Plataformas Digitales Multiempresa Extremo a Extremo* que permiten la conexión de datos estructurados y no estructurados de Sistemas Dispares, para ofrecer una visión unificada de las operaciones de la Red de Suministro y responder en Tiempo Real (CIATI-JFK, 2022). Para disminuir el GAP que presentan las empresas del Sector Comercio es necesario desarrollar las siguientes habilidades:

Conectividad en la Red de aprovisionamiento. Esta habilidad se evidencia cuando aprovecha sus capacidades digitales, para mantener una amplia visibilidad Extremo a Extremo, influencia y altos niveles de control *Upstream*, pudiendo

reaccionar, relacionarse y comunicarse de manera eficiente y eficaz con sus proveedores, proveedores de sus proveedores y proveedores iniciales (*Upstream*), diagnosticando sus necesidades e inclusive involucrándolos en la planificación de productos, iniciativas de diseño, gestión del riesgo y alternativas de relacionamiento en contexto de Economía de Bajo Contacto (EBC).

Inteligencia en la Red de aprovisionamiento. Esta habilidad se evidencia cuando la empresa aprovecha la conectividad con sus proveedores, proveedores de sus proveedores y proveedores iniciales (*Upstream*), a fin de lograr el acceso a datos y utilizar la tecnología digital para convertir esos datos en información valiosa, aprovechando la analítica, los equipos cognitivos y las aplicaciones inteligentes, proporcionando la información adecuada para la toma de decisiones y orientar la empresa hacia una Red de Aprovisionamiento Inteligente (RAI).

Escalabilidad en la Red de aprovisionamiento. Esta habilidad se evidencia cuando la empresa escala sus Redes de Aprovisionamiento *Upstream* en razón a sus altos niveles de conectividad e inteligencia (habilitada digitalmente), los procesos son más fáciles de optimizar y replicar, las fallas y anomalías son más fáciles de detectar, y se encuentra en las mejores condiciones para reducir o agregar proveedores según sea necesario, y es eficaz a fin de apuntar a mercados, segmentos y proveedores especializados.

Rapidez en la Red de aprovisionamiento. Esta habilidad se evidencia cuando la empresa adquiere materias primas e insumos de manera rápida, eficiente y efectiva en razón a sus altos niveles de conectividad e interoperabilidad con sus proveedores, proveedores de los proveedores, y proveedores iniciales, *Upstream*.

Nivel de preparación para iniciar la evolución de las Cadenas de Suministro (CS) y Redes de Suministro (RS) a Redes de Suministro Digitales, Sostenibles e Inclusivas (RdSDSeI)

Según el Modelo GPRDSI en entornos de Redes de Suministro Digitales esta categoría está relacionada con la capacidad de la empresa para evolucionar hacia una organización fundamentada en Redes de Valor y Redes de Suministro y reconocer que la estrategia competitiva depende de lo digital (CIATI-JFK, 2022). Para disminuir el GAP que presentan las empresas del Sector Comercio es necesario desarrollar las siguientes habilidades:

- *Cultura.* Esta habilidad se evidencia cuando la empresa propicia la innovación impulsada por lo digital y así empoderar a los empleados con tecnologías digitales.

- *Tecnología.* Esta habilidad se evidencia cuando la empresa propicia el uso y adopción de tecnologías emergentes.

- *Organización*. Esta habilidad se evidencia cuando la empresa está alineada con el fin de respaldar la estrategia, la gobernanza y las ejecuciones digitales.

- *Insight*. Esta habilidad se evidencia cuando la empresa utiliza eficiente y eficazmente los datos comerciales de los clientes a fin de medir el éxito e informar sobre la estrategia.

Sostenibilidad

Según el Modelo GPRDSI en entornos de Redes de Suministro Digitales esta categoría está relacionada con la capacidad que tiene la empresa y sus Redes de Suministro para activar procesos que permiten "preservar, conservar y proteger los recursos naturales del planeta en beneficio de las generaciones actuales y venideras, y sus pilares son lo social, ecológico y económico" (Bruntland,1987).

La sostenibilidad de las Redes de Suministro está relacionada con la capacidad que tiene la empresa para gestionar los impactos ambientales y sociales dentro y a través de las redes de proveedores, empresas, distribuidores, clientes y usuarios/consumidores finales, en armonía con los Objetivos de Desarrollo Sostenible.

Compras sostenibles. Esta habilidad se evidencia cuando la empresa adquiere bienes y servicios con un elevado impacto positivo ambiental, social y económico como resultado de las eficientes y efectivas relaciones en la Red de Suministro *Upstream*.

Medio Ambiente. Esta habilidad se evidencia cuando la empresa actúa de tal manera que asegura que las generaciones futuras tendrán suficientes recursos disponibles a fin de tener la misma calidad de vida, o mejor, que las generaciones actuales, y asigna los recursos necesarios (personas, presupuesto, tecnología y otros) para su actuación.

Trabajo y derechos humanos. Esta habilidad se evidencia cuando la empresa propicia un buen trabajo o empleo digno donde existen oportunidades, se respetan los derechos, existe protección social y se fomenta el diálogo social.

Ética. Esta habilidad se evidencia cuando la empresa propicia valores de cooperación, bienestar compartido y visión de conjunto.

Inclusión

Según el Modelo GPRDSI en entornos de Redes de Suministro Digitales esta categoría está relacionada con la capacidad de la empresa para generar un ambiente laboral diverso y de esta manera aprovechar los efectos de la diversidad, y así alcanzar una ventaja competitiva en el negocio (CIATI-

JFK, 2022). Para disminuir el GAP que presentan las empresas del Sector Comercio es necesario desarrollar las siguientes habilidades:

Diversidad / inclusión. Esta habilidad se evidencia cuando la empresa formula y ejecuta la estrategia sobre diversidad / inclusión con compromiso del alto nivel (alta dirección) y la sinergia construida a partir de los esfuerzos individuales, a fin de obtener los resultados deseados.

Adquisiciones inclusivas. Esta habilidad se evidencia cuando la empresa concibe y hace realidad la *diversidad / inclusión* de proveedores mediante un proceso y no como un proyecto.

Empleo inclusivo. Esta habilidad se evidencia cuando la empresa genera empleo a personas en condición de discapacidad y jóvenes en situación de pobreza o cualquier otra condición distinta (género, orientación sexual, etnia, nacionalidad, edad, credo o discapacidad).

Métricas en diversidad e inclusión (D&I). Esta habilidad se evidencia cuando la empresa mide el impacto de su estrategia sobre *diversidad / inclusión*, en tanto considera la D &I como factor crítico de éxito empresarial. (D&I mejora la reputación de la empresa, mejora el clima laboral y la productividad, se incrementan los resultados financieros, soportan planes de inversión e innovación, entre otros)

Conclusiones / Reflexiones finales

La Gestión de las Redes de Suministro como disciplina se constituye en una entidad histórica en permanente evolución como se evidencia con la transformación del paradigma denominado Cadena de Suministro a uno nuevo denominado Gestión de Redes de Suministro Digitales, luego de haber transitado por el de Gestión de Redes de Suministro. De hecho, no es trata de afirmar, como se ha expresado en algunos eventos que es tan sólo es un "juego de palabras" o un problema "de sintaxis o de semántica".

Desde el punto de vista semántico el significado que contiene el vocablo "cadena" es absolutamente diferente al vocablo "red", como también el objetivo de la información que transmiten (pragmática) y su propósito (apobética). Lo real, lo que está sucediendo y lo que sucederá en el futuro es que las Cadenas de Suministro convencionales, domésticas o globales, se están extinguiendo en razón a están evolucionando hacia Redes de Suministro Digitales. Las "Cadenas de Suministro" del Sector Comercio deben mejorar significativamente las siguientes capacidades en aras de transformarse en Redes de Suministro Digitales:

- Conectividad con clientes: para integrarse más y mejor con sus consumidores/ usuarios finales.
- Integración interna automatizando procesos: para extender-

los más allá de sus propias fronteras.
- Conectividad con proveedores: para integrarse más y mejor con los proveedores de los proveedores.
- Preparación para iniciar o continuar con la evolución de las Cadenas de Suministro (CS) y Redes de Suministro (RS) a Redes de Suministro Digitales en entornos sostenibles e inclusivos: para no desaparecer.

Ahora, con el propósito de mejorar estas capacidades este artículo sugiere el desarrollo de un conjunto de habilidades para que las empresas del Sector Comercio propicien una transformación cultural que a la postre permita aceptar nuevos paradigmas organizacionales, aceptar el desafío de atraer y retener el talento humano, tomar decisiones basadas en datos, innovar, y hacer del cliente y del consumidor / usuario final el centro de la estrategia digital de sus Redes de Suministro, porque ellos, además de los productos y servicios ahora buscan experiencias más sencillas, el cumplimiento de protocolos de bioseguridad, más valor social y ambiental y la mejor propuesta de valor; porque ellos, ahora priorizan la velocidad, la exactitud, la confianza y la mejor experiencia posventa (comunicación, devoluciones, cambio de producto, servicio, mantenimiento…); y porque ellos están más informados y son más exigentes.

Lo anterior se logra siempre y cuando se cuente con un liderazgo efectivo.

Referencias

CIATI-JFK (2022). Evolución de las "Cadenas de Suministro". Recuperado de https://nmvsoluciones.com/ciati/ Plataforma de autoevaluación de la gestión de las Redes de Suministro y las Redes Logísticas Digitales, Sostenibles e Inclusivas.

Lambert, D. (2014). Customer relationship management process. En Fisher College of Lambert Business. The Ohio State University. *Supply Chain Management: Processes, Partnerships, Performance*. Tercera edición. (25 – 41). Sarasota Supply Chain Management Institute.

Sinha, A., Bernardes, E., Calderón, E. & Wuest, T. (2021). Digital Supply Networks. Transform your Supply Chain and gain competitive advantage with disruptive technology and reimagined processes. McGraw Hill.

Leinwand, P. & Matt Mani, M. (2022). Beyond Digital: How Great Leaders Transform Their Organizations and Shape the Future. Harvard Business Review Press.

Kilpatrick, J. & Barter, L. (2020). DELOITTE. COVID-19: Gestión del riesgo y las interrupciones en la cadena de suministro. Deloitte Global.

Sahid, F. & Pinzón, F. (14 de junio de 2021) *Gestión de Redes de Suministro y Redes Logísticas Digitales, Sostenibles e Inclusivas* El Modelo GPRDSI V2-2021.
[Ponencia] Congreso Internacional de Logística. Redes de Suministro Digitales. El futuro de la Logística, HOY.
Mesa Sectorial de Logística.

Sahid, F. Pinzón, F. Rodríguez, R. Pinzón, B. & Florez, L. (2022). Gestión de Redes de Suministro y Redes Logísticas Digitales, Sostenibles e Inclusivas. CIATI-JFK / Mesa Sectorial de Logística- SENA.

Deloitte. (s.f.). From supply-chains to supply networks https://www2.deloitte.com/nl/nl/pages/enterprise-technology-and-performance/articles/from-supply-chain-to-a-supply-networks.html

Temmen, M. (29 de septiembre de 2020). Linear Supply Chain Vs Digital Supply Network Supply. https://marian-temmen.medium.com/linear-supply-chain-vs-digital-supply-networks- 74919b3a95b6

ONU. (1987) Nuestro futuro común. Informe Bruntland. ONU.

MIT Center for Transportation & Logistic. (2020). State of Supply Chain sustainability 2020. MIT Center for Transportation & Logistics.

Fabiola Pinzón Hoyos, Msc. *Ingeniera de Sistemas. Especialista en Administración Financiera. Especialista en Logística de Producción y distribución. Magister en Gestión Logística. Magíster en Dirección Universitaria. Consultora. Investigadora. Profesora Universitaria. Coordinadora Académica y de Investigaciones Maestría en Gestión de Redes de Valor y Logística, Unipiloto. Directora Científica y Tecnológica Fundación CIATI-JFK.*

¡Cuidado!

Alto riesgo de empleados **comprometidos** y **motivados.**

Conozca más, **bajo su responsabilidad** en

acreditta.com

ACREDITTA

emprove

moodle Partner

CERTIFIED SERVICES PROVIDER

ÚNICO PARTNER CERTIFICADO EN MÉXICO

Expertos en Moodle

/emprove

/company/e-learning-improve/

e-mprove.com

+52 771 489 1037 | jmerino@e-mprove.com