Fall 8-7-2023

Modelo de Ciberseguridad para el Sector Logístico y Transporte Terrestre

Carlos Bermúdez

Jeimy J. Cano M.

Modelo de Ciberseguridad para el Sector Logístico y Transporte Terrestre

Artículo Completo

Carlos Bermúdez
Escuela Superior de Guerra
carlosbermudezs@yahoo.com.mx

Jeimy J. Cano M.
Universidad de los Andes
jcano@uniandes.edu.co

Abstract

The increase in the use of information technologies and the automation of processes in companies in the logistics and land transportation sector means that the cyber risks to which they are exposed are increasing, due to the fact that within their operations they share and process large volumes of information between interconnected systems to maintain their service offerings. This has become the challenge for this sector to develop capabilities to maintain the operation of its logistics cycle when it is under adverse cybernetic conditions. This document proposes a model for companies in the logistics and ground transportation sector to establish a level of cyber resilience that seeks to maintain the capacity of their logistics operations even when under cyber-attack. Likewise, explains its application in a representative company of the sector in Colombia to illustrate to companies in the sector a way to manage the causes and effects of any adverse cyber event.

Keywords

Cybersecurity; Cyber Resilience; Cyber Risk; Logistics Cycle.

Resumen

El aumento en el uso de tecnologías de información y la automatización de procesos en las empresas del sector logístico y transporte terrestre, hace que los riesgos cibernéticos a los que se encuentran expuestas sean cada vez mayores, esto debido a que dentro de sus operaciones se comparte y procesa grandes volúmenes de información entre los sistemas interconectados para mantener su oferta de servicios. Esto se ha convertido en el desafío de este sector para desarrollar capacidades que permitan mantener la operación de su ciclo logístico cuando este se encuentre bajo condiciones cibernéticas adversas. Este documento propone un modelo para las empresas del sector logístico y transporte terrestre para establecer un nivel de ciber resiliencia que busca mantener la capacidad de sus operaciones logísticas aun cuando se encuentre bajo un ataque cibernético. Así mismo, muestra su aplicación en una empresa representativa del sector en Colombia para ilustrar a las compañías del sector una forma de gestionar las causas y efectos frente a cualquier evento cibernético adverso.

Palabras Clave

Ciberseguridad; Ciber Resiliencia; Riesgo Cibernético; Ciclo Logístico.

Introducción

Un entorno competitivo al que tienen que enfrentarse las empresas del sector logístico y transporte terrestre hoy día, hace que demande el uso constante de nuevas tecnologías de información que les permita mantener sus operaciones como parte integral del producto o servicio suministrado a sus clientes.

Estos avances tecnológicos para el uso y tratamiento de información dentro de las operaciones logísticas y el rápido crecimiento que tienen hoy día, introducen una serie de amenazas y vulnerabilidades que crean un panorama de exposición a riesgos cibernéticos que, aunado al aumento de ciberataques, hace que el sector logístico esté entre los sectores más afectados en los últimos cinco (5) años según el informe del Estado de la Ciberseguridad en la Logística de América latina y el Caribe, desarrollados por la Comisión Económica para América Latina y el Caribe (Díaz, 2021).

Este panorama de riesgo cibernético hace que las empresas logísticas y de transporte terrestre se vean obligadas a preservar y salvaguardar sus operaciones en mayor o menor escala realizando inversiones en herramientas tecnológicas, capacitaciones de personal en ciberseguridad, así como procedimientos que permitan aumentar sus capacidades para mitigar y hacer frente a estos riesgos a los cuales se ven enfrentadas y poder resistir los ataques cibernéticos que se presenten (Cheung et al., 2021)

Estas inversiones y la capacidad de resistencia frente a los ataques cibernéticos demandan un enfoque ciber resiliente y un modelo de Ciberseguridad que se traduzca en una guía práctica que permita a las empresas de logística y transporte gestionar los riesgos cibernéticos y mejorar su postura de seguridad frente a las amenazas en el ciberespacio, así como fortalecer el sector logístico y transporte, y así mantener la confianza en las operaciones logísticas y sus clientes.

Para establecer el contexto de este modelo, se inicia con una lectura del contexto general del ciclo productivo de una empresa logística, basado en la experiencia propia en el sector logístico y transporte, y apoyado en investigación de ciclos logísticos de diferentes artículos científicos. Seguidamente se realizó un análisis de la normatividad que rige el sector logístico y transporte terrestre en Colombia con el fin de enmarcar cual es el contexto legal de ciberseguridad en el sector que permita a través del modelo propuesto delimitar la función y las operaciones, para finalmente aplicarlo en una empresa representativa del sector en Colombia.

A continuación, se identificaron los diferentes riesgos cibernéticos asociados al ciclo logístico que permiten establecer qué datos y sistemas son los críticos, dónde se encuentran, qué procesos claves los usan, quiénes son los responsables de uso, para establecer las diferentes amenazas e impactos a las cuales se enfrentan las actividades críticas de la logística y el transporte terrestre en Colombia. Finalmente, conectando los elementos anteriores se presenta el Modelo LCR (Logística Ciber Resiliente), para la protección de las operaciones del ciclo logístico frente a ataques cibernéticos en el cual se enmarca el aporte conceptual y práctico de este documento.

Para desarrollar lo anterior este artículo se estructura de la siguiente forma. En primer lugar se detalla el problema identificado en el ciclo logístico de las empresas del sector frente a la ciberseguridad, luego se presenta la revisión de la literatura alrededor de las diferentes temáticas relevantes para este estudio, seguidamente se propone el Modelo LCR donde se detallan sus fundamentos, elementos, relaciones y operación. Adicionalmente se describen los resultados de aplicación del Modelo LCR en una empresa del sector logístico y transporte en Colombia finalizando con las conclusiones de este estudio.

Declaración del Problema

El autor Arati (2020) en sus investigaciones y artículo sobre la ciberseguridad para la industria del transporte y la logística que a hoy es un blanco para el ciberdelito, resalta el uso de nuevas tecnologías tales como el internet de las cosas y la inteligencia artificial las cuales introducen nuevos riesgos en relacion con los ataques cibernéticos.

Los hallazgos encontrados por Arati (2020), muestran que el estado de conciencia de las organizaciones respecto a la ciberseguridad en la industria logística y transporte es muy bajo así como también describe que el 55% de los empleados logísticos sienten que no están preparados para identificar o manejar un ataque cibernético. Finalmente deja planteadas unas estrategias y medidas de seguridad a largo plazo para reducir significativamente los riesgos cibernéticos tales como un enfoque basado en riesgo, gestión de vulnerabilidades, segmentación de red y gestión centralizada, seguridad TI multicapa o defensa en profundidad y por último el monitoreo continuo (Arati, 2020).

Según los autores Chan, et al. (2021) coinciden en sus investigaciones con Arati (2020) cuando afirman sobre las desventajas que trae para el sector logístico y transporte el uso de nuevas tecnologías haciéndolo vulnerable a los ataques cibernéticos. Además, expresan que este tipo de industrias sufre de regulaciones y estándares cibernéticos rezagados, de una conciencia en ciberseguridad inadecuada y una escasez de talento en ciberdefensa. Así mismo centran su propuesta de modelo en el concepto de separar las vulnerabilidades cibernéticas en tres (3) categorías: la tecnología, relacionada con el uso de sistemas de posicionamiento, la nube, redes de interconexión, sistemas de alertas y monitoreo, procesamiento logístico entre otros.

Igualmente señala Chan, et al. (2021), la regulación, relacionado con la poca normatividad relacionada a la ciberseguridad que permita tomar conciencia sobre el impacto peligroso en el comercio mundial y la estabilidad económica que puede ocasionar un ataque cibernético y las personas y procesos, relacionado con las capacidades y la falta de conocimiento sobre ciberseguridad.

Estos autores definen tres (3) pasos que las empresas del sector logístico y transporte deben adoptar para mejorar sus posiciones internas de ciberprotección. Primero transformar la cultura empresarial en una que priorice la ciberseguridad como una forma de protegerse frente a las amenaza cibernéticas, segundo utilizar la función de la gestión de riesgos para atraer personal de ciberseguridad de universidades y empresas privadas con el fin de que se sientan atraídos al crear nuevos modelos de ciberseguridad generando retos profesionales y tercero ubicar la fuerza laboral tecnológica existente con habilidades en ciberseguridad, mejorar estas competencias, proponer incentivos con el fin de lograr que las empresas de estas industrias logren dominar las capacidades requeridas; Chan, et al. (2021).

Otros autores como Cheung, et al. (2021) quienes, en su investigación sobre la ciberseguridad en logística y gestión de la cadena de suministro, hacen una revisión de los estudios sobre los controles que mejoran este aspecto y las direcciones de investigaciones futuras que pueden realizarse a raíz de los hallazgos encontrados. Así mismo describen que debe adoptarse un enfoque de tres (3) etapas para una postura frente ataques cibernéticos dentro del sector, la primera etapa de planificación preventiva, la segunda de planificación de recuperación en tiempo real y la tercera de planificación posterior después de un ciberataque.

Algunos de los hallazgos encontrados por los autores Cheung, et al. (2021.) que se constituyen en elementos claves para la investigación planteada en el presente documento son los siguientes:

- Falta de datos reales de seguridad cibernética: relacionado con los pocos datos sobre ciberseguridad que se publican en el contexto de la logística dado que las empresas son muy reacias a compartir o divulgar información sobre incidentes cibernéticos debido a los acuerdos de privacidad existentes con los clientes o el potencial daño a la reputación de la marca; Cheung, et al. (2021).
- Estudios insuficientes sobre ciberseguridad en la gestión logística: la literatura existente se centra en las cadenas de suministro pasando por alto el papel de la ciberseguridad en la logística.
- Las empresas subcontratan su logística a terceros dejando que asuman la responsabilidad de la gestión de riesgos cibernéticos en relación con la logística.
- Falta de diversidad metodológica: se encontró que la mayoría de estudios revisados adoptan metodologías cualitativas marcando un grado de inmadurez metodológica en este
- Escasos estudios sobre las medidas relacionadas con la recuperación en tiempo real y las medidas posteriores dado que se centran más en medidas de control preventivas; Cheung, et al. (2021).

Sobre la base de los hallazgos anteriormente mencionados los autores Cheung, et al. (2021), dejan marcado el camino para futuras investigaciones cuyo eje de exploración se centren en metodologías

cuantitativas como una opción para modelos de ciberseguridad en el sector logístico, aplicar técnicas de optimización para estudiar y proponer medidas de recuperación en tiempo real y que para reducir la complejidad del problema, los investigadores pueden centrarse en una sola empresa o limitar sus estudios a los procesos logísticos como primer paso.

En ese sentido se indica que al analizar los estudios e investigaciones anteriores vemos que los modelos y estrategias propuestas por los autores se enfocan en la cadena de suministro de manera general pero no se percibe un tratamiento de la ciberseguridad asociado al ciclo logístico de este tipo de industria.

Es por eso que esta investigación se desmarca de esa línea general y según los futuros estudios de investigación propuestos por Cheung, et al. (2021), busca ahondar más en la definición de un modelo especifico que permita concatenar las actividades de los ciclos logísticos de las empresas del sector, gestionar los riesgos cibernéticos asociados a ellas y ser resiliente cuando se encuentren bajo un ciberataque.

Revisión de la Literatura

El autor Arati (2020) en sus investigaciones previas sobre la ciberseguridad para la industria del transporte y la logística, hace una descripción general del sector resaltando el uso de nuevas tecnologías tales como el internet de las cosas y la inteligencia artificial siendo los impulsores claves de la transformación digital dentro del mismo.

De igual manera plantea que este tipo de empresas se ha convertido en un blanco fácil para el ciberdelito dado que a medida que las cadenas logísticas se integran rápidamente con estas tecnologías, la existencia de muchas partes interesadas y terceros proveedores en estas actividades surge un riesgo significativo con respecto a los ataques cibernéticos.

Los hallazgos encontrados dentro de la investigación de Arati (2020), muestran que el estado de conciencia de las organizaciones respecto a la ciberseguridad en la industria logística y transporte es muy bajo así como también describe que el 55% de los empleados logísticos sienten que no están preparados para identificar o manejar un ataque cibernético.

De otra parte, Cheung et al. (2021) presentan elementos claves para esta investigación alrededor de la seguridad cibernética en el sector logístico:

- Falta de datos reales de seguridad cibernética: relacionado con los pocos datos sobre ciberseguridad que se publican en el contexto de la logística dado que las empresas son muy reacias a compartir o divulgar información sobre incidentes cibernéticos.
- Estudios insuficientes sobre ciberseguridad en la gestión logística.
- Falta de diversidad metodológica: se encontró que la mayoría de los estudios revisados adoptan metodologías cualitativas marcando un grado de inmadurez metodológica en este campo.
- Escasos estudios sobre las medidas relacionadas con la recuperación en tiempo real y las medidas posteriores dado que se centran más en medidas de control preventivas.

Algunas de las primeras pruebas de la resiliencia de la cadena de suministro se pueden encontrar en el trabajo de Christopher y Peck (2014), quienes propusieron un modelo de referencia para la caracterización de la resiliencia en la oferta y los principales aspectos que contribuyen a la resiliencia de la cadena de suministro se identificaron como reingeniería, cultura organizacional, agilidad y colaboración.

En el mismo contexto, Sheffi y Rice (2005) presentaron un modelo de disrupción basado en una teoría de disrupción propuesta para sistemas de producción, donde esta propuesta se representó como una disminución transitoria en el desempeño del proceso. Este aporte identificó ocho (8) fases secuenciales que describen un evento disruptivo: preparación, evento disruptivo, primera respuesta, impacto inicial, tiempo de impacto total, preparación para la recuperación, recuperación e impacto a largo plazo. Basándose en este modelo, Sheffi y Rice (2005) proponen un “mapa de vulnerabilidad” empresarial a través del cual se comparan las diferentes probabilidades y consecuencias de eventos de interrupción y se clasifican para priorizar.

Igualmente Sheffi y Rice (2005), identificaron la demanda de productos como la principal fuente de incertidumbre en la cadena de suministro y reconocieron el aumento de la incertidumbre global debido al aumento de las expectativas de los clientes, más competencia global, cadenas de suministro más largas y complejas, mayor variedad de productos y ciclos de vida del producto. Consideraron la resiliencia organizacional como una iniciativa estratégica para reducir la vulnerabilidad y, por lo tanto, reducir la probabilidad de que ocurra una interrupción. Finalmente, identificaron tres (3) factores importantes para desarrollar la resiliencia en una organización: redundancia, flexibilidad y cambio cultural.

Por su parte, el autor Linkov et al. (2013) propusieron una matriz de resiliencia de cuatro pasos que representan un proceso para los ciclos de gestión de eventos de interrupciones: i) planificar / preparar, ii) absorber, iii) recuperar y iv) adaptar. Cada uno de estos pasos se describe para diferentes dominios dentro de la organización (es decir, físico, de información, cognitivo y social). Estos autores han sugerido además cómo medir la resiliencia de acuerdo con esta matriz.

Con base en el marco propuesto por Christopher y Peck (2014), así como en un estudio de investigación empírica para identificar vulnerabilidades y capacidades dentro de las organizaciones, Pettit, Fiskel y Croxton (2010) propusieron el marco de evaluación y gestión de la resiliencia de la cadena de suministro (SCRAM). Este marco identifica una relación activa entre las capacidades y las vulnerabilidades en una organización, y su resiliencia resultante. Argumentan que el nivel de resiliencia al que debe aspirar una empresa es un equilibrio entre el desarrollo de múltiples vulnerabilidades (debido a la falta de inversión en capacidades), lo que podría resultar en interrupciones con efectos económicos indeseables, e invertir en muchas capacidades lo que erosionaría la rentabilidad. Por lo tanto, destacan una compensación económica entre inversión (capacidades) y riesgo (vulnerabilidades).

Blackhurst et al. (2011) propusieron un marco de resiliencia global basado en la teoría de sistemas y el marco propuesto por Sheffi y Rice (2005). Distinguen entre potenciadores de la resiliencia y reductores de la resiliencia, que son atributos organizacionales que aumentan o disminuyen la capacidad de una empresa para recuperarse rápida y eficientemente de un evento disruptivo. Identificaron trece (13) potenciadores de la resiliencia y siete (7) reductores de la resiliencia, cada uno dentro de tres (3) categorías. Su trabajo deriva estos atributos de un entorno industrial y, por lo tanto, puede servir como base para futuras investigaciones en la confirmación empírica de estos u otros atributos de resiliencia.

Modelo Propuesto

Partiendo del estudio realizado de los anteriores modelos propuestos de la cadena de suministro y considerando que no se identifican muchas aproximaciones específicas a modelos relacionados con la resiliencia y ciberseguridad sobre el ciclo logístico, el modelo que se describe a continuación propone un marco de trabajo conceptual y práctico que habilita a las empresas del sector logístico y de transporte mantener niveles de ciber resiliencia y hacer frente a las interrupciones cuando se presente un ataque cibernético sobre sus operaciones.

Para describir el modelo de ciberseguridad propuesto se establecen algunos fundamentos que definen las características esenciales sobre los cuales opera, seguido se relacionan los elementos del modelo que son los componentes activos y vigilantes que la empresa debe tener en cuenta para mantener un ambiente resiliente frente a un ataque cibernético, posteriormente se definen las relaciones del modelo que permite establecer la coordinación de cada uno de dichos elementos, para finalmente establecer la operación de cómo cada uno de sus componentes operan para mantener la oferta de valor logístico.

Fundamentos del Modelo

El modelo de ciberseguridad propuesto establece sus bases en los siguientes fundamentos los cuales permiten entender el contexto en el cual se desarrolla.

- La oferta de valor logístico. Cuando ocurre un ataque cibernético se debe propender por mantener la oferta de valor ofrecida a los clientes que requieren un servicio logístico y de transporte.
- Estructura de ciberseguridad alineada al ciclo logístico, que para efectos del modelo se define el ciclo logístico en la Figura 2.

- Gestión de riesgo cibernético, esto lleva dentro del modelo a mantener el ciclo logístico asegurado por lo que es importante identificar, medir, evaluar y tratar los diferentes riesgos cibernéticos a los cuales se encuentran expuestas las actividades de la operación logística y de transportes.
- Gestión de resiliencia cibernética, en este contexto se indica que, el desarrollo de esta resiliencia dentro del modelo se podría considerar dentro de los siguientes aspectos: uno, qué tan dominante y cuáles ventajas competitivas tiene la empresa frente al mercado en el que se opera, y dos, cuál es su capacidad para absorber los impactos frente a los ataques cibernéticos, lo cual permite establecer dentro del modelo propuesto el nivel de resiliencia con el que se cuenta.

Elementos y Relaciones del Modelo

Partiendo de los fundamentos que sustentan el modelo, para efectos de identificarlo se ha denominado Modelo LCR (Acrónimo de Logística Ciber Resiliente).

Para entender la forma como se relacionan los elementos del modelo se propone el siguiente diagrama del modelo como lo muestra la Figura 1 que nos permite identificarlos e interrelacionarlos.

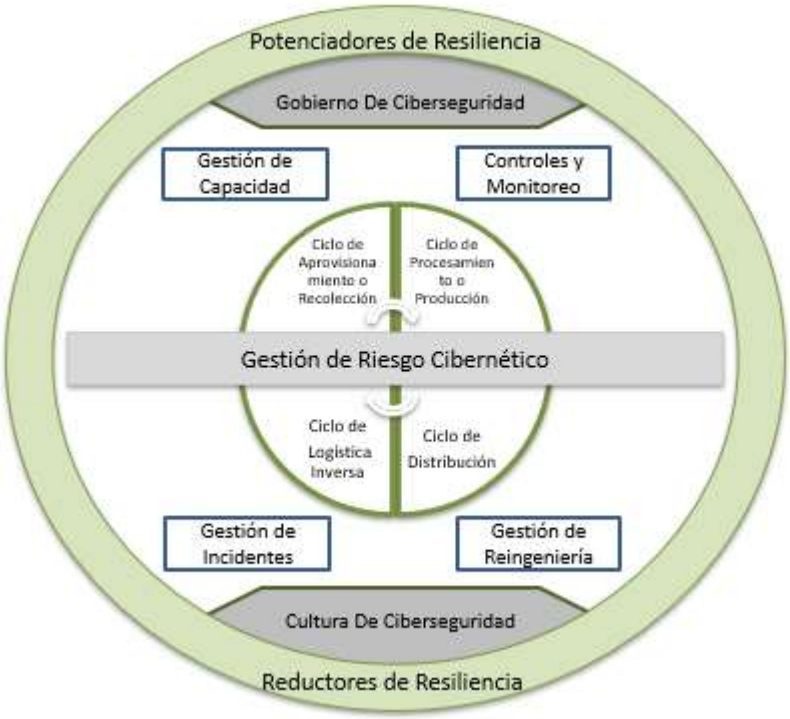

Figura 1. Modelo LCR (Logística Ciber Resiliente)

Como fundamento clave el modelo LCR propuesto se realiza de manera circular asemejando una "pelota antiestrés" para generar la conciencia del efecto absorción de impacto cuando un ataque cibernético pueda poner en riesgo la resiliencia en el ciclo logístico, es así como el modelo está compuesto por las siguientes líneas de relaciones que permiten su entendimiento:

- La línea de relación círculo central encontramos el ciclo logístico, el cual se convierte en el elemento que representa el fundamento del negocio logístico.
- En la línea central se encuentra la gestión de riesgo cibernético de manera transversal a todo el modelo, el cual atraviesa el ciclo logístico manteniendo una relación directa con él, dado que todos los elementos del ciclo logístico deben estar enmarcados bajo un nivel de riesgo cibernético el cual debe ser identificado, evaluado y tratado.

- En la siguiente línea encontramos elementos de apoyo en el cual se centra toda la ejecución de controles y procedimientos de apoyo que permiten absorber los impactos de un ataque cibernético que pueda recibir el ciclo logístico, su acción principal es medir la capacidad de operaciones del ciclo, mantener una adecuada implementación de controles, un monitoreo constante, estar preparados en caso de una interrupción y realizar una reingeniería frente a las operaciones logística posterior al impacto de interrupción.
- La línea estratégica se relaciona con los elementos de estructura de gobierno y cultura de ciberseguridad, los cuales según el modelo se colocan al borde de la última línea como posición estratégica que permite la medición y la toma de decisiones sobre la línea de los elementos de apoyo. Encontramos todo el direccionamiento de acciones que se deben seguir para mantener la operación del ciclo logístico en condiciones normales y resiliente o cuando este se encuentre bajo un ataque cibernético.
- La última línea que representa la resiliencia en términos de Blackhurst et al. (2011).

Estas líneas mencionadas que nos permiten dividir el modelo en ciclos de acciones para establecer la forma de operación de este el cual se describe en el capítulo siguiente.

Operación del Modelo

Es importante que antes de la implementación y operación del modelo, se realice la designación de dos (2) roles principales, el primero relacionado con la logística, que es la persona con el conocimiento de las operaciones logísticas y de transporte y el segundo relacionado con la ciberseguridad que es la persona con el conocimiento técnico y del negocio necesario para llevar a cabo el aseguramiento de las operaciones frente a los ataques cibernéticos que se pueden enfrentar.

Se definió, siguiendo a Blackhurst et al. (2011), que un potenciador de resiliencia es un atributo que aumenta la capacidad de una empresa para recuperarse rápida y eficientemente de un evento disruptivo y un potenciador de resiliencia realiza el efecto contrario que es disminuir dicha capacidad.

Así mismo se estableció el ciclo logístico propuesto como se observa en la Figura 2.

Figura 2. Ciclo Logístico Propuesto (Elaboración propia)

Establecido lo anterior, la forma como las empresas del sector logístico y transporte deben implementar y operar el Modelo LCR se define en las siguientes fases:

- Identificar el ciclo logístico, relacionado con las actividades definidas en la Figura 2
- Identificar las actividades del ciclo logístico, para definir el alcance y la funcionalidad de cada ciclo
- Identificar los habilitadores de la operación, se deben identificar todos los sistemas, elementos de TI/TO (Tecnología de información/Tecnología de operación) que hacen parte de las actividades del

ciclo logístico incluyendo aquellos componentes definidos en la normatividad para el sector y que definen alcances o restricciones a la operación.

- Identificar los potenciadores (planes de formación en ciberseguridad, estrategias de mitigación de riesgos, roles y responsabilidades, controles, sistemas de monitoreo, estructura y actividades del ciclo logístico, entre otros) y reductores de resiliencia (regulaciones y normatividad logística, control y requisitos sobre proveedores, limitaciones de procesamiento técnico, limitaciones sobre las actividades y operaciones logísticas, entre otros), son los elementos del Modelo LCR que van a permitir realizar un diagnóstico y establecer un nivel de resiliencia para el ciclo logístico.

  Así mismo, para cada potenciador o reductor, se debe establecer un criterio de calificación de resiliencia que permita evaluar como alto o bajo teniendo en cuenta su contexto dentro del ciclo logístico como se encuentra descrito en la Tabla 2.

  Se propone el porcentaje del 80% como un valor inicial de calificación del criterio de resiliencia estableciendo que para los potenciadores el criterio de calificación de resiliencia se considera alto cuando sea mayor o igual al 80% y bajo sea menor al 80%. Para los reductores el criterio de calificación de resiliencia se considera alto cuando es menor al 80% y bajo cuando es mayor o igual al 80%. Esto basado en la teoría de OKR (*Objective and Key Result*) que en el manual de OKR propuesto por los autores Contero y Martín (2020) definen una evaluación del 0 al 100% pero establecen que resulta óptimo alcanzar una medición del 80%

- Establecer el nivel de resiliencia, para ello se detalla una tabla para concretar dicho nivel.

Referencia	Descripción	Potenciadores	Reductores
Muy Alto	>=90% <=100%	Alto	Bajo
Alto	>=80% <=89%	Alto	Bajo
Bajo	>=40% <=79%	Bajo	Alto
Muy Bajo	>=0% <=39%	Bajo	Alto

TABLA 1. Nivel de referencia de medición de potenciadores y reductores

Acto seguido se debe registrar la calificación para cada uno de ellos, y se debe proceder a contabilizar con el fin de establecer la cantidad de potenciadores altos y bajos, así como la cantidad de reductores altos y bajos que nos permita establecer el nivel de resiliencia con base en lo propuesto en la Tabla 2.

Condición De Potenciadores	Clasificación
Si todos los Potenciadores de resiliencia cumplen el criterio de resiliencia alto (>= 80%)	Potenciadores Altos
Si uno o todos los potenciadores de resiliencia cumplen el criterio de resiliencia bajo (< 80%)	Potenciadores Bajos
Condición De Reductores	Clasificación
Si uno o todos los reductores de resiliencia cumplen el criterio de resiliencia alto (< 80%)	Reductores Altos
Si todos los reductores de resiliencia cumplen el criterio de resiliencia bajo (>=80%)	Reductores Bajos

TABLA 2. Matriz de criterios de clasificación de potenciadores y reductores

Ya clasificado el tipo de potenciadores y reductores se establece el nivel de resiliencia para el cual se utiliza la matriz de la cadena de abastecimiento propuesta por Blackhurst et al. (2011), donde se hace una adaptación de dicha propuesta y se utiliza el termino de ciclo logístico como se muestra en la Figura 3.

Figura 3. Matriz de resiliencia (*Adaptado* de Blackhurst et al., 2011)

- Si los potenciadores son altos y los reductores son altos se establece que el ciclo logístico es volátil, significa que los reductores de resiliencia son los que causan dicha volatilidad interpretado en ciertas características tales como múltiples actividades del ciclo logístico no controladas, incumplimiento de regulaciones, falta de capacidad de infraestructuras físicas y tecnológicas y falta de control y seguimiento en la gestión de proveedores. Sobre estos reductores, se deben establecer acciones prioritarias para disminuir sus niveles y se deben monitorear y conservar un esfuerzo sostenido en los potenciadores para mantener sus niveles altos.
- Si todos los potenciadores son altos y todos los reductores son bajos se establece que el ciclo logístico es resiliente, que es la razón de ser y el estado ideal en el que se debe mantener el Modelo LCR, interpretado en características tales como un capital humano educado y formado en ciberseguridad, estrategias de mitigación definidas, así como procesos de retroalimentación y reingeniería posterior a la interrupción, programas de gestión de riesgo cibernético, contingencias, cooperación y colaboración definidos, cumplimiento de regulaciones, gestión con proveedores controlados, ofertas de valor dinámicas y flexibles y una capacidad operativa resiliente física y tecnológica.
- Si los reductores son altos y los potenciadores bajos se establece que el ciclo logístico es vulnerable, es decir que tanto los potenciadores como los reductores en este caso son los que causan dicha vulnerabilidad y se deben establecer acciones inmediatas para aumentar los niveles de resiliencia en los potenciadores y disminuir los niveles de resiliencia en los reductores. Este es el estado menos deseado de resiliencia para la organización y se debe evitar este resultado que estaría enmarcado en las características de manera contrario a las definidas en la medición resiliente.
- Si los reductores son bajos y los potenciadores bajos se establece que el ciclo logístico es sensible, significa que los potenciadores en este caso son los que causan dicha sensibilidad interpretado en ciertas características como un capital humano sin la suficiente formación y educación en ciberseguridad, falta de estrategias de mitigación así como la falta de planes concretos efectivos para las interrupciones presentadas y su posterior retroalimentación y planes de reingeniería, deficiencia o falta de programas de gestión de riesgos cibernéticos y sus respectivos controles y falta de capacidad de monitoreo de las actividades y sistemas del ciclo logístico, lo que hace que se deba ejecutar acciones inmediatas tendientes a aumentar los niveles de resiliencia de los potenciadores y monitorear y conservar un esfuerzo sostenido que permita que los reductores permanezcan en un nivel bajo.

Este nivel de resiliencia con sus potenciadores y reductores se convierte en un tablero de control del Modelo LCR el cual debe ser actualizado y medido (establecer un nuevo nivel) cada vez que se realiza una evaluación de riesgos cibernético, incorporación de nuevas tecnologías (habilitadores de operación), se crea

un nuevo ciclo logístico, cuando ocurran incidentes cibernéticos o cambios significativos en la infraestructura de apoyo.

La periodicidad de actualización y medición debe realizarse mínimo una vez al trimestre y sus resultados deben ser comunicados a través del gobierno de la ciberseguridad a toda la organización y a la junta directiva una vez al semestre.

Resultados

Cumplidas las fases del modelo descrito anteriormente, esta herramienta produce como resultado dos (2) tableros de control asociados al nivel de Ciber resiliencia y a la gestión de riesgo cibernético.

La aplicación del modelo se adelantó en una compañía reconocida del sector logístico y transporte en Colombia dado que hoy día mueve la mayor cantidad de envíos a nivel nacional, más de 7 millones de envíos mensuales. Cuenta con una infraestructura física de más de 3500 puntos así como una arquitectura tecnológica de más 1300 servidores, 6000 equipos, más de 800 bases de datos y más de 200 módulos de aplicativos que apalancan las operaciones logísticas haciendo que la operación sea la más grande y robusta del país lo que implica que la aplicación del Modelo LCR en esta empresa ofrezca orientaciones sobre cómo puede materializarse operacionalización en el sector.

Primero se estableció el nivel de resiliencia representado con el cuadro de color amarillo, donde se evaluaron 17 potenciadores y 7 reductores de resiliencia cuyo resultado se muestra en la Figura 4. Este color se utiliza para resaltar cual es el nivel de potenciadores que en este caso son bajos y cuál es el nivel de reductores que ente caso son altos, luego según la combinación de éstos se resalta el nivel de resiliencia que en este caso es un ciclo logístico sensible.

Total Potenciadores	Total Reductores
17	7
Potenciadores Altos	**Reductores Altos**
5	0
Potenciadores Bajos	**Reductores Bajos**
12	7

NIVEL DE RESILIENCIA RESULTADOS		
Color De resultados		Resultado Nivel De Resiliencia
Ciclo Logístico Volátil	Ciclo Logístico Resiliente	Ciclo logístico volátil: potenciadores altos y reductores altos
		Ciclo logístico resiliente: potenciadores altos y reductores bajos
Ciclo Logístico Vulnerable	Ciclo Logístico Sensible	Ciclo logístico vulnerable: potenciadores bajos y reductores altos
		Ciclo logístico sensible: potenciadores bajos y reductores bajos

Figura 4. Nivel de ciber resiliencia (Elaboración propia)

La figura anterior muestra un ciclo logístico sensible debido a que la cantidad de potenciadores mayores fueron los bajos mientras que los reductores fueron bajos tomando como base la Tabla 2.

Para la gestión de riesgo cibernético, que es el segundo tablero de control, se tomó como base el modelo propuesto por Cano (2017) la ventana de AREM, como un recurso metodológico en la gestión de riesgos cibernéticos, en el cual se identificó y clasificó cada uno de los riesgos asociados al ciclo logístico cuyo resultado se muestra en la Figura 5.

Gestión de Riesgo Cibernético **Ventana de AREM**

Lo que conoce el entorno	Amenazas y riesgos conocidos R1 R2 R3 R4 R5 R12	Amenazas y riesgos latentes R6 R7 R8 R10 R11 R14
Lo que desconoce el entorno	Amenazas y riesgos focalizados R13 R15 R18	Amenazas y riesgos emergentes R16 R17
	Lo que conoce la organización	Lo que desconoce la organización

Figura 5. Ventana de AREM parar Riesgo Cibernético (Cano, 2017)

El resultado obtenido frente al panorama de riesgos cibernéticos establece que el modelo LCR marca una necesidad de ir más allá de los riesgos conocidos y de los esquemas tradicionales de identificación y evaluación de riesgos.

Basado en lo anterior se tiene una vista sistémica como tablero de control de los riesgos cibernéticos en cuatro cuadrantes, que va más allá de una lectura técnica, para convertirse en una construcción colectiva y una visión de riesgo cibernético del ciclo logístico propuesto en el modelo LCR. De esta forma, los riesgos se priorizan en su tratamiento de acuerdo con los niveles de resiliencia propuesto en la Figura 3.

Conclusiones

El modelo LCR (Logística Ciber Resiliente) descrito se presenta como una herramienta práctica que facilita a las empresas del sector logístico y transporte conectar y visualizar el ciclo logístico en un marco resiliente, así como la gestión de riesgos en el contexto cibernético.

La implementación de este modelo advierte que las empresas del sector logístico y transporte deben propender por mantener un esfuerzo sostenido para alcanzar un ciclo logístico resiliente o superar las mediciones óptimas de niveles de resiliencia propuestas, ya que cualquier limitación puede motivar efectos negativos que lleven a un ciclo logístico volátil o sensible y en el peor de los casos vulnerable.

Considerando los elementos generales del modelo propuesto, este puede ser adaptado y adoptado por empresas diferentes al sector logístico y transporte, dado que el contexto de ciclo logístico podría ser ajustado y alineado al quehacer principal de la empresa en la que se esté implementando, sin perder el resultado con los demás componentes que hacen parte del modelo, manteniendo su objetivo central: tener una empresa ciber resiliente.

Si bien, la aplicación del Modelo LCR se hace en para un caso en una empresa representativa del sector logístico y transporte terrestre en Colombia, y los resultados de su aplicación en otras organizaciones de este gremio puede variar por condiciones particulares de las empresas y la escasa normatividad disponible sobre el tema en este sector, el modelo se presenta como una oportunidad para continuar avanzando en la incorporación del concepto de ciber resiliencia en este entorno.

Referencias

Arati, P. 2020. “Cybersecurity for transport and logistic industry. Infosys”, https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf

Blackhurst, J., Dunn, K. S. y Craighead C. 2011. “An empirically derived framework of global supply resiliency,” Journal of Business Logistics, (32:4), pp. 374–391.

Cano J. 2017. “La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial,” Isaca, pp. 5.

Cheung K., Bell, M. G. H. y J. Bhattacharjya. 2021. “Cybersecurity in logistics and supply chain management: An overview and future research directions,”Transportation Research Part E: Logistics and Transportation Review, 146, 102217.

Christopher M., y Towill D. 2001. “An integrated model for the design of agile supply chains,” International Journal of Physical Distribution & Logistics Management, (31:4), pp. 235–246.

Christopher M., y Peck H. 2014. “Building the resilient supply chain,” The International Journal of Logistics Management, (15:2), pp. 1–14.

Contero S., y Martin J. 2020. “Manual OKR,” Singular People S.L.
Diaz R. 2021. “Estado de la ciberseguridad en la logística de américa latina y el caribe,” Serie Desarrollo Productivo, (228), pp. 68.
Linkov I., Eisenberg D.A., Plourde K., Seager T.P., Allen J., y Kott A. 2013. “Resilience metrics for cyber systems,” Environment Systems and Decisions, (33:4), pp. 471–476.
Khan O., Sepúlveda A., Estay D. 2015. “Supply chain cyber-resilience: Creating an agenda for future research,” Technology Innovation Management Review, (5:4), pp. 6–12.
Pettit T.J., Fiksel J. y Croxton K.L 2010. “Ensuring supply chain resilience: Development of a conceptual framework,” Journal of Business Logistics, (31:1), pp. 1–21.
Sheffi Y., y Rice J. 2005. “A supply chain view of the resilient Enterprise,” pp. 47.