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.*