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.

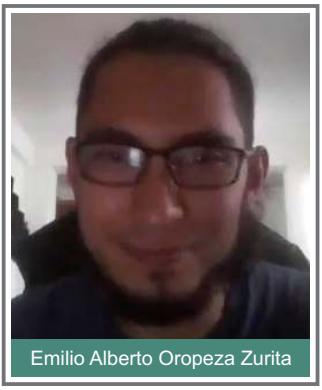
Juan Mario Posada Daza
Líder de Ciberseguridad
Accenture Colombia
A lo ya planteado podría agregar que en la cadena de suministro digital hay otros elementos como la adopción de nuevas tecnologías, la interoperabilidad y la interacción digital de los diferentes actores de la cadena, quienes, al automatizarse 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

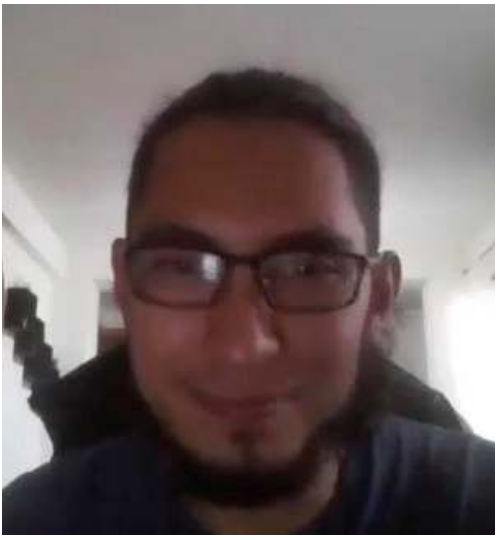

Liliana Patricia Quiñonez García


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.*