UNIVERSIDAD SIMÓN BOLÍVAR | INSTITUTO DE POSGRADOS

ANALISIS DE EVALUACION DE LOS RIESGOS EN LA RED EN LA COOPERATIVA DROGUERIA DETALLISTAS (COPIDROGA)*

Edilberto Payares Benítez
Jaime Junior Bahoquez Ruiz

Trabajo de Investigación o Tesis Doctoral como requisito para optar el título de especialización de gestión de tecnologías de la información

RESUMEN

El presente análisis de gestión de riesgo, tiene como objetivo exponer y evaluar los posibles riesgos en la red de comunicaciones de la cadena de suministros copidroga (cooperativa de droguistas detallistas) la cual se dedica a la comercialización y distribución de productos farmacéuticos y varios, enfocándolos en la vulnerabilidad cibernética o seguridad cibernética de su CS, a su vez identificar estrategias de mitigación y contingencia creando finalmente un caso de estudio de nos permita medir la resiliencia de acuerdo a los riesgos posteriormente establecidos.

Para contextualizar sobre una empresa cooperativa de droguistas detallistas, es una empresa asociativa de la economía solidaria, sin ánimo de lucro, que tiene como objetivo proteger y propender por el desarrollo empresarial y la dignificación del droguista detallista, para lo cual efectúa la distribución de bienes en las mejores condiciones de precio, calidad, surtido y abastecimiento que demandan los consumidores en los establecimientos de sus asociados, a los cuales les presta otros servicios complementarios con valor agregado y de alta calidad. En cumplimiento de su misión, esta cooperativa procura satisfacer las necesidades de carácter económico, personal y familiar de los asociados para mejorar su bienestar comercial, social y cultural, sobre la base de la ayuda mutua y de los demás principios y valores cooperativos, con una participación en los sectores solidario y de la salud, para que con su acción y la de sus afiliados se beneficie también la comunidad en general. (Información suministrada por la cooperativa, 1969).

Mediante la intensificación de la competencia, el rápido crecimiento de la tercerización y la globalización, las rápidas variaciones ambientales y tecnológicas, y al aumentar las expectativas de los clientes , las organizaciones se han enfrentado a numerosos desafíos e incertidumbres (Hofmann et al., 2014).

Una cadena de suministro funcione bien ayuda a mejorar el sistema de planificación, optimizar el inventario de almacén, realizar entregas a tiempo, garantizar la oferta a

la demanda de la conformidad, reducir costes y, como consecuencia, aumentar el valor de mercado de la compañía. Las tendencias actuales en el desarrollo de tecnologías de administración de la cadena de suministro son definidos por las enormes posibilidades de Internet. Las cadenas de fabricantes, proveedores, contratistas, empresas de transporte y el comercio están entrelazados de la manera más íntima y ya son las redes en línea reales. Las empresas se fusionan en la comunidad de negocios, y los límites entre ellos se encuentran desaparecidos. Sin embargo, hay una transparencia de las actividades conjuntas, los intérpretes pueden adaptarse rápidamente a las necesidades del cliente, así como de forma rápida llevar nuevos productos al mercado usando métodos avanzados de predicción y planificación. El Internet es el medio tecnológico más simple, más barato y más eficiente para gestionar y controlar las redes asociadas. Las empresas por lo general comienzan con la combinación de las actividades más simples que utilizan correos electrónicos y sistemas de automatización de flujo de trabajo, a continuación, pasar a soporte virtual de los procesos de negocios más importantes, y luego fusionar en una sola corporación virtual dentro del cual se sincroniza toda la red. Esto ya es una transición hacia el comercio electrónico mundial, cuando todas las transacciones comerciales y los pagos están dispuestos a través de la Web, sin excepción. Como resultado, no sólo aumenta significativamente la productividad, sino también todos los procesos acelerar significativamente que conducen a cualitativamente nuevos efectos. (Boiko et al., 2019).

Ahora bien, el riesgo cibernético es el factor que más está afectando a las organizaciones hoy en día, mientras más compleja se hace la Cadena de Suministro más propensa está de cambios turbulentos que afectan sus actividades diarias. En primer lugar, la infraestructura interconectada en la que se apoya el negocio global es intrínsecamente insegura y, en segundo lugar, la naturaleza humana y el ingenio son a la vez la mayor fortaleza y la mayor debilidad. Las cadenas de suministros dependen cada vez más de las tecnologías de la información y las comunicaciones (TIC), ya que une oficinas entre diferentes países en cada una de las organizaciones involucradas, dependiendo de las interacciones con múltiples partes interesadas y con aplicaciones creadas exclusivamente para su propio uso, donde los protocolos de seguridad pueden no estar alertas a las últimas y más recientes vulnerabilidades. La variedad del impacto es amplia, va desde el simple robo o fraude mediante el potencial de control o manipulación de sistemas o equipos, hasta la liberación de datos o la misma propiedad intelectual. (Club, 2017)

Objetivos

Objetivo general

Realizar un análisis de gestión de riesgo de la cadena de suministros copidroga (cooperativa de droguistas detallistas) con el fin de identificar las vulnerabilidades, amenazas y riesgos en la red y los sistemas de información.

Objetivos Específicos

- Identificar las falencias actuales de la red y relacionarla a los protocolos de diseño y planeación que encaminen a la mejora de la estructura de la empresa por medio de una matriz de riesgo donde se analicen las amenazas y debilidades del sistema.

- Sugerir mecanismos de control y gestión que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.

Materiales y Métodos:

La metodología utilizada fue la siguiente.

Metodología AMEF

Tomado delos sectores que apuestan alto como las industrias aeroespacial y defensa, el análisis de modo de defensa y efecto de fallos (amef) es un conjunto de directrices, un método y una forma de identificar problemas potenciales (errores) y sus posibles efecto en un sistema con el fin de priorizarlos y concentrar los recursos en planes de prevención y supervisión de respuestas.

Resultados

#	Riesgo	Descripción	Origen
R1	Falla en comunicaciones de la empresa que suministra la red	Caída en la red por fallas internas de la empresa que suministra el servicio, por temas de fibra óptica, cableado, infraestructura u otros.	Externo a CS
R2	Falla del backup en la empresa que suministra la red	Caída en la red por fallas internas de la empresa que suministra el servicio back up, por temas de fibra óptica, cableado, infraestructura u otros.	Externo a CS
R3	Caída del sistema desactualización en la versión de voice picking	La no actualización del software utilizado por la empresa puede tener afectación sobre el correcto funcionamiento de estos.	Interno
R4	Falla en aplicativo Return Pool	Falla en aplicativo para la trazabilidad y seguimiento en la distribución de las entregas o pedidos a los clientes.	Interno
R5	Falla en aplicativo Cedis Para almacenamiento	Falla en aplicativo para la trazabilidad y seguimiento en el almacenamiento de productos en las bodegas destinadas para tal fin.	Interno

R6	Falla del ERP SAP	Caída en el funcionamiento del ERP como tal por sobrecarga en el uso de transacciones o problemas de configuración de atributos y parámetros.	Interno
R7	Falla en el Internet inalámbrico	Caída en el funcionamiento de los acces point, por deficiencias en el equipo, falta de mantenimiento, obsolescencia, capacidad insuficiente, o mala ubicación.	Interno
R8	Falla en sistema Vocollet (Voice picking)	Caída en el sistema Vocollet por problemas en el sistema operativo por sobrecarga en el tráfico de información, por problemas en la configuración de atributos y parámetros.	Interno
R9	Ataques cibernéticos	Destrucción o vulnerabilidad de los sistemas de información a raíz de ataques con virus a través de descargas de sitios web poco confiables o correos con archivos dañinos adjuntos.	Externo a CS
R10	Falla en el servidor principal	Caída en todos los sistemas de información que dependen del servidor principal de la regional, a raíz de la falla en dicho servidor por falta de mantenimiento, problemas de configuración u obsolescencia de partes.	Interno
R11	Falla en la plataforma en la que los asociados realizan pedidos SIP.	Caída en el sistema SIP para generar pedidos desde las droguerías y por los vendedores, lo cual frenaría el flujo de los procesos en la cadena de suministros, ya que la demanda se estancaría.	Interno
R12	Fuga de información por dispositivos de empleados	Descarga y hurto de información confidencial y de gran valor para el funcionamiento de la cadena de suministro por dispositivos móviles o de almacenamiento portátil.	Interno
R13	Robo de información por hackeo del sistema	Manipulación de los sistemas de información por una persona externa, para hurto o destrucción de información de gran valor para la organización.	Externo a CS
R14	Falla en las redes de fibra óptica	Caída del internet y el tráfico de datos e información por desconexión de la fibra óptica por obsolescencia, falta de mantenimiento, mal empalme en conectores y en la llegada a los servidores.	Interno
R15	Fuga de información por correo electrónico	Envió de información confidencial y de gran valor para el funcionamiento de la cadena de suministro por correo electrónico corporativo.	Interno

Conclusiones

Como resultado de este proyecto se obtiene la evaluación del riesgo de los activos analizados en la Entidad, la evaluación de las salvaguardas actuales como controles para mitigar ese riesgo y la propuesta de nuevos controles en los activos para los cuales las salvaguardas existentes no son las más indicadas.

Aplicar la metodología AMEF para el análisis de riesgo es el primer paso para garantizar la seguridad de los activos de información y el normal funcionamiento interno de la entidad.

Los resultados muestran los riesgos identificados como modo de falla en red de comunicaciones de la cadena de suministro esta empresa cooperativa, el análisis su probabilidad de ocurrencia, de detención y la severidad, para priorizar los riesgos. Es así como realizando un análisis detallado basado en los resultados pertinentes a esta investigación, teniendo en cuenta la información real suministrada por una cooperativa de droguistas, se deduce que las interrupciones no planificadas en la red de comunicaciones son la causa principal de interrupción en el funcionamiento de sistema logístico de su cadena de suministro, teniendo a ataques cibernéticos en segundo lugar de acuerdo al informe de la Resiliencia en la Cadena de Suministro. Partiendo de lo anterior, el siguiente paso basado en el análisis es adoptar estrategias para la prevención y mitigación de dichos riesgos, para fortalecer la cadena de suministro que pueda soportar amenazas en la red de comunicaciones. La estrategia robusta es manejar los pequeños riesgos antes del evento y manejar las fluctuaciones regulares, como algunos impactos bajos con ocurrencia de alta probabilidad. La estrategia de resiliencia ayuda a las organizaciones a adaptar, improvisar y superar aquellas perturbaciones e interrupciones que se le presente y en general a las cadenas de suministro a sobrevivir después de estar expuesto a grandes riesgos y sufrir grandes cambios como consecuencias de eventos no deseados.
La matriz de relación fue la herramienta utilizada y bajo la cual se estableció la priorización de los riesgos, también suministro el orden o jerarquización de las medidas de mitigación de más impacto: disponibilidad de un soporte especializado de expertos en los sistemas específicos, que solucionen los inconvenientes que se puedan presentar en el menor tiempo y contar con departamento de sistemas para vigilancia permanente en la red con herramientas de control, y barreras como antivirus y sitios web restringidos, puertos USB bloqueados y firewall actualizados, y tener varios proveedores de internet, tener redundancia para contar con un sistema robusto y un backup confiable, resultan ser las más determinantes para fortalecer la resiliencia en la cadena de suministro desde la óptica de redes de comunicación en la cooperativa de droguistas utilizada para la investigación.

Palabras clave: Cadena de suministro, riesgo cibernético, fallas en la red de comunicaciones, logística, resiliencia.

ABSTRACT

All objective

Perform a risk management analysis of the co-supply supply chain (cooperative of retail drug dealers) in order to identify vulnerabilities, threats and risks in the network and information systems.

Specific objectives

- Identify the current shortcomings of the network and relate it to the design and planning protocols that lead to the improvement of the structure of the company through a risk matrix where the threats and weaknesses of the system are analyzed.

- Requires control and management mechanisms that minimize the vulnerabilities found in the study of the risk analysis performed.

Materials and Methods:

The methodology used was as follows. AMEF methodology Taken from the high-betting sectors such as the aerospace and defense industries, the defense mode and fault effect (amef) analysis is a set of guidelines, a method and a way to identify specific problems (errors) and their possible effects on a system in order to prioritize them and concentrate resources on prevention and response monitoring plans.

Conclusions

As a result of this project, the risk assessment of the assets analyzed in the Entity is obtained, the evaluation of current safeguards as controls to mitigate that risk and the proposal of new controls on the assets for which existing safeguards are not the most indicated.

Applying the AMEF methodology for risk analysis is the first step to guarantee the security of information assets and the normal internal functioning of the entity.

The results show the risks identified as a mode of failure in the supply chain communications network of this cooperative company, the analysis of its probability of occurrence, of detention and severity, to prioritize the risks. Thus, by carrying out a detailed analysis based on the results pertinent to this investigation, taking into account the real information provided by a drug cooperative, it is deduced that unplanned interruptions in the communications network are the main cause of interruption in operation. logistics system of its supply chain, having cyber attacks in second place according to the report of the Resilience in the Supply Chain. Based

on the above, the next step based on the analysis is to adopt strategies for the prevention and mitigation of these risks, to strengthen the supply chain that can withstand threats in the communications network. The robust strategy is to manage small risks before the event and handle regular fluctuations, such as some low impacts with a high probability occurrence. The resilience strategy helps organizations to adapt, improvise and overcome those disturbances and interruptions that arise and in general supply chains to survive after being exposed to great risks and undergo major changes as a consequence of unwanted events.
The relationship matrix was the tool used and under which the prioritization of risks was established, it also provided the order or hierarchy of the most impact mitigation measures: availability of specialized support from experts in specific systems, to solve the inconveniences that may occur in the shortest time and have a system department for permanent surveillance in the network with control tools, and barriers such as antivirus and restricted websites, blocked USB ports and updated firewall, and have several internet providers, have redundancy to have a robust system and a reliable backup, prove to be the most decisive to strengthen the resilience in the supply chain from the perspective of communication networks in the drug cooperative used for research.

KeyWords: Supply chain, cyber risk, communications network failures, logistics, resilience.

REFERENCIAS

Cert-Uk. (2015). *Cyber-security risks in the Supply Chain*. Obtenido de CERT-UK PUBLICATION: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf

Club, T. (14 de Agosto de 2017). *Considerando el riesgo cibernético de la cadena de suministro*. Obtenido de http://rm-forwarding.com/2017/08/14/considerar-riesgo-cibernetico-la-cadena-suministro/

Insurance, O. P. (May de 2013). *Managing Cyber Supply Chain Risks*. Obtenido de Advisen Insurance Intelligence: http://www.advisenltd.com/wp-content/uploads/2013_OBPI_SupplyChainCyberRM_Whitepaper.pdf

Sam Jenks, K. R. (16 de Agosto de 2017). *The Cyber Security of Supply Chains: Who's the real risk, Man or Machine?* Obtenido de Medium Corporation: https://medium.com/@KodiakRating/the-cyber-security-of-supply-chains-whos-the-real-risk-man-or-machine-ecdcc365d49d

Verizon. (2014). *Data Breach Investigation Report*. Obtenido de Verizon: https://enterprise.verizon.com/resources/reports/dbir/

Weimar A. Ardila, D. H. (Julio de 2014). *Estrategias para la Gestión de Riesgos en la Cadena de Suministros*. Obtenido de LACCEI Latin American and Caribbean Conference for Engineering and Technology : http://www.laccei.org/LACCEI2014-Guayaquil/RefereedPapers/RP233.pdf

Zurich. (2017). *BCI Supply Chain Resilience 2017*. Obtenido de https://www.zurich.co.uk/_/media/dbe/united-kingdom/docs/business/corporate-and-multinational/bci_resilience_report_2017.pdf?la=en&hash=FE670D95113865B41282FB268002E1A78A9D9B3E