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

Edilberto Payares Benítez *
Jaime Junior Bahoquez Ruiz **

UNIVERSIDAD SIMÓN BOLÍVAR

*Ingeniero Sistema, Universidad autónoma del caribe, Colombia. Estudiante, Especialización en Gestión de tecnología y la información de la Universidad Simón Bolívar, Colombia.
Correo electrónico: ing.edilbertopb@gmail.com
**Ingeniero Sistema, Universidad Simón Bolívar, Colombia. Estudiante, Especialización en Gestión de tecnología y la información de la Universidad Simón Bolívar, Colombia.
Correo electrónico: jbahoquez@gmail.com

CONTENIDO

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

Análisis de evaluación de los riesgos en la red en la cooperativa droguería detallistas (copidroga) *

Analysis of assessment of risks on the network in the drogueria details cooperative (copidroga)

RESUMEN

Este análisis de gestión de riesgo tiene propósito exponer y evaluar los posibles riesgos en la red de comunicaciones de la empresa copidroga, el cual se explora la gestión del riesgo del modo de falla en la red de comunicaciones en la cadena de suministros de la empresa copidroga (cooperativa de droguistas detallistas) afectaría la resiliencia en ella. Se identifica, analiza y evalúan diez riesgos con modo de falla en la red de comunicaciones, se propone estrategias de mitigación y contingencias. Pasando por una matriz de relación se priorizan las estrategias para su ejecución y se realiza un caso de estudio de medición de la resiliencia. Así, la gestión del riesgo contribuiría al aumento de la resiliencia de la cadena de suministro.

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

ABSTRACT

This risk management analysis is intended to expose and evaluate the possible risks in the company's communications network, which explores the risk management of the failure mode in the communications network in the company's supply chain. of retailers would affect the resilience in it. Ten risks are identified, analyzed and evaluated as a failure in the communications network, mitigation strategies and contingencies are proposed. Going through a relationship matrix, the strategies for its execution are prioritized and a case study of resilience measurement is carried out. Thus, risk management would contribute to increasing the resilience of the supply chain.

Keywords: Supply chain, cyber risk, communications network, logistics, and resilience.

1. INTRODUCION

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 activa 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)

2. PROBLEMA

2.1. Descripción

El caso de estudio manifiesta la urgente necesidad de proteger su activo más valioso "la información" y esto se ve agravado con el constante incremento de la información en la entidad como también de los sistemas de información que son necesarios para la gestión de información en sus diferentes centros de servicio. Como también manifiesta la preocupación de haber sido objetivo de ataques de interceptación a la información confidencial en sus sistemas de información y recalca la gran importancia que tiene para la Entidad velar por la seguridad de sus Sistemas de Información.

Se evidencia que no existen procedimientos definidos de seguridad de la información como tampoco existen controles y políticas de contingencia que permitan mitigar un posible evento negativo y continuidad del negocio (caída del sistema SAP).

Desde el punto de vista de la Entidad que maneja los datos, existen amenazas de origen externo, como las agresiones técnicas (cibercriminales), naturales o humanas y de origen interno por la negligencia del propio personal o fallas en las condiciones técnicas de procesos operativos internos.

De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de riesgos; muy seguramente en un futuro cercano podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros.

Con base a la problemática planteada, es importante realizar esta investigación ya que la información es uno de los activos más valiosos en las organizaciones y de ella depende tanto los procesos internos como externos de negocio. Por ello es importante el aseguramiento de la misma haciendo uso de mecanismos y herramientas que ayuden a resguardar la información ya que en caso de caer en manos incorrectas podía ocasionar daños a la imagen y credibilidad.

2.2. Formulación del Problema

¿Cómo identificar y tratar los riesgos que afecten la seguridad de la información y la red de comunicación de la cadena de suministros copidroga (cooperativa de droguistas detallistas), con el fin de definir e implementar a futuro un Sistema de Gestión de Seguridad de la Información y mejora en la red (TIC), mediante el análisis de riesgos?

3. OBJETIVOS

3.1. Objetivos generales

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.

3.2. 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.

4. TRABAJOS RELACIONADOS

4.1. Resiliencia y gestión del riesgo en la cadena de suministros.

Se dice que una cadena de suministro es más resiliente cuando ésta tiene la capacidad de absorber cualquier impacto negativo del entorno que la rodea generando una catástrofe, mitigan el riesgo adaptándose, creciendo y emergiendo con más firmeza en caso de enfrentar demás eventos disruptivos. Entendiendo el riesgo como la probabilidad de ocurrencia de un evento inesperado

generando impactos negativos o positivos que implique una amenaza potencial en el desempeño de las operaciones de una organización.

Hoy en día las organizaciones se están viendo vulnerables a diferentes tipos de riesgos que estas puedan enfrentar, normalmente son las grandes empresas quienes atienden o gestionan el riesgo en su cadena de suministro. Debido a los grandes avances tecnológicos y de globalización las grandes empresas son las más expuestas a los riesgos del entorno. Según Sheffi (2005) propone que la atención de la Gestión de Riesgos en la Cadena de Suministro, más que determinar los factores de riesgo, debe emprender un análisis de los posibles modos de falla del sistema una vez sea afectado por un evento disruptivo, así:

Tabla 1.
Definición de los modos de fallas.

	MODOS DE FALLAS
Falla en el suministro	Se da cuando ocurre una interrupción de las actividades relacionadas con el suministro, como retrasos o indisponibilidad de materiales de proveedores. Conduciendo a una escasez de las entradas que podrían paralizar la actividad de la empresa.
Falla en la demanda	Puede verse reflejado en el retraso o la interrupción de la demanda, temporal o permanente que conduce a la pérdida de la demanda.
Falla en el transporte	Se presenta una falla en el transporte cuando existe un retraso en la infraestructura de transporte, conduciendo a la imposibilidad para transportar el producto o servicio.
Falla en las instalaciones	Indisponibilidad de plantas, depósitos y edificios de oficina; si se presenta obstaculizaría la capacidad de seguir realizando las operaciones.
Falla en la red de comunicaciones	Se percibe en el retraso o la indisponibilidad de la información y la infraestructura de comunicación, dentro o fuera de empresa, que conduce a la inhabilidad de coordinar operaciones y ejecutar transacciones.
Violaciones de la carga	Se presentan problemas de violación de la integridad de la carga y productos. Conduce a la pérdida o adulteración de bienes (p.e. contrabando de armas dentro de contenedores)

Fuente: Elaboración de los autores.

Las diversas estrategias propuestas por la literatura para prevenir y/o mitigar el impacto de un evento que pueda afectar las operaciones de la Cadena de suministros en cualquiera de los modos

anteriormente descritos, están esbozadas en tres enfoques distintos. El primero hace referencia al diseño de Cadenas Suministros robustas, capaces de soportar el impacto de pequeñas disrupciones asociadas con la variabilidad del entorno, sin que su desempeño se vea afectado. Un segundo enfoque trata sobre el análisis y mediación de confiabilidad de la cadena de suministros, el cual permite determinar la probabilidad de falla de la Cadena bajo condiciones normales de operación. Por último, el tercer enfoque busca implementar mecanismos que hagan de la cadena de suministros un sistema resiliente, es decir, que no solo sea capaz de soportar las perturbaciones del entorno, sino que a su vez sea capaz de reponerse de manera ágil ante cualquier evento inesperado con la capacidad de afectar notablemente desempeño de esta. (Weimar A. Ardila, 2014)

Para Melnyk, S. (2014), la resistencia de la cadena de suministro es "la capacidad de una cadena de suministro tanto para resistir las interrupciones como para recuperar la capacidad operativa después de que se producen las interrupciones". Como se mencionó anteriormente, vista desde esta perspectiva, la resistencia consiste en dos componentes críticos pero complementarios del sistema: la capacidad de la resistencia y la capacidad de recuperación. La capacidad de resistencia es la capacidad de un sistema para minimizar el impacto de una interrupción evitándola por completo (evitación) o minimizando el tiempo entre el inicio de la interrupción y el inicio de la recuperación de esa interrupción (contención); La capacidad de recuperación es la capacidad de un sistema para volver a la funcionalidad una vez que se ha producido una interrupción. El proceso de recuperación del sistema se caracteriza por una fase de estabilización (con suerte breve) después de la cual se puede lograr un retorno a un estado estable de rendimiento. El rendimiento final alcanzado en estado estable puede o no volver a adquirir niveles de rendimiento originales, y depende de muchos factores de interrupción y competencia.

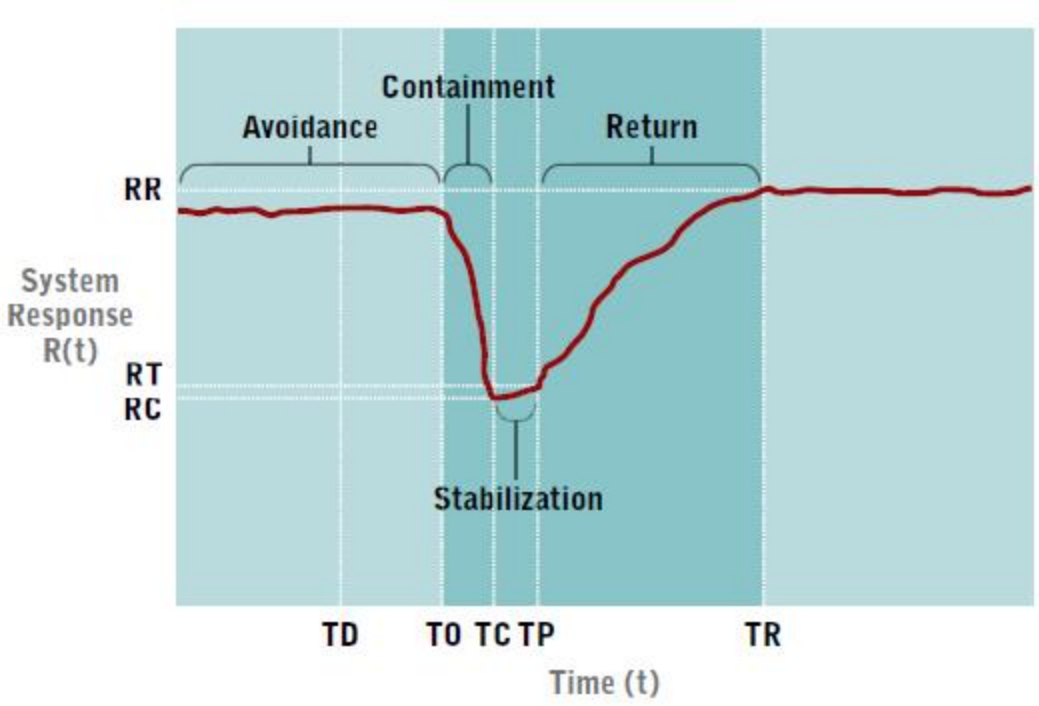

Figura 1. Visualización en el tiempo del factor de resiliencia en la cadena de suministro.
Fuente: Universidad del estado de Michigan.

La figura 1 muestra el impacto de una interrupción en el tiempo, desde el momento en que la interrupción se origina en algún lugar del sistema (en el momento TD) hasta que el sistema ha regresado a alguna forma de estado estable (TR).

En la figura 1, podemos identificar las cuatro etapas de la resiliencia, que son la evitación, la contención, la estabilización y el retorno. Cuando se observan interrupciones en la cadena de suministro y sus características, es interesante comparar cómo las políticas y estrategias utilizadas por la empresa pueden afectar los diversos eventos identificados en la figura 1.

Una vez que se completa la recuperación, las empresas a menudo reflexionan sobre su experiencia para documentar las lecciones apropiadas e identificar mejoras en el sistema para reducir los riesgos futuros. Esto completa un ciclo de resiliencia en la cadena de suministro de: Evitación → Contención → Estabilización → Retorno → Revisión Evitación.

De acuerdo a los resultados del informe de la Resiliencia en la Cadena de Suministro BCI de Zurich (2017), tenemos que las principales causas de los riesgos que contemplan los sistemas de

la cadena de suministro se encuentran: Las interrupciones no planificadas de TI o de telecomunicaciones, los ataques cibernéticos y violaciones de datos, y la pérdida de talento / habilidades. Al mismo tiempo, una vez identificado el posible riesgo pueden asociarse consecuencias que impactan al sistema, por ejemplo, la pérdida de productividad puede generar pérdidas de ingreso, el aumento del costo de trabajo; conduce a numerosos reprocesos o bien llamado procesos de reingeniería y las quejas de los clientes; conduce a la mala reputación de la marca. De un solo incidente en las organizaciones, se pueden generar múltiples consecuencias, por lo cual es de vital importancia atender a tiempo los riesgos a los que se están expuestos.

4.2. Riesgo cibernético.

El término “riesgo cibernético” se refiere a una multitud de diferentes fuentes de riesgo que afectan a los activos de información y tecnología de una empresa. Algunos ejemplos destacados de riesgo cibernético son el robo de identidad, la divulgación de información sensible, y la interrupción del negocio. Se han hecho muchos intentos para definir “riesgo cibernético”. Algunas de ellas emplean conceptos bastante estrechos; por ejemplo, Mukhopadhyay et al. se refieren a los riesgos cibernéticos como el riesgo que suponen los eventos electrónicos maliciosos que causa la interrupción del negocio y pérdidas monetarias. Otros toman una perspectiva más amplia al definirlo como el riesgo de seguridad de la información o el riesgo que resulta en fallo de los sistemas de información. El término “cibernética” es la abreviatura de la palabra ciberespacio, que generalmente se entiende como el dominio interactivo compuesta de todas las redes digitales utilizados para almacenar, modificar y comunicar información. Incluye todos los sistemas de información utilizados para apoyar a las empresas, la infraestructura y los servicios

En la actualidad muchas organizaciones, se ven afectadas por los ataques cibernéticos, por lo cual luchan por proteger la confidencialidad, la disponibilidad y la integridad de sus redes y sistemas en un panorama de amenazas cibernéticas en rápida evolución. Los servicios complejos de tecnología de la información y la comunicación (TIC) y el soporte, a menudo se subcontratan en un intento de reducir los costos de infraestructura o simplificar las organizaciones. Se entiende por "vulnerabilidad cibernética" una dependencia de las TIC desconocida o no mitigada. (Cert-Uk, 2015). Casi todas las organizaciones experimentan problemas debido a fallas en el funcionamiento

del software o hardware, pero generalmente estos eventos no generan un gran inconveniente, aunque tienen el potencial de ser catastróficos. Sin embargo, las amenazas cibernéticas deliberadas pueden llegar a la organización a través de cualquier número de puntos vulnerables a lo largo de la cadena de suministro.

En cuanto a la gestión de los riesgos de la cadena de suministro, las organizaciones modernas siguen estableciendo procedimientos para mitigar dependencias y vulnerabilidades que podrían afectar sus cadenas de suministro. Estos riesgos al ser detectados hacen que las organizaciones aumenten su visibilidad y permite a estas anticipar su impacto. Sin embargo, este enfoque rara vez se identifica cuando se trata de riesgos relacionados con la seguridad cibernética, porque estos riesgos son los más ocultos, ya que se eliminan varios pasos del centro de análisis y toma de decisiones de una organización determinada. Como resultado, son desplazados fuera del control de una organización y, por lo tanto, una organización puede encontrar que, a pesar de las fuertes medidas de seguridad cibernética que ha implementado a través de su sistema de TIC, ha sido víctima de ataques deliberados o daños colaterales. (Insurance, 2013)

Siguiendo la idea, con la información y los acuerdos de seguridad compartidos en una cadena de suministro, la seguridad cibernética de cualquier organización dentro de la cadena es potencialmente tan fuerte como la del miembro más débil de la cadena de suministro. Un agresor determinado, especialmente las amenazas persistentes avanzadas (APT), utilizará esto identificando a la organización con la seguridad cibernética más débil dentro de la cadena de suministro, y utilizando estas vulnerabilidades presentes en sus sistemas para obtener acceso a otros miembros de la cadena de suministro. Si bien no siempre es el caso, a menudo son las organizaciones más pequeñas dentro de una cadena de suministro las que, debido a recursos más limitados, tienen los acuerdos de seguridad cibernética más débiles. Las pequeñas organizaciones representaron el 92% del número total de incidentes cibernéticos analizados en el Informe de investigación de violación de datos (Verizon, 2014). A menudo son objetivo porque son más vulnerables, representan un punto único de falla o tienen acceso desproporcionado a información importante dado su tamaño dentro de una cadena de suministro, esto plantea un riesgo particular para las grandes empresas de las que dependen.

Para abordar los riesgos de la cadena de suministro relacionados con la tecnología, las organizaciones deben implementar estrategias para tratar de manera activa y preventiva la seguridad cibernética en toda la cadena de valor. Por otro lado, la seguridad cibernética de la cadena de suministro de una organización no depende únicamente de la prevención de infracciones de sistemas basados en máquinas, fallos o ataques cibernéticos, cuantas más personas participan en el proceso de actividades de la cadena de suministro mejoradas digitalmente, más se ha abierto el sistema cibernético a los posibles riesgos de la seguridad cibernética. No solo son los equipos de administración internos de la cadena de suministro interna, sino también, sus proveedores, fabricantes, reparto de mercancía, minoristas, comerciantes, entre otros; lo cual hace aún más vulnerable y compleja la cadena de suministro, con diferentes orígenes, diferentes niveles de habilidad tecnológica y diferentes competencias generando mayor accesibilidad en la red de comunicaciones (Sam Jenks, 2017). Aunque la habilidad de ser colaborativos en la cadena de suministro es esencial para tener visibilidad y agilidad, cabe citar la siguiente frase "Compartir información con los proveedores es esencial, pero aumenta el riesgo de que esa información se vea comprometida" (Bowman, 2013), por lo cual las organizaciones deben estratificar la información a compartir.

Los riesgos claves de la cadena de suministro Cibernética, según lo establecido por el NIST son:

- Proveedores o proveedores de servicios de terceros, desde servicios de limpieza hasta ingeniería de software, con acceso físico o virtual a sistemas de información, código de software o IP.
- Las malas prácticas de seguridad de la información de los proveedores de nivel inferior.
- Software o hardware comprometido comprado a los proveedores.
- Vulnerabilidades de seguridad del software en la gestión de la cadena de suministro o sistemas de proveedores.
- Falsificar hardware con malware incrustado.
- Almacenamiento de datos de terceros o agregadores de datos (NIST).

Tabla 2
Riesgos Cibernéticos en la Cadena de Suministro.

WHAT DOES SUPPLY CHAIN HAVE TO DO WITH CYBER RISKS?	
80%	De todas las infracciones de información se originan en la cadena de suministro.
45%	De todas las violaciones cibernéticas se atribuyeron a socios anteriores.
72%	De las empresas no tienen plena visibilidad en sus cadenas de suministro.
59%	De las empresas no cuenta con un proceso para evaluar la ciber-seguridad de terceros proveedores con los que comparten datos o redes.
40%	De las campañas de ataque se dirigieron a los sectores de fabricación y servicios (20% cada uno).

Fuente: NIST RSA Conference 2016.

Por lo anterior, se demuestra que la visualización "riesgos claves de la cadena de suministro cibernética", depende igualmente de la forma en que cada una de las partes utilicen las plataformas tecnológicas en cuanto a la seguridad de la tecnología en sí. Además, indica cuán flexibles pueden ser los atacantes en sus ataques. Esto tiene serias implicaciones para las organizaciones que buscan mejorar la gestión de riesgos de su cadena de suministro. Si bien existen múltiples soluciones técnicas y una serie de estándares comunes que pueden ayudar a mitigar estos riesgos, mejorar las relaciones entre los miembros de la cadena de suministro también es muy importante para mejorar la seguridad cibernética dentro de ella.

Los productos y servicios basados en ciberseguridad se adquieren a través de cadenas de suministro que generalmente involucran a numerosos proveedores de componentes y servicios de hardware, firmware y software de origen global (Boyson et al., 2016). Cuando los objetivos de adquisición y sus requisitos no se definen y gestionan rigurosamente, los productos y servicios basados en ciberseguridad pueden presentar riesgos operativos para las organizaciones de usuarios finales y posiblemente para la sociedad si la seguridad , la fiabilidad y / o la seguridad se ven comprometidas. (Windelberg et al., 2016).

5. Análisis y resultados

La tabla 3 contiene 15 riegos de modo de falla en la red de comunicaciones que se han presentado o podrían presentarse en la cadena de suministro de una cooperativa que distribuye productos farmacéuticos, de aseo, dispositivos médicos y en general todo lo que se vende en una droguería, con su respectiva descripción y el origen del riesgo si son internos (dentro de la organización), externos dentro de la cadena de suministro o externos fuera de la cadena de suministro.

Tabla 3
Identificación de riesgo.

#	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

Continúa ⟶

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

Fuente: Elaboración de los autores.

Con el fin de analizar las consecuencias de los riesgos ya identificados, la tabla 4 provee detalles sobre el modo de la falla y el RPN que es el número Prioritario de Riesgo y se calcula como el producto de tres calificaciones cuantitativas, relacionadas cada una a los efectos, causas y controles:

$$Severidad\ x\ Ocurrencia\ x\ Detención = RPN \qquad (1)$$

Donde severidad es la estimación de la gravedad del efecto del modo de falla; ocurrencia es la probabilidad de que una causa específica, resulte en un modo de falla; y detección es un valor para clasificar la probabilidad de encontrar la falla antes de que ocurra; se evalúan del 1 al 10, con lo cual RPN puede tener un valor entre 1 a 1000.

Tabla 4

Tabla de referencia para asignar valor a la severidad:

Calificación		Criterio	
Cuantitativa	**Cualitativa**	**Efecto en el cliente**	**Efecto en el proceso**
1	Ninguno	Sin efecto perceptible	Ligero inconveniente para la operación u operador
2	Muy menor	No se cumple con el ajuste, acabados o presenta ruidos. Defecto notado por clientes críticos (25%)	Una parte del producto puede tener que ser procesado. Sin desechos
3	Menor	No se cumple con el ajuste, acabados o presenta ruidos. Defecto notado por el 50% de los clientes	Una parte del producto puede tener que ser procesado. Sin desechos
4	Muy bajo	No se cumple con el ajuste, acabados o presenta ruidos. Defecto notado por el 75% de los clientes	El producto debe ser seleccionado y una parte reprocesada. Sin desechos
5	Bajo	Producto con especificaciones de calidad o niveles de desempeño bajos. Operable o usable.	100% del producto puede tener que ser desechado sin selección o reparado con un tiempo y costo alto
6	Moderado	Producto operable o usable pero el cliente estará insatisfecho	Una parte del producto puede tener que ser desechado sin selección o reparado con un tiempo y costo alto
7	Alto	Producto operable o usable pero el cliente estará insatisfecho	El producto tiene que ser seleccionado y una parte reparada con un tiempo y costo alto
8	Muy alto	El producto es inoperable o inusable	El 100% del producto debe ser desechado o puede ser reparado a un costo inviable
9 - 10	Peligroso	En modo potencial afecta la operación segura del producto y/o involucra un no cumplimiento con alguna regulación gubernamental	Puede exponer al peligro operador o al equipo

Fuente: ingenieríaindustrialonline.com

Tabla 5

Tabla de referencia para asignar valor a la ocurrencia:

Calificación	
Cuantitativa	**Probabilidad**
1	Remota: Falla improbable
2 3	Baja: Pocas fallas
4 5 6	Moderada: Fallas ocasionales
7 8	Alta: Fallas frecuentes
9 10	Muy alta: Fallas persistentes

Fuente: Fuente: ingenieríaindustrialonline.com

Tabla 6

Tabla de referencia para asignar valor a la detección:

Calificación	
Cuantitativa	**Criterio**
1	Controles seguros para detectar: El ítem ha pasado prueba de errores. Es casi improbable el hecho de realizar partes conformes
2	Controles casi seguros para detectar: El ítem ha pasado por medición automática. No puede pasar la parte no conforme
3	Controles con buena oportunidad de detectar: Detección inmediata del error de la estación o en la estación siguiente. No pasa la unidad no conforme
4	Controles con buena oportunidad de detectar: Detección del error en la estación siguiente. No pasa la unidad no conforme
5	Controles que pueden detectar: Mediciones "pasa" o "no pasa" realizando el 100% de las partes despues de la estación
6	Controles que pueden detectar: Control en menos del 100% de las partes; puede estar apoyado en métodos estadísticos
7	Controles con poca oportunidad de detectar: Control logrado con doble inspección visual

8	Controles con poca oportunidad de detectar: Control efectuado con una inspección visual
9	Controles que probablemente no detectarán: Control logrado con verificaciones indirectas o al azar
10	Certeza absoluta de no detección: No se controla, no se detecta

Fuente: ingenieríaindustrialonline.com

Tabla 7
Matriz de evaluación de riesgo.

#	Consecuencia	Severidad	Ocurrencia	Detección	RPN
R1	Incremento en costos/Incumplimiento a clientes	7	4	6	168
R2	Incremento en costos/Incumplimiento a clientes	7	3	6	126
R3	Incremento en costos/Incumplimiento a clientes	6	2	2	24
R4	Incremento en costos/Incumplimiento a clientes	6	4	7	168
R5	Incremento en costos/Incumplimiento a clientes	6	4	7	168
R6	Incremento en costos/Incumplimiento a clientes	7	4	7	196
R7	Incremento en costos/Incumplimiento a clientes	5	5	7	175
R8	Incremento en costos/Incumplimiento a clientes	7	3	8	168
R9	Pérdida de clientes/Afectación Imagen corporativa	10	2	8	160
R10	Incremento en costos/Incumplimiento a clientes	6	3	8	144
R11	Pérdida de ingresos	6	3	8	144
R12	Incremento en costos/Incumplimiento clientes	7	2	9	126
R13	Pérdida de clientes/Afectación Imagen corporativa	9	2	7	126
R14	Incremento en costos/Incumplimiento a clientes	8	1	9	72
R15	Pérdida de clientes	8	3	3	72

Fuente: Elaboración de los autores.

La tabla 8 muestra las estrategias de mitigación y contingencia para controlar los riesgos.

Tabla 8
Matriz de estrategias de mitigación y contingencia.

#	Estrategias de mitigación y contingencia
M1	Tener disponible un soporte especializado de expertos en los sistemas específicos, que solucionen los inconvenientes que se puedan presentar en el menor tiempo.
M2	Tener un data center subcontratado que asegura la disponibilidad de la información en servidores alternos como backup ante la falla de los servidores actuales en un 99,7%.
M3	Tener varios proveedores de internet, tener redundancia para contar con un sistema robusto y un backup confiable.
M4	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.
M5	Contar con vendedores en un call center que toman los pedidos vía telefónica cuando se caiga el sistema.
M6	Conexiones inalámbricas y por UTP.

Fuente: Elaboración de los autores.

La tabla 9 muestra la interacción entre los riesgos y las estrategias de mitigación y contingencia, donde (1) significa que la estrategia de mitigación sirve de control para ese riesgo, y (0) que no aplica la estrategia para el riesgo y por último se tiene el total para identificar cuáles son las estrategias que debe priorizar la organización para controlar los riesgos. Para este caso la empresa del sector farmacéutico debe priorizar las estrategias M1 y M4 las cuales tienen mayor valor 1018 y 628 respectivamente; y de acuerdo a la tabla 5 la descripción de estas estrategias son, M1: tener disponible un soporte especializado de expertos en los sistemas específicos, que solucionen los inconvenientes que se puedan presentar en el menor tiempo y M4: 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..

Tabla 9
Matriz de Relación.

	Riesgos																
Estrategias de mitigación y contingencia	**R 1**	**R 2**	**R 3**	**R 4**	**R 5**	**R 6**	**R 7**	**R 8**	**R 9**	**R 10**	**R 11**	**R 12**	**R 13**	**R 14**	**R 15**	**Total**	**Priorización**
M1	1	1	1	1	1	1	0	1	0	0	0	0	0	0	0	1018	1
M2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	144	4
M3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	175	3
M4	0	0	0	0	0	0	0	0	1	0	1	1	1	0	1	628	2
M5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	144	5
M6	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	72	6

Fuente: Elaboración de los autores.

6. CONCLUSIONES Y RECOMENDACIONES.

6.1. 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 mas 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.

6.2. Recomendaciones

- Conexiones inalámbricas y por UTP: Se recomienda tener conexiones por clave utp para que estas sean más estables.
- Se recomienda contratar a un proveedor de servicios de internet adicional que funcione como contingencia cuando falle uno.
- Se recomienda tener un data center de contingencia que se encuentre en un lugar

diferente a la empresa para que en caso dado falle el principal este siga funcionando y no se afecten las actividades en la compañia

- Se recomienda realizar la socialización “análisis de riesgos de la red y la seguridad de la información para la cadena de suministros una cooperativa de droguistas detallistas" para aprobar o mejorar la ejecución de los controles propuestos al interior de la Copidroga.

- Se recomienda evaluar y aprobar las políticas generadas dentro de este proyecto.

- Se recomienda poner en funcionamiento los nuevos controles de seguridad que resultaron del análisis a la mayor brevedad.

- Se recomienda incluir dentro de las tareas del equipo de TIC auditorias permanentes a los activos de información para actualizar controles y contribuir con el desarrollo de mejores prácticas relacionadas con la seguridad de la información.

- Se recomienda fortalecer la política de seguridad que maneja la compañía realizando ajustes enfocados a los objetivos de negocio.

- Se recomienda reforzar las medidas de control de acceso físico para ingreso al centro de datos, colocando un sistema biométrico y llevando un control de los empleados autorizados.

- Se recomienda que existan conexiones independientes para los equipos de cómputo; este cuidado se debe tener en las oficinas donde estén conectadas terminales o microcomputadoras.

- Se recomienda que realicen el Análisis de Riesgos de los sistemas de comunicación (activos de red), por lo menos dos veces al año, para así conocer sus fortalezas o debilidades e implementar salvaguardas para reducir las debilidades encontradas.

- Actualizar el sistema operativo y aplicaciones: se recomienda siempre mantener actualizados los últimos parches de seguridad y software del sistema operativo para evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

- Utilizar contraseñas fuertes: Se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud no menor a los 8 caracteres.

- No permitir que personas ajenas usen sus equipos: Se recomienda que las visitas no deben tocar los equipos en la compañía. Es preciso supervisar que personas sin autorización los utilicen.

- Comprobar la procedencia de los correos electrónicos: Una forma muy común de realizar un ataque cibernético a una empresa grande es solicitarle información vía correo electrónico. Muchas veces los integrantes de las grandes compañías no toman precauciones y responden a correos electrónicos desconocidos. Hacerlo es confirmar que la dirección de correo está activa, lo que da pie a que el ataque avance. En las grandes empresas se debe confirmar la identidad de quien envía el correo electrónico siempre que sea posible. Además de contar con controles que permitan evitar los ataques directos utilizando esta herramienta esencial.

- Esté alerta del tráfico anormal: Se recomienda recolectar datos para establecer el comportamiento anormal de la red: protocolos, aplicaciones o actividad de los usuarios. Preste atención al volumen del tráfico y a los cambios inesperados en el uso del protocolo.

7. Bibliografía

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