



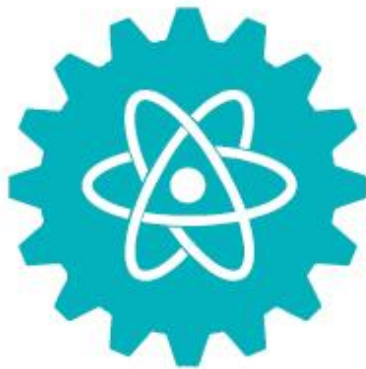
UNIVERSIDAD
DE LA GUAJIRA

SHIKII EKIRAJIA
PÜLEE WAJIIRA

Vigilado Mineducación

Enero 2023
Junio

e-ISSN 2389-9484



Ciencia^e Ingeniería

Revista Interdisciplinaria de Estudios en
Ciencias Básicas e Ingenierías

Edición 1 | Volumen 10

Ciencia e Ingeniería

Revista Interdisciplinaria de Estudios en
Ciencias Básicas e Ingenierías
ISSN 2389-9484

Año 2021, enero-junio, Vol. 10, N.º 1, e8091879

Facultades de Ciencias Básicas y Aplicadas e
Ingeniería. Universidad de La Guajira
La Guajira, Riohacha, Colombia

<http://revistas.uniguajira.edu.co/index.php/cei>

Este documento fue depositado en Zenodo. DOI:

<https://www.doi.org/10.5281/zenodo.8091879>

José Azabache Santos

<https://orcid.org/0000-0001-8553-9766>

jdazabaches@unitru.edu.pe

Facultad de Ingeniería,

Universidad Nacional de Trujillo, Perú

Nelson Angeles Piedra

<https://orcid.org/0000-0002-3146-3206>

nangeles@unitru.edu.pe

Facultad de Ingeniería,

Universidad Nacional de Trujillo, Perú

Alberto Mendoza De los Santos

<https://orcid.org/0000-0002-0469-915X>

amendezad@unitru.edu.pe

Departamento de Ingeniería de Sistemas,

Universidad Nacional de Trujillo, Perú

LA SEGURIDAD DE LA INFORMACIÓN EN EL INTERCAMBIO DE INFORMACIÓN DE LAS CADENAS DE SUMINISTRO

Information Security in the information sharing in Supply Chains

RESUMEN

En el mundo actual, el intercambio de información en las cadenas de suministro de las organizaciones es cada vez más necesaria, esto debido a los grandes beneficios de reducir costos y entablar relaciones mucho más beneficiosas para la organización. Para las empresas es fundamental compartir documentación de una manera selectiva, pero a la vez es más compleja. La fuga de la información dificulta su intercambio, lo cual perjudica la productividad, las ganancias, confianza y competitividad. El presente artículo tiene como objetivo determinar cuál es la situación actual y la importancia de la seguridad de la información en la pérdida de datos durante su canje en las cadenas de suministro. Por tal motivo, se hizo una revisión sistemática que se basa en la metodología PRISMA, abarcando principalmente información que está comprendida entre los años 2018 y 2022. Donde se encontró que no solo se mantiene la privacidad de la información a través de soluciones tecnológicas, como el blockchain y controles de acceso sofisticados, también se hace manteniendo ambientes conscientes en la cultura de la preservación de la integridad de los documentos. Concluyendo que la seguridad de la información se ha convertido en un elemento clave para la optimización del intercambio de la información, logrando que las organizaciones tengan confianza del desempeño operacional que puede obtener su cadena de suministro, manteniendo o incluso mejorando la resiliencia de la misma.

Palabras clave: Seguridad de la información, Intercambio de información, Cadena de suministro, Fuga de información.

ABSTRACT

In today's world, the information sharing in the supply chains of organizations is increasingly necessary, due to the great benefits of reducing costs and establishing much more beneficial relationships for the organization. For organizations it is essential to share information and data in a selective way, but at the same time it is more complex. Information leakage makes it difficult to share information, which hurts productivity, profits, trust and competitiveness. The objective of this article is to determine the current situation and the importance of information security in information leakage in the information sharing in supply chains. For this reason, a systematic review was carried out based on the PRISMA methodology, mainly covering information that is between the years 2018 and 2022. Where it was found that not only is the privacy of information maintained through technological solutions, such as blockchain and sophisticated access controls, it is also done by maintaining conscious environments in information security culture. Concluding that information security has become a key element for the optimization of information sharing, ensuring that organizations have confidence in the operational performance that their supply chain can obtain, maintaining or even improving its resilience.

Keywords: Information security, Information sharing, Supply chain, Information leakage.

Recibido: 7 de diciembre de 2022

Aceptado: 9 de marzo de 2023

Publicado: 29 de junio de 2023



INTRODUCCIÓN

Un intercambio de información es una de las estrategias para superar los problemas emergentes de una estructura cambiante en una cadena de suministro (Sicari et al., 2016). Este dentro de una cadena de suministros puede ser muy beneficiosa en cuanto a colaboración entre organizaciones y miembros de la misma cadena, a la vez su rol se hace cada vez más complejo e indispensable, esto se debe a la tendencia de globalización de las empresas y sus capacidades de abastecimiento (Khan et al., 2022). Cuando el canje de data se realiza de manera efectiva, este logra una integración para una eficiencia operativa y la eficacia estratégica de la cadena, es decir, el intercambio de información logra mejorar el desempeño logístico (Orjuela Castro et al., 2016; Silva Rodríguez et al., 2017).

Según Simatupang y Sridharan (2002) el cambio de documentos es la forma en la que un miembro comparte ideas, planes estratégicos, completos y confidenciales, con otros integrantes de la cadena de suministro. Esto les permite reunir la información necesaria para una exacta, transparente, relevante y oportuna toma de decisiones. Además, se indica que el compartir documentación precisa y oportuna hace más fácil filtrar los ruidos de otras variantes y poder tomar decisiones más acertadas.

En el tipo de información compartida según Montoya y Vargas (2011) existe una clasificación sistemática de estrategias de intercambio de información que se basan en el nivel transaccional, donde los datos compartidos son referidos a las capacidades de ventas, las especificaciones de entrega, precios, etc., el operacional donde la información compartida es todo lo que tiene que ver con el inventario y la capacidad de abastecimiento, producción, tiempos de entrega, etc. Y, por último, el estratégico que se refiere a compartir toda la data que tiene que ver con el mercado, la demanda y el cliente.

En este contexto Tan et al. (2016) dicen que adoptar el intercambio de información y otras estrategias colaborativas con el fin de apoyar a las empresas, estas quedan expuestas a mayores riesgos en la cadena de suministro; uno de estos riesgos mayores que desencadena es la recurrencia de fuga de información, debido a que cuando sucede el cambio de documentos eficiente, la información confidencial que va a través de la cadena aumenta en volumen. La pérdida de documentación provoca que las organizaciones pierdan una ventaja competitiva dentro del campo en el que se desarrollan. Además, la falta de conciencia y resiliencia de las empresas para manejar estas fugas se vuelven angustiante para identificar la verdadera razón del problema.

La fuga de información según la CWE (2008) es definida como la información que es expuesta o filtrada de manera intencionada o no intencionada a un participante de la cadena de suministro que no ha sido autorizado para recibir esa documentación, perdiendo confidencialidad. Se entiende entonces que por perdidas de datos se afectan todas las características de confidencialidad, perdiendo valor para la empresa e incluso teniendo efectos negativos.

García (2020) informa que el 93 % de las fugas de información son causadas principalmente por relaciones de la empresa, con intenciones de obtener datos confidenciales. Así también, se indica que el 28 % son causados por ataques externos y en un 19 % mediante incidentes internos. Dicho esto, se reflexiona en que mientras una empresa quiere lograr un mejor desempeño operativo en su cadena de suministro a través de colaboraciones, ya sea internas o externas que involucran un intercambio de datos, la empresa estará más expuesta a este riesgo.

Es por esta razón que el presente artículo de revisión sistemática busca comprender la situación actual de lo que están haciendo las organizaciones y como toman a la seguridad de la información con respecto a la fuga de la información en los intercambios de información de las cadenas de suministro. Ya que según la ISO 27001 seguridad de la información es referida a la confidencialidad, integridad y disponibilidad de información y de datos confidenciales para una empresa u organización, sea en el formato que se encuentre, físico o digital.

Por lo cual, para poder dar desarrollo a este artículo, se hace importante responder a las siguientes preguntas: ¿Cuál es la situación actual de la seguridad de la información y qué importancia tiene con respecto a la fuga de información en el intercambio de información de las cadenas de suministro en los últimos 5 años?

MATERIALES Y MÉTODOS

Metodología

Esta revisión sistemática de la literatura científica para establecer la situación actual de la seguridad de la información y la importancia que tiene su fuga durante el intercambio, se realizó siguiendo los lineamientos de la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses).

Fundamentación de la metodología

La revisión sistemática de la literatura (RSL) tiene una importancia imprescindible en cualquier tipo de trabajo de investigación, esto debido a que da lugar a un estudio más estructurado y que está sustentado tanto de forma teórica como conceptualmente por más investigadores, resolviendo una pregunta de estudio. Además, es considerada como una de las mejores formas de evidencia por encima de las investigaciones básicas, estudios observables e incluso ensayos clínicos aleatorizados por el hecho que lo respaldan múltiples artículos de investigación (Moreno et al., 2018). Así mismo Beltrán (2005) afirma que las revisiones sistemáticas son necesarias cuando hay una pregunta muy puntual y que está relacionada con varios estudios primarios y existe una incertidumbre muy marcada.

El propósito principal por el cual las revisiones sistemáticas son desarrolladas, es que, a través de la aplicación de métodos sistemáticos y explícitos, como una problemática o cuestión específica y obteniendo información de fuentes inclusivas a través de una estrategia de búsqueda explícita y estructurada, se logre disminuir los sesgos existentes en cuanto al tema que se está desarrollando (Arévalo et al., 2010).

Se considera que la metodología PRISMA es una de las metodologías que está ayudando a muchos investigadores a tener un estudio más estructurado y mejor redactado (Molins et al., 2018), razón por la cual se ha escogido este método para ayudar a planificar y realizar la revisión sistemática, asegurando una recopilación y sustentación de información adecuada.

Teniendo en cuenta las definiciones encontradas y considerando la evaluación de riesgo de sesgos, se puede dejar en evidencia la importancia del desarrollo de una investigación siguiendo la metodología Prisma. Arnau y Sala (2020) detallan los siguientes pasos para desarrollar la metodología: diseñar una estrategia de exploración, identificar y seleccionar la literatura relevante, registrar los resultados de la búsqueda para posteriormente organizarla y finalmente analizar e interpretar los resultados seleccionados.

Estrategia de búsqueda

Primero, la pregunta de investigación aborda la relación de los temas seguridad de la información y la fuga de información en el intercambio de información de las cadenas de suministro. Por tal motivo, comenzamos la investigación por definir las palabras claves para comenzar el estudio. Identificamos los siguientes términos: “seguridad de la información”, “fuga de información”, “intercambio de información”, “cadena de suministro”. Así también, los términos en el idioma inglés fueron los siguientes: “information security”, “information leakage”, “supply chain”, “information sharing” (Figura 1). Para el desarrollo de este estudio, se establecieron determinadas fuentes de información o motores de base de datos tales como Scopus, Science Direct, Alicia y Google Académico.

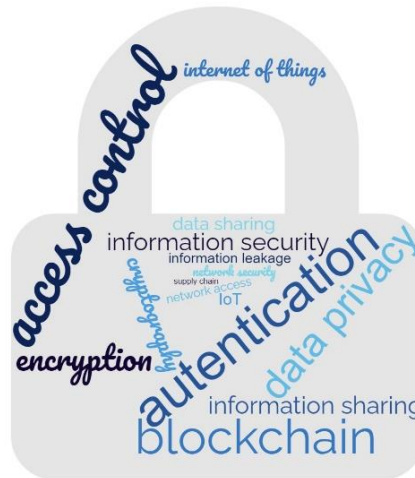


Figura 1. Nube de palabras clave encontradas para la estrategia de búsqueda.

Criterios de inclusión y de exclusión

Según Quispe y colaboradores (2021) los criterios de exclusión e inclusión son importantes de considerar al momento de hacer una investigación, debido a que guían, maximizan el tiempo de búsqueda, los errores son mínimos y aseguran la transparencia en la investigación si no se usan, se estaría adoptando una visión general que no serviría para responder a las preguntas que se tienen y saber discriminar entre las referencias, aquellas que son adecuadas para la investigación. Por lo cual, tres capas de criterios de inclusión/exclusión se definen para evaluar la relevancia de cada publicación encontrada.

Como primera capa, los artículos deben cumplir tres criterios de inclusión:

1. Se consideraron artículos escritos en inglés y español.
2. Es importante establecer las fechas desde 2018 al 2022.
3. Se establecieron los tipos de documentos académicos (por ejemplo, artículos, tesis y artículos de revisión).

En segunda capa, se consideró necesario establecer que el artículo debe estar disponible en línea para aumentar la posibilidad de que los artículos seleccionados se encuentran realmente disponibles. En caso de que el artículo no está disponible públicamente, se pasa al siguiente procedimiento. Por último, en la tercera capa se estableció como criterio de exclusión dejar fuera aquellas publicaciones con temas no relevantes a la investigación.

Catálogos y base de datos

Se encontraron un total de 114 entre artículos y artículos de revisión distribuidos de la siguiente manera: Scopus: 6 referencias, Science Direct: 54 referencias; Alicia: 1 tesis de grado; Google académico: 66 referencias en inglés y 11 en español. Los tipos de documentos encontrados variaron entre tesis, revistas, libros, artículos y artículos de revisión (Figura 2).

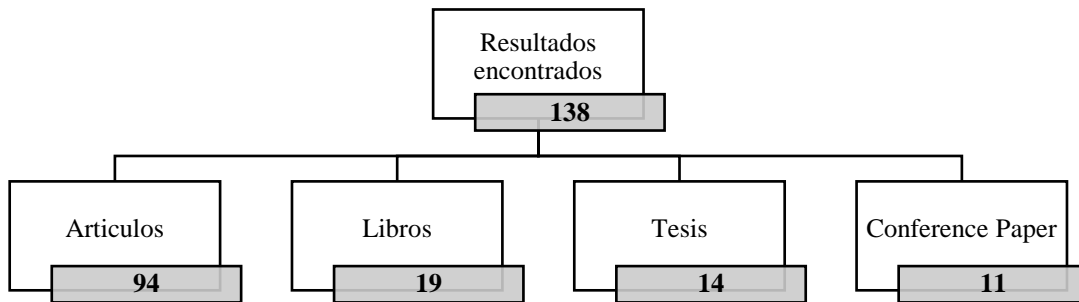


Figura 2. Catálogo de referencias encontradas.

SCOPUS – 6: TITLE-ABS-KEY ("information security" AND ("information sharing" OR "data sharing") AND "supply chain" AND "information leakage")

SCIENCE DIRECT – 54: "information security" AND ("information sharing" OR "data sharing") AND "supply chain" AND "information leakage"

Alicia – 1: "seguridad de la información en el intercambio de información de cadenas de suministro".

Google Académico - 66: "information security" "information sharing" "supply chain" "information leakage"

Google Académico - 11: "seguridad de la información" "intercambio de información" cadena de suministro

A continuación, se va muestra en la Figura 2 el flujograma para el descarte de referencias en el cual se detalla la cantidad de artículos encontrados, que, con los criterios de exclusión establecidos anteriormente, se han ido descartando.

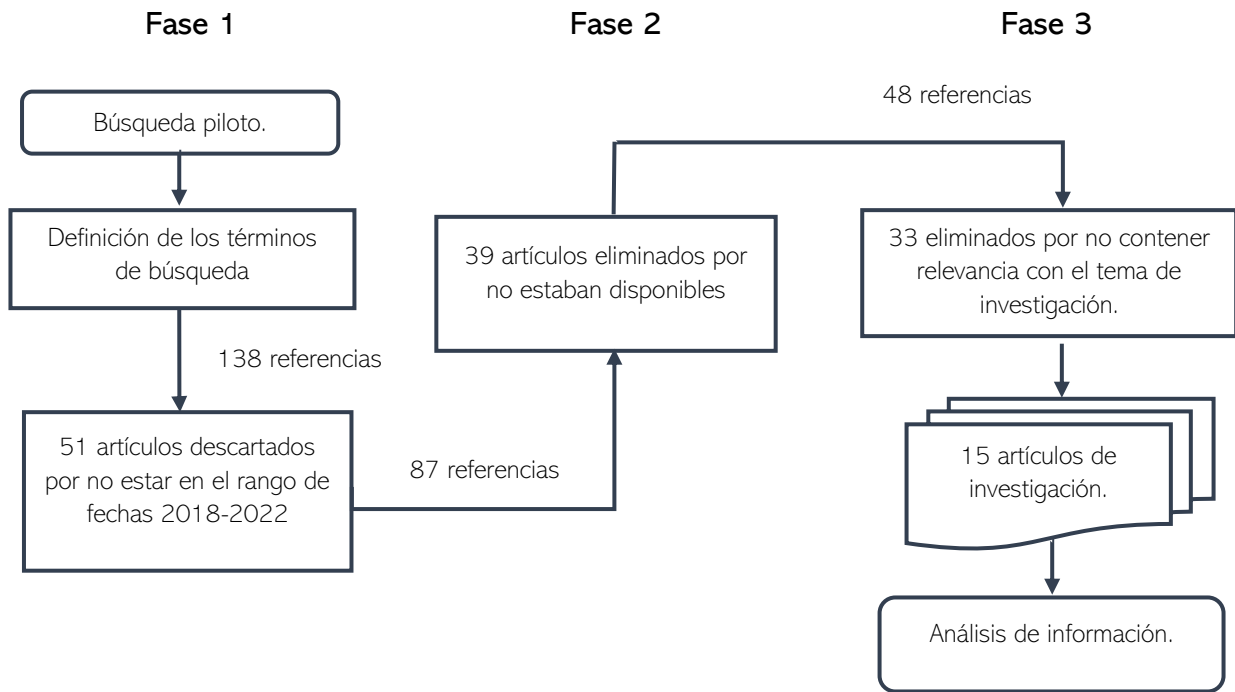


Figura 2. Flujograma de descarte de referencias.

RESULTADOS Y DISCUSIÓN

Se obtuvieron los siguientes resultados después de una identificación de artículos relevantes a la seguridad de la información para fugas de la información en el intercambio de información de las cadenas de suministro (Tabla 1).

Tabla 1. Relación de artículos aprobados en la revisión sistemática según los criterios de inclusión

AUTORES	AÑO	PAÍS	TÍTULO DE LA INVESTIGACIÓN	IMPORTANCIA RESCATADA
Wai-Peng Wong, Kim Hua Tan, Kannan Govindan, Di Li, Ajay Kumar	2021	Malaysia	A conceptual framework for information-leakage-resilience	El estudio respalda una relación inversa entre la cultura de seguridad de la información y la fuga de la información, esto implica que, si se tiene un grado alto de cultura de seguridad de la información en una organización, menos fuga de datos habrá y el intercambio de información en la cadena de suministro será efectivo. Eso quiere decir, que las organizaciones deberían usar la cultura de seguridad de la información para mitigar la fuga de información y mantener la resiliencia en sus cadenas de suministro en el intercambio de información.



AUTORES	AÑO	PAÍS	TÍTULO DE LA INVESTIGACIÓN	IMPORTANCIA RESCATADA
Wai-Peng Wong, Kim Hua Tan, Stephanie Hui-Wen Chuah, Ming-Lang Tseng, Kuan Yew Wong and Shamraiz Ahmad	2020	Malaysia	Information sharing and the bane of information leakage: a multigroup analysis of contract versus noncontract	Destaca una serie de relaciones desde la calidad de la información, tecnología de seguridad de la información y el intercambio de información, todas moderadas positivamente por la cultura de seguridad de la información, terminan en una influencia en el desempeño de la cadena de suministro de forma positivamente fuerte. Indican que la cultura de la información es elemento clave de la seguridad de la información.
Ali Vafaei-Zadeh, Thurasamy Ramayah, Haniruzila Hanifah, Sherah Kurnia, Imran Mahmud	2020	China	Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia	El tema de la seguridad de la información no es meramente técnico, es una disciplina que tiene varias dimensiones, que van desde lo social, cultural, tecnológico, educativo, administrativo, humano y psicológico hasta la ley y la aplicación. Además, las posibilidades de violación de la seguridad de la información se reducen considerablemente si los empleados son conscientes del problema y el efecto que trae una mala seguridad de la información. Consideran que, si se tiene un sistema de soporte a las decisiones, es importante contar con soluciones tecnológicas, pero rescatan que debe ir en conjunto con una cultura de seguridad de la información.
Hiep Cong Pham, Thanh-Thuy Nguyen, Scott McDonald, Nhu Quynh Tran-Kieu	2019	Vietnam	Information Sharing in Logistics Firms: An Exploratory Study of the Vietnamese Logistics Sector	Consideran que la razón por la cual se les permitió obtener beneficios de un intercambio de información sin problemas y con bajas probabilidades de un riesgo de fuga de información fue la consciencia de seguridad de la información implantada por parte del personal de TI hacia los participantes de una cadena de suministros, razón por la cual el plan de integración de un intercambio de información les resulto sencillo.
Yanting Huang, Yuqing Liang	2022	China	Influence of corporate social responsibility considering dual-channel recycling competition and privacy information protection	Se apoyaron de la inteligencia artificial para desarrollar un borrado de datos en su cadena de suministro para dispositivos electrónicos que reciclaban, para darle la confianza al cliente que usaba los servicios de reciclaje, de que los datos confidenciales guardados en sus dispositivos no serían expuestos. De cierta manera la seguridad de la información permitió que los clientes tomaran más confianza en los servicios prestados, mejorando la utilidad de la empresa y desarrollando un mejor flujo en la cadena de suministro.



AUTORES	AÑO	PAÍS	TÍTULO DE LA INVESTIGACIÓN	IMPORTANCIA RESCATADA
Xuran Li, Bishenghui Tao, Hong-Ning Dai, Muhammad Imran, Dehuan Wan, Dengwang Li	2021	China	Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic?	Las tecnologías de la información han llegado a facilitar muchas operaciones que hasta en una cadena de suministro de vacunas COVID-19 se han implementado una red de blockchain con tecnologías IoT para optimizar el reparto de vacunas, lo cual ha beneficiado mucho a los centros médicos y durante la época de pandemia ayudó a reducir la posibilidad de riesgo de una fuga de información privada de pacientes. Además, el rendimiento de la cadena de suministros mejoró notablemente y el sistema contaba con una transparencia, fluidez y buena recepción.
Yan Li, Ming K. Lim, Chao Wang	2022	Reino Unido	An intelligent model of green urban distribution in the blockchain environment	En una cadena de suministro de distribución urbana, las partes interesadas desconfiaban de los colaboradores, por lo cual decidieron apoyarse de la tecnología del blockchain para poder optimizar los tiempos y recorridos de entrega con el fin de poder reducir la contaminación ambiental. Obtuvieron como resultado que la implementación de una red de blockchain en una cadena de suministro de distribución urbana, logró que las partes interesadas tengan confianza al momento de un intercambio de información debido a que los datos ya estaban protegidos de manera encriptada, de forma que se logró hacer una cooperación logística horizontal, que esta a su vez permite mejorar el desempeño operacional de la cadena de suministro.
Adam Dachowicz, Siva Chaitanya Chaduvula, Mikhail J. Atallahb, Ilias Bilonis, Jitesh H. Panchal	2018	Estados Unidos	Strategic information revelation in collaborative design	La estrategia de un diseño colaborativo para una cadena de suministro está en aportarle trazabilidad, transparencia, fluidez y seguridad de que los datos o información confidencial que va a ser compartida, se realice de una manera efectiva de tal manera, que se obtengan todos los beneficios de un intercambio de información. Para eso afirman que el apoyo de la tecnología blockchain, además de una trazabilidad y transparencia, aporta confianza en cuanto a información compartida con las partes interesadas de la cadena de suministro.
Renee Rui Chen, Kun Chen, Carol X.J. Ou	2022	Holanda	Facilitating interorganizational trust in strategic alliances by leveraging blockchain-based systems: Case studies of two eastern banks	El blockchain como solución ante posibles fugas de información, beneficia más a las cadenas de suministro en donde se requiere en mayor medida el cifrado, la autenticidad y la disponibilidad de los datos. Además, se identificó que el apoyo de los altos mandos es imprescindible en la implementación de una red blockchain.



AUTORES	AÑO	PAÍS	TÍTULO DE LA INVESTIGACIÓN	IMPORTANCIA RESCATADA
Claudia Colicchia, Alessandro Creazza, Carlo Noè, Fernanda Strozzi	2018	Reino Unido	Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA)	Se denota que el principal riesgo de un intercambio de información es la fuga de la información intencional o no intencional, por eso, es importante tener un plan de seguridad de la información en un intercambio de información de una cadena de suministro para lograr el mayor beneficio de la colaboración. No solo es importante abarcar los problemas o riesgos técnicos de una cadena de suministro, debe de tenerse en cuenta el factor humano que participa en la cadena de suministro.
Xiaoting Guo, Zhaojun Yang, Chrissie Diane Tan	2019	China	Emerging Information Technologies Usage: Opportunities and Challenges for Supply Chain Vulnerability	Implementar tecnologías emergentes como medidas para la seguridad de la información puede implicar ciertas desventajas si es que no cuentan con la capacidad tecnológica para mantener la información segura. Por lo que se recomiendan mantener seguras estas tecnologías a través de controles de acceso, encriptaciones y medidas de seguridad de la información para mantener protegida la información que se comparte a través de ellas en una cadena de suministro operativa.
Siva Chaitanya Chaduvula, Adam Dachowicz	2018	Estados Unidos	Security in Cyber-Enabled Design and Manufacturing: A Survey	La implementación de una solución tecnológica, a través de controles de acceso o de políticas de seguridad, es de vital importancia para un diseño de una cadena de suministro de manufacturación al momento de que se quiere mejorar el desempeño operativo, esto si se trabaja con sistema de soporte a las decisiones, donde estos sistemas y con los sistemas de las partes interesadas o colaboradores deben estar interconectados entre sí para permitir el intercambio de información.
Showkat Ahmad Bhat, Nen-Fu Huang, Ishfaq Bashir Sof, Muhammad Sultan	2021	Taiwan	Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability	Para garantizar el uso eficiente de las tecnologías IoT es importante contar con seguridad de privacidad de datos y poder sacar los máximos beneficios de las tecnologías que facilitan el intercambio de información y la colaboración. El uso de estas tecnologías acompañadas del blockchain se vuelve un dúo potente en cuanto a mejora de eficiencia y seguridad, le da confianza a la empresa a poder desarrollar sistemas colaborativos. Sugieren que debe considerarse importante evaluar el comportamiento de los usuarios, contribuyendo a la seguridad de la información y mejorar el intercambio.

AUTORES	AÑO	PAÍS	TÍTULO DE LA INVESTIGACIÓN	IMPORTANCIA RESCATADA
Malaver Michael Garzón,	2021	Colombia	Propuesta conceptual para la implementación de la cadena de suministro de las vacunas contra el covid-19 en Colombia, a partir de una revisión sistemática de la aplicación de blockchain en la cadena de suministro de fármacos	El blockchain como solución tecnológica en cuanto a seguridad de la información para la fuga de la información, no solo protege los datos de este riesgo, sino que también aporta a la cadena de suministro el poder de tener acceso a la información en tiempo real, así como también el poder tener el control de brindar el acceso de la información a un tercero. Además, la trazabilidad de un producto como la capacidad de verificar el historial o el estado del producto y dándole un seguimiento exhaustivo, es un beneficio extra en cuanto a la implementación de la tecnología, aparte de que se hace más fácil y posible el intercambio de información dándole transparencia a la cadena de suministro.
Shuchih Ernest Chang, Yi-Chian Chen, Ming-Fang Lu	2019	Taiwan	Supply chain re-engineering using blockchain technology: A case of smart contract-based tracking process	Las partes interesadas de la cadena de suministro se benefician de un seguimiento transparente y controles que se puede dar al momento de implementar una blockchain, además, un contrato inteligente basado en la blockchain permite establecer acuerdos y que sean cumplidos estrictamente debido a que las cláusulas establecidas en el contrato inteligente ya no pueden ser modificadas, en cierta parte es un beneficio para la empresa que establece las cláusulas, pero para las partes interesadas no se puede saber del todo.

La tendencia de ubicación geográfica del lugar de procedencia a los que pertenecen las universidades o instituciones identificadas en los artículos de estudio, dando a conocer que el tema abordado es de interés global. Liderando China con cuatro referencias, posteriormente Malasia, Reino Unido, Estados Unidos y Taiwán son los países con mayor seguimiento dentro de nuestra investigación (Figura 3).

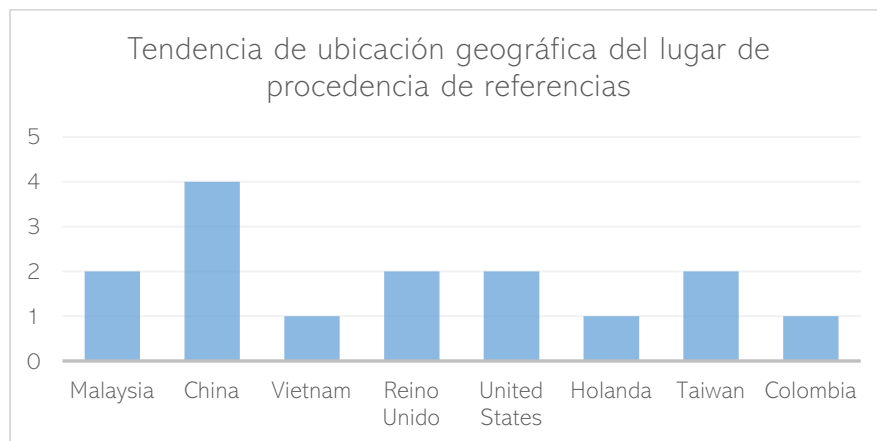


Figura 3. Tendencia de ubicación geográfica del lugar de procedencia de referencias.

En los resultados obtenidos se observa que solo se pudo contar con una tesis relacionada con lo que se viene investigando, la cual proveniente del país vecino: Colombia, en este trabajo se realizó una investigación precisa en cuanto al tema que se está desarrollando. La tesis se obtuvo como único resultado de la búsqueda en la base de datos de Google Académico en el idioma español. Lo cual da un indicio de que las investigaciones en este tema aún no se desarrollan lo suficiente y deberían acrecentarse aún más en el idioma español.

El riesgo del intercambio de información en las cadenas de suministros

En la literatura revisada, se sabe que al momento de decidir por un intercambio de información implica un cambio de datos de forma bidireccional y en tiempo real que pueden ser de varios aspectos en cuanto a la gestión de operaciones, tales como, niveles de inventario, estado de pedidos, pronósticos y preparativos para los socios de la cadena de suministro (Colicchia et al., 2018). Al compartir este tipo de información de manera efectiva, los miembros de la cadena de suministro recibirán una información precisa y oportuna, lo cual, por consecuencia trae decisiones más acertadas y un mejor rendimiento de la cadena de suministro. Además, en un cambio de datos de la cadena, está siempre abierta al surgimiento de nuevos canales de riesgo de fuga de información lo cual suele privar el efecto positivo que puede causar el canje de documentación. Y a medida que los documentos dentro de una cadena de suministro van en aumento, el riesgo de una pérdida aumenta en paralelo con esto, debido a que, un volumen de información con mucho más valor y fluye por la cadena de suministro (Pham et al., 2019).

Seguridad de la información y la fuga de información en el intercambio de información

Estudiar el tema de seguridad de la información es muy amplio, se encontró que actualmente está no solo implica ver el tema técnico o de soluciones tecnológica para mitigar riesgos, sino que también interviene el factor humano y la cultura de confianza y garantía que se le implanta. La seguridad de la información se trata de una disciplina que tiene varias dimensiones y van desde un tema social, cultural, tecnológico, educativo, gerencial, humano e incluso psicológica hasta la ley y la aplicación de esta. Una documentación segura no solo implica el reconocer cualquier posible riesgo en la cadena de suministro, sino también a las partes interesadas y al actuar de estas (Vafaei-Zadeh et al., 2020).

Si comenzamos viendo la implementación de seguridad de la información como un tema cultural tenemos que existen estudios donde dicha seguridad es aplicada como cultura y se relaciona con la eficacia del intercambio de datos. La fuga de la información es moderada por la cultura de seguridad de la información y también afecta negativamente a la resiliencia de la cadena de suministro. Donde se infiere a que esta cultura influye en la resiliencia de la cadena de forma directa e indirecta a través de un cambio de documentación eficaz. Por lo que, actualmente se ve que las empresas apuestan o deciden invertir por utilizar la cultura de seguridad de la información como una forma de mitigar la pérdida de datos. De no ser así, dicho escape puede destruir la resiliencia de una cadena de suministro (Wong et al., 2021).

Según algunos resultados contar con una cultura de seguridad de la información en un cambio de datos garantiza la calidad de la información, ya que junto con las tecnologías de la seguridad se moderan el desempeño operacional de una cadena de suministro. Esto quiere decir que, fortaleciendo dicha cultura, la calidad de la documentación que se comparte es la mejor, y el canje y las tecnologías usadas para la preservación de la integridad de la información siempre serán efectivas. Se afirma que la cultura de la seguridad de la información de los empleados es la que asegura una calidad en estos documentos, así como su integridad, confidencialidad y valor. Es por esto por lo que, los autores de los artículos recomiendan

contar con una conciencia por parte de los integrantes de las organizaciones donde se comparte creencias, valores y prácticas similares dándole la importancia que se merece a la seguridad de la información y los sistemas informáticos (Wong et al., 2020).

Así como hemos visto la forma en que las empresas adoptan a la seguridad de la información abarcando principalmente lo que es el tema cultural, con las nuevas tecnologías emergentes del mundo actual, implementar el blockchain para garantizar una privacidad de datos e información es una tendencia, debido a que aporta una trazabilidad, una mayor fluidez, transparencia y seguridad (Li et al., 2022).

La forma en que las empresas han optado por las colaboraciones a través del intercambio de información segura es a través de tecnologías como el IoT, que si bien es cierto les benefician en cuanto a operatividad, estas incrementan su nivel de eficiencia al momento de juntarlo con una red segura que mantenga la privacidad e integridad de los datos como lo es el blockchain. Así lo afirma Li y colaboradores (2021) en un estudio de una cadena de suministro de distribución de vacunas durante el COVID-19 donde el IoT junto con el blockchain resulta eficiente en cuanto atención a pacientes y el intercambio de información que se da a través de los dispositivos IoT de una manera segura, obteniendo la información precisa, oportuna y en perfecto estado.

Así también, no se debe olvidar que hay empresas que cuentan con un sistema de soporte a las decisiones en su cadena de suministro, estas vienen implementando controles de acceso sofisticados para poder controlar quien tiene acceso a la información, ya que estos sistemas de soporte, al momento de generar una colaboración con otro de los participantes de su cadena, deben conectarse a otros sistemas y lograr un cambio de documentación efectivo, para así obtener los beneficios de esa colaboración (Huang et al., 2022). Para ayuda del intercambio de información se desarrollan encriptaciones de los datos que se está compartiendo en los sistemas de soporte, esto garantiza la seguridad de la información de las partes de la transacción (Li et al., 2022). Aun así, se recomienda la implementación del blockchain que abarca todas estas soluciones, debido a la capacidad de rastrear y automatizar transacciones en todos los procesos de la cadena de suministro (Dachowicz et al., 2018).

Adicionalmente, muchas de los autores señalan que las empresas no adoptan medidas de seguridad ante fugas de información por lo costosas y tediosas que pueden llegar a ser, si bien es cierto la implementación de una red de blockchain requiere de una base digital, es decir contar con sistemas digitales de soporte a decisiones, gestión, etc. también requiere de una cantidad de técnicos de TI suficientes para poder llegar a implementarla y dar soporte a la misma red. Es por eso por lo que el apoyo de la alta dirección sea sostenido para poder llegar a implementarse una red de blockchain o cualquier medida de seguridad de la información que se decidan llevar a cabo (Chen et al., 2022).

Como se mencionó anteriormente, este artículo de revisión está enfocado en la situación actual y la importancia de la seguridad de la información en la fuga de la información cuando se realiza un intercambio de información en una cadena de suministro, obteniendo como las empresas u organizaciones están haciendo o desarrollando un intercambio de información de manera que sea efectiva y segura que garanticen la mejora de su desempeño operativo.

Aun así, encontramos que en Latinoamérica no se cuenta con las investigaciones suficientes con respecto al tema planteado, el único país en el cual se pudo encontrar un estudio sobre lo que la seguridad de la información ofrece ante una fuga de información en un intercambio de información de una cadena de suministro, fue Colombia. Malaver (2021) indica en su estudio que la blockchain como una medida de seguridad se vuelve imprescindible en el cambio de datos de la cadena y que la seguridad debe ser un moderador para poder validar aspectos como el desempeño operacional de la secuencia de suministro. Esto

debido a la capacidad de reportaje eficiente en cuanto a actividades de información se tratase, permitiendo que toda la documentación que se comparte es rastreable y dándole un mayor flujo a la información.

Según Bath y colaboradores (2021) si actualmente se cuenta con un sistema de soporte que facilite el intercambio de información, es necesario contar con soluciones técnicas para la seguridad de la información debido a que existen factores externos que pueden privar los beneficios de un canje en una cadena de suministros colaborativa, exponiendo la información confidencial quitándole valor. Sin embargo, consideramos que no debe de pasarse por alto el contar con una conciencia y cultura de seguridad de la información, debido a que no es suficiente una solución técnica para poder mitigar el riesgo de una fuga de información en la cadena de suministro. Por lo que se pone en discusión que, en un intercambio de información la secuencia de suministro debe contar con todos los factores que implica preservar la integridad de la información, tanto el técnico, como el cultural. Si bien una solución técnica para mitigar la fuga de datos toma el punto de colaboradores externos que pueden hacer daño, accidental o intencionalmente, se deja de lado los colaboradores internos que también importan en el desarrollo de una seguridad de la información robusta dentro de una cadena de suministro ya que también pueden causar daños.

Con la investigación realizada proponemos a todos los países latinoamericanos realizar investigaciones respecto al tema del factor humano y como gestionarlo, debido a la escasa información en este sector, ya que según un informe técnico de Cisco (2008) la fuga de la información es un tema no muy investigado y que la principal causa de estas pérdidas se da por los mismos colaboradores de una empresa, sea de manera intencional o no intencional, lo cual deja en tela de juicio el cómo actuar con respecto al comportamiento humano frente a esta problemática. Asimismo, invitamos a seguir investigando sobre el tema, debido a que este tema esta presto a diferentes perspectivas y pueden tomar un rumbo distinto al descrito en esta discusión.

CONCLUSIÓN

Concluimos que la seguridad de la información actualmente es un elemento clave para que las cadenas de suministro funcionen adecuadamente debido a la relación que tiene con la eficacia de un intercambio de información y el desempeño operacional de la cadena de suministro de la empresa y sus procesos. Mejora la confianza de las organizaciones para decidir por un intercambio de información eficiente con el objetivo de optimizar los procesos y desarrollar un plan estratégico colaborativo. Así también, se destaca que una solución tecnológica como la tendencia blockchain por más segura que sea, no es suficiente cuando interviene el comportamiento de los colaboradores que se involucran en el proceso. Las soluciones tecnológicas y el factor humano dependen siempre entre sí para poder lograr que los sistemas sean lo más seguro posible garantizando que la información esté protegida. Por ello al hablar de una seguridad de la información debe de tomarse en cuenta todos los factores que influyen en ella, a pesar del costo que pueda implicar, pero teniendo en cuenta que los beneficios que se arrojan en la revisión son mayores siempre.

LITERATURA CITADA

- Arévalo, R. A., Ortuño, G., y Arévalo, D. E. (2010). Revisiones sistemáticas (1). *Revista médica -Colegio Médico de La Paz*, 16(2), 69-80.
- Arnau, L., y Sala, J. (2020). La revisión de la literatura científica: Pautas, procedimientos y criterios de calidad. *Uab.cat*. 22 pp.
- Beltrán G., Ó. A. (2005). Revisiones sistemáticas de la literatura. *Revista Colombiana de Gastroenterología*, 20(1), 60-69.
- Bhat, S. A., Huang, N.-F., Sofi, I. B., & Sultan, M. (2021). Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. *Agriculture*, 12(1), 40. <https://doi.org/10.3390/agriculture12010040>
- Chaduvula, S. C., Dachowicz, A., Atallah, M. J., & Panchal, J. H. (2018). Security in cyber-enabled design and manufacturing: A survey. *Journal of Computing and Information Science in Engineering*, 18(4), 040802. <https://doi.org/10.1115/1.4040341>
- Chang, S. E., Chen, Y.-C., & Lu, M.-F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract-based tracking process. *Technological Forecasting and Social Change*, 144, 1–11. <https://doi.org/10.1016/j.techfore.2019.03.015>
- Chen, R. R., Chen, K., & Ou, C. X. J. (2022). Facilitating interorganizational trust in strategic alliances by leveraging blockchain-based systems: Case studies of two eastern banks. *International Journal of Information Management*, 102521, 102521. <https://doi.org/10.1016/j.ijinfomgt.2022.102521>
- Colicchia, C., Creazza, A., Noè, C., & Strozzi, F. (2018). Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA). <https://doi.org/10.1108/SCM-01-2018-0003>
- CWE - CWE-2008: Exposure of sensitive information to an unauthorized actor (4.9). (s/f). *Mitre.org*. Recuperado el 15 de octubre de 2022, de <https://cwe.mitre.org/data/definitions/200.html>
- Dachowicz, A., Chaduvula, S. C., Atallah, M. J., Bilonis, I., & Panchal, J. H. (2018). Strategic information revelation in collaborative design. *Advanced Engineering Informatics*, 36, 242–253. <https://doi.org/10.1016/j.aei.2018.04.004>
- Cisco Systems Inc. (2008). Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados. *Cisco.com*. Recuperado el 15 de octubre de 2022, de https://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf
- García, V. (2020). El 93% de las fugas de información provienen de terceros relacionados con la compañía. *Revista Byte TI*. <https://revistabyte.es/ciberseguridad/informacion/>
- Guo, X., Yang, Z., & Tan, C. D. (2019). Emerging information technologies usage: Opportunities and challenges for supply chain vulnerability. 2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).

- Huang, Y., & Liang, Y. (2022). Influence of corporate social responsibility considering dual-channel recycling competition and privacy information protection. *Journal of Cleaner Production*, 373(133850), 133850. <https://doi.org/10.1016/j.jclepro.2022.133850>
- Khan, A. A., & Abonyi, J. (2022). Information sharing in supply chains – Interoperability in an era of circular economy. *Cleaner Logistics and Supply Chain*, 5(100074), 100074. <https://doi.org/10.1016/j.clscn.2022.100074>
- Li, X., Tao, B., Dai, H.-N., Imran, M., Wan, D., & Li, D. (2021). Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic? *Pervasive and Mobile Computing*, 75(101434), 101434. <https://doi.org/10.1016/j.pmcj.2021.101434>
- Li, Y., Lim, M. K., & Wang, C. (2022). An intelligent model of green urban distribution in the blockchain environment. *Resources, Conservation, and Recycling*, 176(105925), 105925. <https://doi.org/10.1016/j.resconrec.2021.105925>
- Malaver Garzon M. (2021). Propuesta conceptual para la implementación de la cadena de suministro de las vacunas contra el covid-19 en Colombia, a partir de una revisión sistemática de la aplicación de blockchain en la cadena de suministro de fármacos. Universidad Católica de Colombia.
- Molins, F. y Serrano, M. (2018). Bases neurales de la aversión a las pérdidas en contextos económicos: revisión sistemática según las directrices PRISMA. *Revista de Neurología*, 68, 47-58.
- Montoya Torres, J. R., & Vargas, D. O. (2011). Análisis del concepto de colaboración en la cadena de suministro: Una revisión de la literatura científica. http://laccei.org/LACCEI2011-Medellin/RefereedPapers/LO075_Montoya.pdf
- Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. *Revista Clínica de Periodoncia, Implantología y Rehabilitación Oral*, 11 (3), 184–186. <https://doi.org/10.4067/s0719-01072018000300184>
- Orjuela Castro, J. A., Caicedo-Otavo, A. L., Ruiz-Moreno, A. F., & Adarme-Jaimes, W. (2016). Efecto de los mecanismos de integración externa en el desempeño logístico de cadenas Frutícolas. Un enfoque bajo dinámica de sistemas. *Revista colombiana de ciencias hortícolas*, 10(2), 311–322. <https://doi.org/10.17584/rcch.2016v10i2.5073>
- Pham, H. C., Nguyen, T.-T., McDonald, S., & Tran-Kieu, N. Q. (2019). Information sharing in logistics firms: An exploratory study of the Vietnamese logistics sector. *The Asian Journal of Shipping and Logistics*, 35(2), 87–95. <https://doi.org/10.1016/j.ajsl.2019.06.001>
- Quispe, A. M., Hinojosa-Ticona, Y., Miranda, H. A., & Sedano, C. A. (2021). Serie de Redacción Científica: Revisiones Sistemáticas. *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*, 14(1), 94–99. <https://doi.org/10.35434/rcmhnaaa.2021.141.906>
- Rawewan, M., & Ferrell, W. G., Jr. (2018). Information sharing in supply chain collaboration. *Computers & Industrial Engineering*, 126, 269–281. <https://doi.org/10.1016/j.cie.2018.09.042>
- Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Portisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers: A Journal of Research and Innovation*, 18(4), 665–677. <https://doi.org/10.1007/s10796-014-9538-x>

-
- Silva Rodríguez, J. D. (2017). Gestión de la cadena de suministro: una revisión desde la logística y el medio ambiente. *Entre ciencia e ingeniería*, 11 (22), 51–59. <https://doi.org/10.31908/19098367.3549>
- Simatupang, T. M., & Sridharan, R. (2002). The collaborative supply chain. *International Journal of Logistics Management*, 13(1), 15–30. <https://doi.org/10.1108/09574090210806333>
- Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and knowledge leakage in supply chain. *Information Systems Frontiers: A Journal of Research and Innovation*, 18(3), 621–638. <https://doi.org/10.1007/s10796-015-9553-6>
- Vafaei-Zadeh, A., Ramayah, T., Hanifah, H., Kurnia, S., & Mahmud, I. (2020). Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia. *Information & Management*, 57(8), 103386. <https://doi.org/10.1016/j.im.2020.103386>
- Wong, W.-P., Tan, K. H., Chuah, S. H.-W., Tseng, M.-L., Wong, K. Y., & Ahmad, S. (2020). Information sharing and the bane of information leakage: a multigroup analysis of contract versus noncontract. *Journal of Enterprise Information Management*, 34(1), 28–53. <https://doi.org/10.1108/jeim-11-2019-0368>
- Wong, W.-P., Tan, K. H., Govindan, K., Li, D., & Kumar, A. (2021). A conceptual framework for information-leakage-resilience. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-021-04219-5>