Innovación y Software
ISSN: 2708-0927
ISSN: 2708-0935
facin.innosoft@ulasalle.edu.pe
Universidad La Salle
Perú

De La Cruz Rodríguez, Gerson; Méndez Fernández, Alberto C.; Méndez Fernández, Ronny A.
Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática
Innovación y Software, vol. 4, núm. 1, 2023, Marzo-Agosto, pp. 219-236
Universidad La Salle
Perú

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 219-236
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos de revisión
Temática: Redes y seguridad informática
Recibido: 30/11/2022 | Aceptado: 10/01/2023 | Publicado: 30/03/2023

Identificadores persistentes:
ARK: ark:/42411/s11/a79
PURL: 42411/s11/a79

Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática

Information security in e-commerce based on ISO 27001: A systematic review

Gerson De La Cruz Rodríguez [1][0000-0002-9276-3376]*, **Ronny Adrián Méndez Fernández** [2][0000-0003-0867-7326], **Alberto Carlos Méndez Fernández** [3][0000-0002-0469-915X]

[1] Universidad Nacional de Trujillo. Perú. gdelacruz@unitru.edu.pe
[2] Universidad Nacional de Trujillo. Perú. rmendezf@unitru.edu.pe
[3] Universidad Nacional de Trujillo. Perú.amendozad@unitru.edu.pe

Autor para correspondencia: rmendezf@unitru.edu.pe

Resumen

En los últimos años, con la popularización tan acelerada del eCommerce (comercio electrónico), que facilita mucho la vida de las personas que, solo dando un clic, tiene la posibilidad de adquirir innumerables productos prescindiendo de la infraestructura física del mundo real. Este crecimiento va de la mano con la seguridad de la información por el valor de esta por lo tanto se vio necesario analizar las evidencias aportadas desde la investigación para conocer el estado actual de la gestión de la seguridad de la información en el ámbito del eCommerce. Se ha llevado a cabo una revisión sistemática siguiendo las directrices PRISMA de los artículos publicados encontrados en Scopus, incluyendo un total de 6 artículos. Los resultados señalan consistentemente que los sistemas de eCommerce son vulnerables en gran manera, y para esto se requiere de una mejora en la gestión de la seguridad de la información y una gestión de riesgos de seguridad consciente de las amenazas que van en aumento, para así ofrecer un buen servicio de ciberseguridad. Actualmente se encuentran en el mercado muchos gestores que ayudan a tener segura la información de las empresas, los cuales abarcan las necesidades de los sistemas y sus vulnerabilidades en conjunto, correspondientes a la gestión de la seguridad de la información relacionada con el eCommerce, pero la norma ISO 27001 abarca en gran manera muchas áreas de la seguridad de la información en una empresa, la cual brinda una mayor protección y confianza de los datos de sus clientes.

Palabras clave: ciberseguridad, comercio electrónico, gestión de la seguridad de la información, ISO 27001, seguridad de la información.

Abstract

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 219-236
https://revistas.ulasalle.edu.pe/innosoft

In recent years, with the rapid popularization of eCommerce (electronic commerce), which greatly facilitates the lives of people who, with just one click, have the possibility of acquiring innumerable products regardless of the physical infrastructure of the real world. This growth goes hand in hand with the security of information due to its value, therefore it was necessary to analyze the evidence provided from the investigation to know the current state of information security management in the field of eCommerce. A systematic review has been carried out following the PRISMA guidelines of the published articles found in Scopus, including a total of 6 articles. The results consistently indicate that eCommerce systems are highly vulnerable, and this requires an improvement in information security management and security risk management aware of the threats that are increasing, in order to offer a good cybersecurity service. Currently there are many managers on the market that help to keep company information secure, which cover the needs of the systems and their vulnerabilities as a whole, corresponding to the management of information security related to eCommerce, but the ISO 27001 standard largely covers many areas of information security in a company, which provides greater protection and confidence in customer data.

Keywords: *cybersecurity, e-commerce, information security management, information security, ISO 27001.*

Introducción

En los últimos años, con la popularización tan acelerada del comercio electrónico que facilita mucho la vida de las personas que solo dando un clic tienen la posibilidad de adquirir innumerables productos prescindiendo de la infraestructura física del mundo real, ha llegado a tomar un papel muy importante la seguridad de la información de los clientes que realizan este tipo de transacciones. Definiendo de forma técnica, según Torre y Codner, "electrónico hace referencia a la infraestructura mundial de la información, compuesta por la conjunción del hardware, el software, las redes informáticas y las telecomunicaciones, que permiten la transmisión, el procesamiento, el almacenamiento y la recuperación de datos en formato digital. En conjunto, estas tecnologías han dado origen a Internet, una gran red de carácter abierto y multifuncional cuyo acceso es cada vez más económico y amigable para gran parte de la población mundial" [1]. Y ya adentrándonos en el comercio electrónico para Turban, Volonino y Wood, "el comercio electrónico describe el proceso de compra, venta, transferencia, servicio o intercambio de productos y servicios o información mediante una red de computadores, incluyendo Internet" [2]. Podemos ahora decir que el comercio electrónico es una serie de operaciones comerciales y financieras realizadas mediante el procesamiento y la transmisión de información. Dicha información puede ser el objeto principal o un elemento relacionado con una transacción, lo que incluye compartir información sobre un negocio entre proveedores, consumidores, agencias gubernamentales y otras organizaciones a través de cualquier medio electrónico como correo principal o un elemento relacionado con

una transacción, lo que incluye compartir información sobre un negocio entre proveedores, consumidores, agencias gubernamentales y otras organizaciones a través de cualquier medio electrónico como correo electrónico, sitio web, etc., para realizar y ejecutar transacciones en actividades comerciales, administrativas y de consumo. Para [3] "las tiendas virtuales son páginas web cuyo objetivo es la venta de productos o servicios", ofreciendo al cliente un nuevo espacio para realizar transacciones en sus compras, de una forma más rápida desde cualquier lugar y a cualquier hora con acceso a todos los productos y el pago sea de forma virtual y rápida con un envió según la estructura física de lo adquirido. El comercio electrónico se define como "transacciones comerciales habilitadas de manera digital entre organizaciones e individuos". En donde estas transacciones sean mediadas a través de la tecnología digital, es decir, internet y la web, y en la cual se encuentren involucrados el intercambio de valores, como el dinero, entre los límites organizacionales o individuales a cambio de productos y servicios [4].

"El comercio electrónico entendido en sentido estricto cubre, principalmente, dos tipos de actividades: el pedido electrónico de bienes materiales que se entregan a través de canales tradicionales como el correo o los servicios de mensajería (comercio electrónico indirecto, que depende de factores externos, como la eficacia del sistema de transporte); y el pedido, el pago y la entrega en línea de bienes y servicios intangibles, como programas informáticos, revistas electrónicas, servicios recreativos y de información (comercio electrónico directo, que aprovecha todo el potencial de los mercados electrónicos mundiales)" [5].

De manera más doctrinaria, según [6] "el comercio electrónico constituye un fenómeno jurídico y se concibe como la oferta y la contratación electrónica de productos y servicios a través de dos o más ordenadores o terminales informáticos conectados a través de una línea de comunicación dentro del entorno de red abierta que constituye Internet. Representa un fenómeno en plena expansión con votos de crecimiento extraordinario en número de conexiones, clientes y operaciones". En cuanto a la Seguridad de la Información, es uno de los conceptos más importantes en el comercio electrónico, y es muy importante tener en claro lo que esto significa. Muchos son los riesgos que han tenido las tiendas virtuales desde que comenzaron hasta la actualidad, se debe saber que ningún sistema es seguro al 100%, pero se debe cubrir las brechas existentes para que la información no llegue a personas no autorizadas.

“La información, es como el aparato circulatorio para las organizaciones y requiere que se proteja ante cualquier amenaza que pueda poner en peligro las empresas, tanto públicas como privadas, pues en otro caso podría dañarse la salud empresarial. La realidad nos muestra, que las organizaciones empresariales se enfrentan en la actualidad con un alto número de riesgos e inseguridades procedentes de una amplia variedad de fuentes” [7].

“Un Sistema de Gestión de Seguridad de la Información (SGSI) es, tal como su nombre lo indica, un elemento para administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información” [8]. La norma ISO 27001 especifica los requisitos para una correcta implementación de un sistema de gestión de la seguridad de la información. Esta norma fue publicada por primera vez en el año 2005 y brinda las pautas para establecer, implementar, mantener y mejorar continuamente dicho sistema dentro del contexto de la organización [9]. “En los actuales momentos la norma ISO 27001:2007, presenta un compendio que proporciona una base común para la elaboración de reglas, un método de gestión eficaz de la seguridad y permite establecer informes de confianza en las transacciones y las relaciones entre empresas” [10]. La seguridad de la información son todas las medidas preventivas y reactivas de las personas, organizaciones y sistemas técnicos que permiten guardar y proteger la información con el fin de mantener su confidencialidad, autenticidad e integridad. Podríamos decir también que la seguridad de información se enfoca en la data o aquellos activos que tienen las empresas y se ven representados de diferentes formas como correo, papel, etc. Si se le llega a dar un mal uso a esta información, se puede comprometer de forma negativa a la empresa; en conclusión, es el conjunto de medidas que le permite a la empresa asegurar la confidencialidad, integridad y disponibilidad de su información, lo que conocemos como la triada de la información. “La seguridad de la información es conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa” [11]. Podemos ahora indicar que la seguridad de la información es la protección de la confidencialidad, integridad y disponibilidad de la información (ver Figura 1.1); es decir, cuidar de la triada de la información, lo que esto quiere decir es que la información sea accesible solo a las

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 219-236
https://revistas.ulasalle.edu.pe/innosoft

personas autorizadas, sea exacta sin modificaciones no deseadas y que esté disponible a los usuarios cuando lo requieran.

Figura 1. *Triada de la Información*

Métodos y Metodología computacional

Tipo de Estudio

En este trabajo se ha llevado a cabo una revisión sistemática de la literatura científica publicada en materia de seguridad de la información en aplicaciones de compraventa electrónica. Para su elaboración, se han seguido las directrices de la metodología PRISMA para la correcta elaboración de revisiones sistemáticas.

La pregunta seleccionada que conducirá el proceso metodológico fue la siguiente: ¿Cuál es el estado actual de la seguridad de la información en el comercio electrónico basado en ISO 27001?

Fundamentación de la Metodología

La revisión sistemática es la evaluación ordenada y explícita de la literatura a partir de una pregunta clara de investigación, junto a un análisis crítico de acuerdo a diferentes herramientas y un resumen cualitativo de la evidencia [12]. Teniendo en cuenta esta definición podemos ver la importancia de sintetizar información para poder destacar lo más relevante ante la gran diversidad de documentación existente que tratan el mismo punto desde diferentes contextos pero que tienen el mismo objetivo al final de todo. A continuación, se detalla el proceso de realización en sus distintas etapas.

Búsqueda inicial

Las primeras búsquedas se realizaron en la primera semana de octubre del 2022 combinando los términos ‘seguridad de la información’, ‘compraventa electrónica’, ‘ISO 27001’ en las bases de datos Scopus, Scielo, PubMed, Cochrane y Eric. Posteriormente, se amplió con una combinación, usando los operadores booleanos AND y OR según convino, de los términos ‘e-commerce’, ‘ecommerce’, ‘electronic commerce’, ’ISO 27001’, ’ISO/EIC’, ‘comercio electrónico’, ‘compraventa electrónica’, ‘tienda virtual’, ‘security information’. Debido a la poca cantidad de artículos encontrados en “Cochrane y Eric” y que estos además tenían poca relación y/o relevancia para con la revisión, se optó por retirarlos de la búsqueda sistemática.

Búsqueda sistemática

Se realizó una nueva búsqueda sistemática en la segunda semana de octubre de 2022, en Scopus, Scielo y PubMed. Acortando la cantidad de resultados a las publicaciones realizadas en un marco temporal no mayor a 5 años, es decir, con fecha de publicación desde el año 2018 (incluyéndolo) hasta la actualidad. La fórmula de búsqueda que se usó en el buscador **Scopus** fue:

KEY (e-commerce, OR ecommerce, OR information OR security OR management, OR information OR security, OR cybersecurity, AND iso AND 27001.) AND (LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018)) AND (LIMIT-TO (LANGUAGE, “English”) OR LIMIT-TO (LANGUAGE, “Spanish”))

En los buscadores **Pubmed** se usó la siguiente fórmula de búsqueda:

("information security management" OR "information security" OR security OR cybersecurity OR cyber-security OR e-commerce OR ecommerce OR "electronic commerce" OR e-business OR "online shopping" AND ISO 27001) Filters: in the last 5 years, English, Spanish.

Mientras que en **Scielo** fue:

("seguridad" OR "seguridad de la información" OR "information security management" OR "information security" OR security OR cybersecurity OR cyber-security OR "comercio electronico" OR "venta en linea"

OR e-commerce OR ecommerce OR "electronic commerce" OR e-business OR "online shopping" OR ISO 27001). Concretamente, se obtuvieron 80 resultados en Scopus, 10 en Scielo y 8 en PubMed. Antes de proceder a depurar los artículos, se definieron los criterios de inclusión y exclusión.

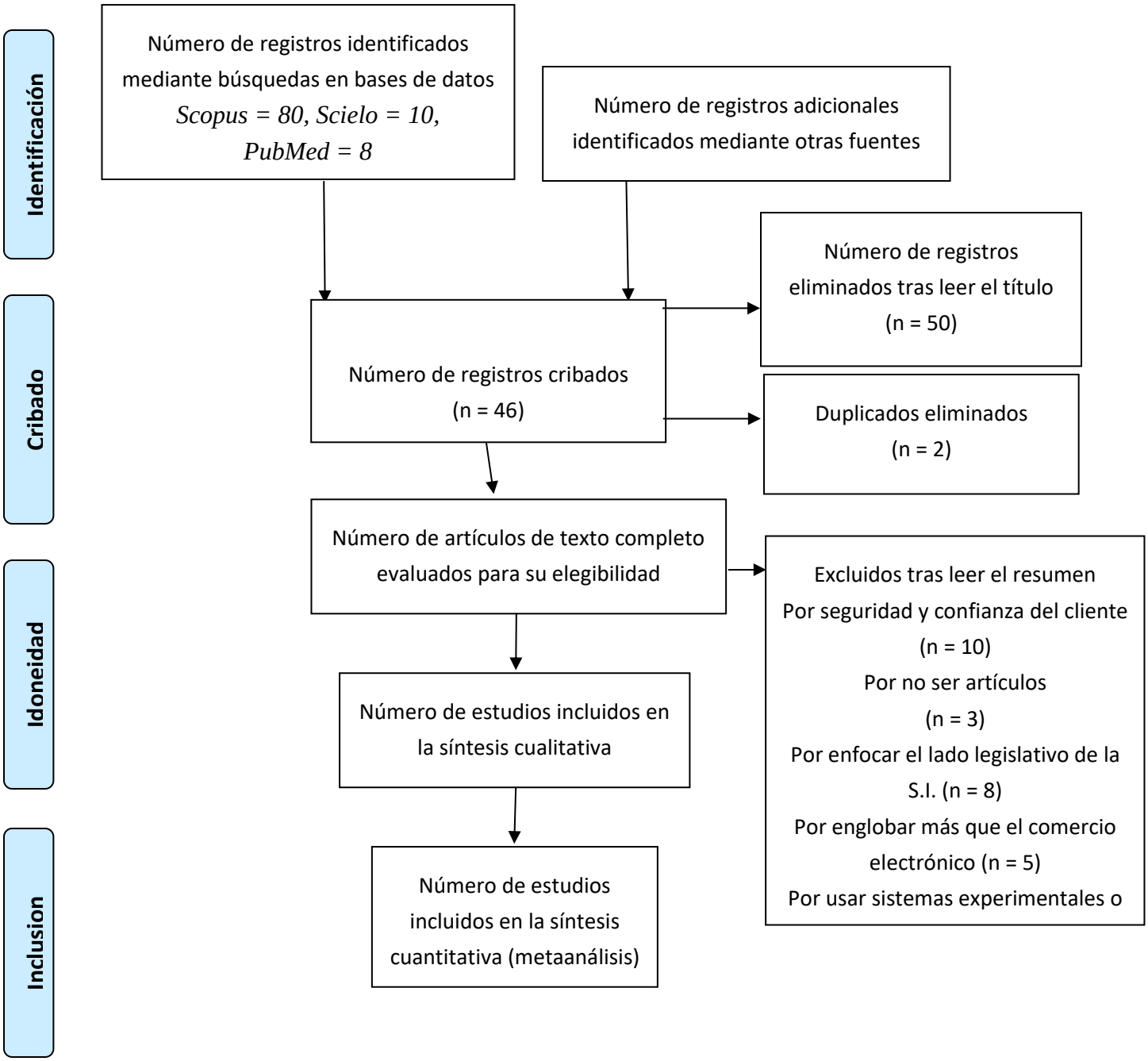


Figura 2. Diagrama de flujo PRISMA en cuatro niveles

Criterios de inclusión

- Para el desarrollo de la presente revisión sistemática, se incluyeron artículos originales publicados entre los años 2018 y 2022.
- Se seleccionan artículos redactados en inglés y español.
- Los artículos deben describir un enfoque de la gestión de la seguridad de la información en el comercio electrónico desde la perspectiva del sistema y la seguridad del mismo basado en la norma ISO 27001.
- Los artículos deben tartar comercio electrónico local como internacional.

Criterios de exclusión

- Se excluyeron aquellos artículos que se enfocan en la seguridad personal y confianza del cliente para participar en el comercio electrónico.
- Los documentos que no eran artículos.
- Aquellos que hablan del lado legislativo de la seguridad de la información.
- Los que englobaban contextos irrelevantes para la revisión (salud, finanzas, educación, etc.)
- Los que usaban tecnologías poco conocidas y/o sospechosas.

Según estos criterios, y sólo con la lectura del título, se consideraron adecuados 46 artículos (tras eliminar 2 articulo duplicado). Se procedió a leer el resumen y, a partir de esta lectura, se descartaron 30, principalmente por centrarse en la perspectiva del consumidor y la confianza del mismo para su participación en el comercio electrónico (n = 10), por tratarse de artículos de revisión(n = 3), por darle un enfoque más legislativo o político (n = 8), por tratar temas más generales que solo el comercio electrónico (n = 5) y por usar tecnologías poco mencionadas y/o sospechosas, lo que dificultaría la interpretación y síntesis de los resultados (n = 4).

Finalmente, 9 cumplieron los criterios de inclusión y se seleccionaron para llevar a cabo la revisión sistemática, pero 2 de ellos eran inaccesibles, nos indicaba error al tratar de ubicarlos mediante el link que nos proporcionaba la base de datos (Scopus), por lo tanto, se redujeron a 7 los artículos que formarán parte de la revisión sistemática. Todos ellos trataban el tema de la seguridad de la información en el comercio

electrónico, así como algunos proponen soluciones o sistemas de mejora para el mismo y dentro de un contexto de compraventa entre empresas, consumidores o empresa y consumidor (ver Figura 2).

Resultados y discusión

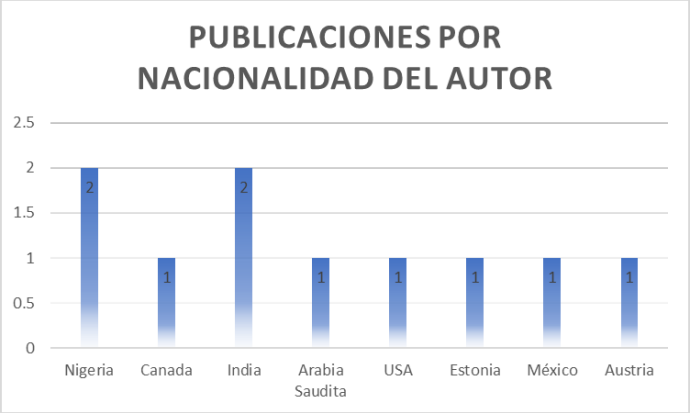
En primera instancia se procedió a identificar los datos de los artículos seleccionados para poder ver el desenvolvimiento y abordamiento del tema en el mundo como se muestran en las revistas donde fueron publicados, todo esto expresado en la Tabla 1.

Tabla 1. Artículos elegidos para la revisión sistemática

N.º	Año	Autor(es)	País	Base de datos	Título
1	2019	Ehikioya, Sylvanus A. Olukunle, Adepele A.	Nigeria, Canadá	Scopus	A formal model of distributed security for electronic commerce transactions systems
2	2020	Akinyede, Raphael Olufemi Adegbenro, Sulaiman Omolade Omilodi, Babatola Moses	Nigeria	Scopus	A security model for preventing e-commerce related crimes
3	2019	Khan, Shazia W	India	Scopus	Cyber Security Issues and Challenges in E-Commerce
4	2020	Dushyant, Kaushik Ankur, Gupta Swati, Gupta	India	Google Scholar	E-Commerce Security Challenges A Review

5	2022	Alfadli, Ibrahim	Arabia Saudita	Scopus	Integrated e-commerce security model for websites
6	2020	Affia, Abasi Amefon O. Matulevičius, Raimundas Nolte, Alexander	Estonia, USA	Scopus	Security risk management in E-commerce systems: A threat-driven approach
7	2020	Christopher A. Kanter-Ramirez, Josue A. Lopez-Leyva, Lucia Beltran-Rocha & Dominica Ferková	México, Austria	Scopus	Marco para el diseño óptimo de un sistema de información para diagnosticar el nivel de seguridad empresarial y gestionar el riesgo de la información basado en ISO/IEC-27001

En la Figura 3 se muestra un gráfico donde se representan la cantidad de autores, distribuidos por nacionalidad, que participaron en la redacción de los documentos seleccionados para la revisión, se considera como 0.5 de valor a aquellos autores que participaron en conjunto, pero su compañero era de otra nacionalidad. Esto nos permite ver en qué partes del globo se encuentran los investigadores que abordan el tema de estudio de nuestra revisión sistemática.



Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 219-236
https://revistas.ulasalle.edu.pe/innosoft

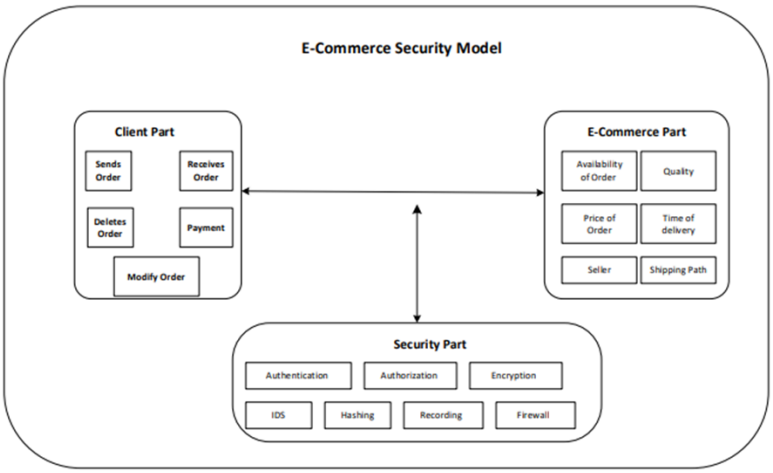
Figura 3. Publicaciones por nacionalidad del autor

Ahora mostraremos el porcentaje de artículos por año (ver Tabla 2), donde se observa que, en el año 2018 y 2021 se tiene un porcentaje de 0%, esto quiere decir que en estos años no se publicaron artículos relevantes que hayan pasado nuestros filtros de selección, en el año 2019 se encuentran 2 publicaciones, en el año 2020 se realizaron más de la mitad de las publicaciones que fueron seleccionadas para la realización de esta revisión sistemática y finalmente en el año 2022 se obtuvo un porcentaje de 14,29% siendo el año con menos publicaciones pero existentes, es decir, más que 0.

Tabla 2. Artículos publicados por año

Año	Número de publicaciones	Porcentaje
2018	0	0%
2019	2	28,57%
2020	4	57,14%
2021	0	0%
2022	1	14,29%

El proceso de compra es muy complicado, ya que se debe mantener toda la información protegida desde que los clientes hacen su pedido, pasando por el pago y envío, por lo cual se debe tener en cuenta ciertas técnicas que aseguren que todo saldrá bien, y sin filtración de datos importantes que puedan perjudicar a los clientes.



Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 219-236
https://revistas.ulasalle.edu.pe/innosoft

Figura 4. E-commerce security model for websites

A continuación, se muestra un diagrama de la interacción segura entre el cliente y la página en donde está comprando:

La Figura 4 nos muestra que para que una transacción sea segura, se debe trabajar con un apartado para la seguridad de la información que se verá afectada en dicho proceso, y dividiéndolo en varias partes para abarcar cada punto posible de filtrado de datos y asegurándolos pasando por ciertos muros de protección y verificando que el usuario sea el que dice ser y todo se realice con integridad.

Figura 5. Top e-commerce companies by market value

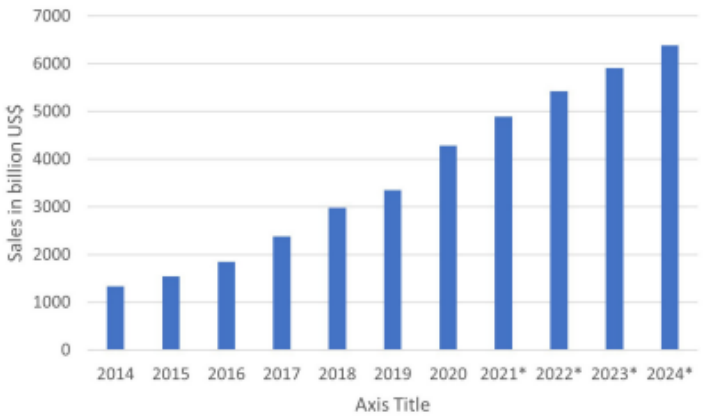


Figura 6. Top e-commerce companies by market value

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 219-236
https://revistas.ulasalle.edu.pe/innosoft

En la Figura 5, según [13], se muestra las principales empresas a nivel mundial que han optado por tener sus e-commerce y cuanto han llegado a costar a través de los años, estas empresas son de las pocas que han llegado a invertir más en su seguridad, debido a que tienen millones de clientes y los riesgos a los que están expuestos son muy grandes, ya que los ciberdelincuentes suelen fijarse en empresas grandes para robar la información. En la Figura 6, podemos apreciar una estimación de las ventas de estas empresas en corto plazo, mostrando el aumento que tendrá el mercado electrónico en un futuro no tan lejano y su gran impacto a nivel mundial, debido a que estas deben contar con una gran protección de toda la información de sus clientes, tomando en cuenta la triada de la información. En los últimos años, las empresas han optado por invertir más dinero en la seguridad de su información, debido al constante aumento de ataques cibernéticos que, por la alta competencia en el crecimiento de la tecnología y nuevas maneras de vulnerar sistemas de información, en este caso un comercio electrónico, han implementado estándares que les facilitan tener un control más eficiente, lo cual brinda mayor seguridad y confianza a sus clientes.

MAPA DE CALOR

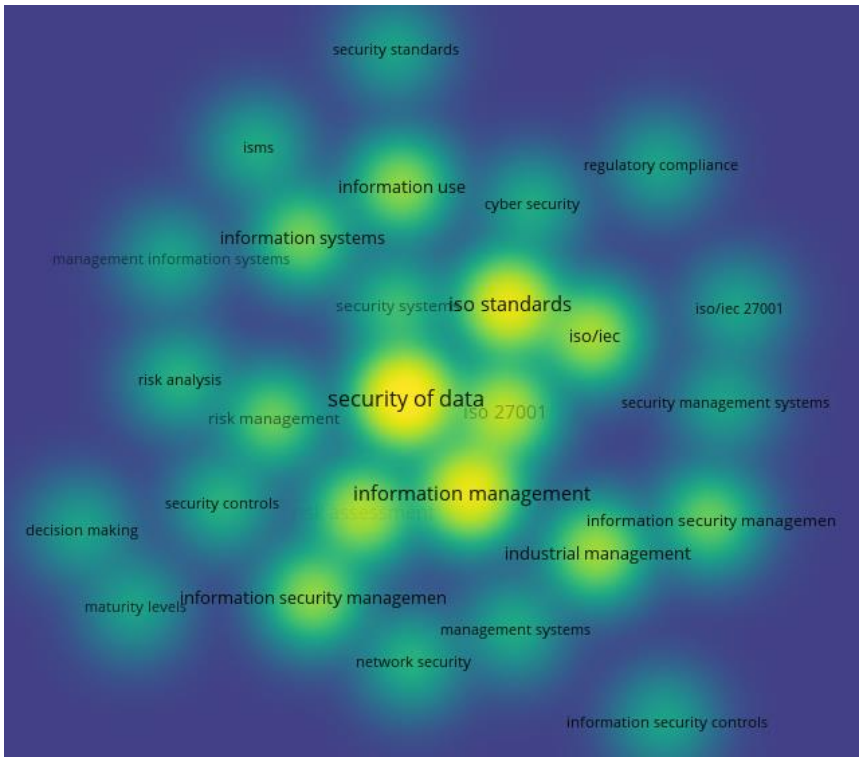


Figura 7. Palabras clave

En las búsquedas realizadas de revisiones sistemáticas previas y con la misma línea que nuestro tema de revisión, y gracias a la herramienta VosViewer se puede observar en la Figura 7 que las palabras más utilizadas en las búsquedas en los últimos 5 años son referentes a seguridad de datos y estándares ISO, entre las cuales resalta ISO 27001 ya que es una de las más aplicadas al momento de implementar un sistema de gestión de seguridad de la información, la cual permite a las organizaciones tener un estándar internacional y tener mayor confiabilidad en el comercio electrónico.

Concepto Comercio electrónico

El comercio electrónico ha transformado la industria del comercio tal como la conocemos, introduciendo mejores compras, envíos y servicios al cliente. Estos servicios comerciales generan y utilizan información confidencial, como compras de clientes, información financiera y personal, que son de gran valor para los atacantes [14].El comercio electrónico (comercio electrónico) es la compra y venta de mercancías y empresas, o la transmisión de activos o información, a través de una red electrónica, esencialmente Internet. Estos intercambios comerciales ocurren como b a b (empresa a empresa), b a c (empresa a consumidor), c a c (consumidor a consumidor) o c a b (consumidor a empresa). es el intercambio de artículos o servicios que utilizan redes informáticas como Internet o comunidades informales en línea [15].Los sistemas de comercio electrónico permiten a los clientes realizar compras en línea. Un proceso de pedido típico en los sistemas de comercio electrónico de empresa a cliente permite a los clientes buscar y encontrar artículos para comprar, negociar el precio de los artículos, agregar artículos a un carrito de compras, pagar artículos (es decir, comprar artículos) y pagar artículos. comprado; el sistema también permite a los comerciantes de comercio electrónico actualizar su inventario, verificar los métodos de pago de los clientes y planificar la logística para enviar artículos al cliente [16].

Concepto Gestión de la seguridad de la información

Proteger la información que se maneja en los sistemas de comercio electrónico exige una gestión de seguridad de la información y una gestión riesgos de seguridad consciente de las amenazas de seguridad en evolución

[14]. La gestión de la seguridad de la información se puede describir como la implementación de la colección de protocolos o regulaciones que llevan a cabo todas las transacciones de información. Estos criterios de seguridad deben estar en condiciones de proteger la seguridad de la información de diferentes empresas contra una serie de peligros innegables [17]. A pesar de la cantidad de modelos de seguridad para prevenir delitos relacionados con el comercio electrónico que se han propuesto en el pasado, no muchos de ellos son practicables o implementables. La autenticación de usuario proporciona la garantía de que los detalles del cliente están protegidos y se mantiene la privacidad. El sitio web del comerciante brinda una gran seguridad, asegurando así a los clientes que la transacción se lleva a cabo sin un ápice de duda o temor a la inseguridad y también se mantiene la integridad, la privacidad y la confidencialidad [18].La gestión de la seguridad de la información en el comercio electrónico es una fracción de la estructura de seguridad de la información. Básicamente se considera el uso de componentes que inciden en el comercio electrónico. Incluye la protección informática, la seguridad de datos y otros ámbitos más amplios relacionados con la estructura de seguridad de la información. La seguridad del comercio electrónico también se conoce como la protección de los activos de comercio electrónico contra los piratas informáticos [19].En la literatura revisada se puede apreciar que los autores trabajan con las dimensiones de la seguridad de la información, que incluyen a la triada de la información, que son la confidencialidad, integridad, disponibilidad además de a la autenticación y el no repudio, mismas que son mencionadas, como los ejes de la gestión de la seguridad de la información para su comprensión y gestión de sus riesgos; además de haber utilizado la norma ISO 27001 la cual ayudo a los autores a implementar un sistema de gestión de seguridad de la información para las empresas en las cuales se enfocó el trabajo.

Concepto de la norma ISO 27001

La norma fue diseñada y publicada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) en 2005. Fue planteada como una evolución de BS 7799. La norma 27001 especifica con detalle los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI) dentro del contexto interno y externo de la organización. Y algunos de los requisitos que dicta la norma son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza [20].ISO/IEC

27001 es el único estándar de toda la familia de normas ISO 27000 que se utiliza para brindar certificaciones a las organizaciones. Las demás normas de esta familia se usan para brindar un apoyo robusto y profundo para que la organización pueda construir e implementar un Sistema de Gestión de la Seguridad de la Información de manera correcta y duradera [21].

Discusión

La presente revisión sistemática muestra la realidad actual de la gestión de la seguridad de la información dentro de los sistemas de comercio electrónico, a pesar de la cantidad de modelos de seguridad para prevenir delitos relacionados con el comercio electrónico que se han propuesto en el pasado, no muchos de ellos son practicables o implementables, teniendo en cuenta los múltiples aspectos en los cuales la información puede verse afectada, cumpliendo así las buenas prácticas de la norma ISO 27001 para implementarla correctamente en las empresas de compra y venta en línea.

Una gran ventaja fue el tiempo de las publicaciones para la revisión, siendo el comercio electrónico un área relativamente nueva, el margen fueron 5 años, pero en años de comercio electrónico fue como abarcar todo lo existente hasta ahora. Además de claro empezar a enlazar nuevos términos a este campo para futuras investigaciones, como la utilización de Block Chain para el desarrollo de nuevos sistemas de gestión en el ámbito de la seguridad de la información.

En los artículos encontrados en nuestra investigación tenemos que con las tecnologías actuales se puede complementar de muy buena manera la implementación de medidas de seguridad tal y como dictan las normas ISO 27000. Según nuestra bibliografía la más utilizada viene a ser la ISO 27001 ya que es la única que tiene una certificación que garantiza que la organización es segura. Los clientes, aunque no sepan exactamente lo que dicta la norma, pueden sentirse en confianza al comprar en empresas de comercio electrónico que tengan una certificación en seguridad de la información.

Conclusiones

En los últimos años, las empresas que han conseguido un espacio en la web han crecido considerablemente y se han hecho muy conocidas alrededor del mundo, lo cual ha incrementado el número de sus clientes, y esto ha dado pase a que personas que no tienen que ver con las empresas o clientes y quieren robar información de ellos, para fines de enriquecerse ilegalmente. Este es un problema que aqueja a todas las empresas, ya que ninguna es 100% segura y aunque las brechas que tienen no son siempre las mismas, cabe resaltar que todo el tiempo estarán expuestas a ciberdelincuentes. La presente investigación indicó la gran importancia de contar con un sistema gestión de la seguridad de la información y que por esto se debe invertir mucho más tiempo y dinero para conseguir resguardar la información

del peligro al que suele estar expuesto, siendo los principales problemas que enfrentan tanto los proveedores como los consumidores las transacciones, la privacidad, la seguridad del sistema en el que se desarrollan estas y sus vulnerabilidades. Se puede además apreciar que uno de los aspectos que más aprovechan los ciberdelincuentes es el robo de sesión y muchos métodos más de ataques, lo cual perjudica a muchas empresas, ya sean pequeñas o grandes, y muchas de ellas no cuentan con políticas y controles bien definidos para un correcto manejo de la información. Una manera de proteger los comercios electrónicos seria implementar ISO 27001 que nos brinda una serie de pasos y requerimientos que deben tener para poder tener un alto nivel de seguridad, ya sea de la empresa y sus clientes. Esto lo hace mediante la creación e implementación de un SGSI para que la organización pueda tener el control y la confianza de que sus activos más valiosos como pueden ser: servidores, información, recursos humanos, etc., estén resguardados ante cualquier riesgo de amenaza latente.

Esto ayudará a los investigadores y académicos que trabajan actualmente en este campo a tener una idea de las tendencias y el estado actual para futuras investigaciones sobre el comercio electrónico, para que puedan tener una vista global de cómo existe la necesidad de tener un sistema de gestión de seguridad de la información en las empresas.

Referencias

[1] G. S. Torre y D. G. Codner, Fundamentos de Comercio, Buenos Aires: Universidad Virtual de Quilmes, 2013.

[2] E. Turban, L. Volonino y G. R. Wood, Information Technology for Management, Nueva York: Wiley, 2010.

[3] S. Carrasco Fernández, Venta online, Madrid: Ediciones Paraninfo, 2014.

[4] K. Laudon y C. Traver, E Commerce: Business, Technology, Society, Nueva York: Pearson Prentice Hall, 2009.

[5] A. Martínez Nadal, Comercio electrónico, firma digital y autoridades de certificación, Madrid: Aranzadi, 2001.

[6] R. Mateu De Ros, El consentimiento y el proceso de contratación electrónica, Pamplona: Aranzadi, 2000.

[7] C. M. Fernández, «La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información,» *Calidad*, pp. 40-44, 2012.

[8] F. Pacheco, «Welivesecurity,» 10 Septiembre 2010. [En línea]. Available: https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/.

[9] M. Podrecca, G. Culot, G. Nassimbeni y M. Sartor, «Information security and value creation: The performance implications of ISO/IEC 27001,» *Computers in Industry,* vol. 142, pp. 2-10, 2022.

[10] D. Freitas, «Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolivar,» *Enlace,* vol. 6, nº 1, p. 13, 2009.

[11] A. Pérez, «OBS Business School,» 09 Octubre 2017. [En línea]. Available: https://www.obsbusiness.school/blog/seguridad-de-la-informacion-un-conocimiento-imprescindible.

[12] H. A. García-Perdomo, «Conceptos fundamentales de las revisiones sistemáticas/metaanálisis,» *Urología Colombiana,* pp. 28-34, 2015.

[13] L. Xiang, F. A. Sayed, K. A. Muhammad, K. Jingying, I. Muhammad, U.-H. Jabbar y A. Shujaat, «Cyber security threats: A never-ending challenge for e-commerce,» *Frontiers in Psychology,* vol. 13, nº 2, p. 7, 2022.

[14] A. Nolte, A. Abasi-amefon y M. Raimundas, «Security Risk Management in E-commerce Systems: A Threat-driven Approach,» *Modern Computing,* vol. 8, nº 2, p. 28, 2020.

[15] S. Khan, «Cyber Security Issues and Chanllenges in E-Commerce,» *SSRN,* vol. 10, nº 5, p. 8, 2019.

[16] E. Sylvanus y O. Adepele, «A Formal Model of Distributed Security for Electronic Commerce Transactions Systems,» *International Journal of Networked and Distributed Computing,* vol. 7, nº 2, p. 17, 2019.

[17] A. Ibrahim, «Integrated e-commerce security model for websites,» *International Journal of Advanced and Applied Sciences,* vol. 9, nº 4, p. 8, 2022.

[18] A. O. Raphael, A. O. Sulaiman y O. M. Babatola, «A SECURITY MODEL FOR PREVENTING E-COMMERCE RELATED CRIMES,» *Applied Computer Science,* vol. 16, nº 3, p. 12, 2020.

[19] K. Shweta y G. Charu, «Ensure Hierarchal Identity Based Data Security in Cloud Environment,» *International Journal of Cloud Applications and Computing,* vol. 9, nº 4, p. 16, 2019.

[20] G. Culot, «The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,» *The TQM Journal,* 2021.

[21] X. Zhu y Y. Zhu, «Extension of ISO/IEC27001 to Mobile Devices Security Management,» *Communications in Computer and Information Science,* 2019.

Roles de Autoría

Gerson Roberth De La Cruz Rodríguez: Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Ronny Adrián Méndez Fernández:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Alberto Carlos Mendoza De Los Santos:** Conceptualización, Análisis formal, Supervisión, Redacción - borrador original.