Medidas de control interno para preservar la seguridad de los datos dentro de las empresas e-commerce: Una revisión sistemática

Internal control measures to preserve data security within e-commerce companies: A systematic review

Lecca Rengifo Luis Rolando [1]✉ • Paz Medrano Harrison Jordi [1] • Mendoza de los Santos Alberto Carlos [1]

Recibido: 24 Mayo 2023 / Revisado: 26 Julio 2023 / Aceptado: 8 Agosto 2023 / Publicado: 29 Septiembre 2023

Resúmen

El comercio electrónico ha experimentado un crecimiento exponencial en los últimos años, lo que ha llevado a un aumento considerable en la cantidad de datos confidenciales que almacenan y manejan las empresas de este sector. Por esta razón, es fundamental garantizar la seguridad de estos datos para proteger tanto la reputación de la empresa como la privacidad de los usuarios. El control interno se ha convertido en uno de los principales enfoques para evaluar la confiabilidad y eficiencia de los sistemas de gestión organizacional, misma que permite diseñar pruebas de auditoría y de esta manera determinar el grado de confianza que se puede tener en la información manejada en el comercio electrónico, por ello en la presente revisión sistemática establecemos la siguiente pregunta: ¿Cuáles son las diferentes medidas utilizadas en el control interno y cómo se aplican en las empresas de comercio electrónico?, para responder esta interrogante se efectuó la revisión de artículos publicados en Scopus, Science Direct y IEEE Xplore, dentro del periodo 2018 - 2023.

Palabras clave: Control interno, Protección de datos, Comercio electrónico, Privacidad.

Abstract

E-commerce has experienced exponential growth in recent years, which has led to a considerable increase in the amount of confidential data stored and handled by companies in this sector. For this reason, it is essential to ensure the security of this data to protect both the reputation of the company and the privacy of users. Internal control has become one of the main approaches to assess the reliability and efficiency of organizational management systems, the same that allows designing audit tests and thus determine the degree of confidence that can be obtained in the information handled in e-commerce; so in this systematic review, we establish the following question: What are the different measures used in internal control and how they are applied in e-commerce companies?. To answer this question, the review of articles published in Scopus, Science

Paz Medrano Harrison Jordi
https://orcid.org/0000-0003-3201-109X

Mendoza de los Santos Alberto Carlos
https://orcid.org/0000-0002-0469-915X

✉ Lecca Rengifo Luis Rolando / llecca@unitru.edu.pe
https://orcid.org/0000-0003-1005-1744

1 Escuela de Ingeniería de Sistemas Universidad Nacional de Trujillo - Trujillo - Perú

Direct and IEEE Xplore, was conducted from 2018 to 2023.

Keywords: Internal control, Data protection, E-commerce, Privacy.

Introducción

En la actualidad, según (OECD, 2019), la mayoría de las empresas tienen una presencia en línea a través de sus sitios web y aplicaciones móviles. Con el auge del comercio electrónico, cada vez más empresas confían en estos medios digitales para interactuar con sus clientes y realizar transacciones comerciales. Sin embargo, también es cierto que estos canales digitales presentan vulnerabilidades que pueden poner en riesgo la seguridad y privacidad de los datos de los clientes y la empresa en sí misma.

Se sabe que las aplicaciones pueden recopilar información confidencial a través de fuentes de entrada no estructuradas para eludir los controles de privacidad. Como resultado, los usuarios no pueden determinar el impacto en la privacidad de las aplicaciones al descargarlas e instalarlas en dispositivos móviles. (Mackenzie Lewis & Omoronyia Inah, 2020)

(Mackenzie Lewis & Omoronyia Inah, 2020) Identificar las partes sensibles a la seguridad es una parte importante de una investigación de privacidad de la aplicación. Sin embargo, hay que investigar su capacidad para detectar malware por sí solo, ya que el malware tiene una familia diferente y, por lo tanto, exhibe un comportamiento diferente al depender de entradas sensibles a la seguridad para volverse malicioso.

Creer que el tráfico cifrado es seguro en un mundo donde las empresas de comercio electrónica cada vez más del Internet es un malentendido constantemente común que no es cierto. (Lueck Marc, 2021), además el tema que enfrenta el mundo por el COVID es un acelerador para adoptar nuevas medidas que protejan las empresas del comercio electrónico. (Tam Tracy et al., 2021)

El comercio electrónico está bajo presión para brindar un mejor servicio de manera constante en medio de una dura competencia comercial. Una de las formas más populares de hacer esto es aprovechando los datos de los clientes. A pesar de sus beneficios, hacer uso de los datos de los clientes puede conducir a violaciones de la privacidad que hacen que los clientes establezcan barreras más altas para proteger su privacidad. (Mulia Rafiqa Amini et al., 2020)

Entonces el control interno es un conjunto de políticas y procedimientos que se implementan dentro de una organización para asegurar que se cumplan los objetivos y se eviten o detecten errores o fraudes. En el contexto del comercio electrónico, el control interno se utiliza para garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información.

Esta revisión sistemática examina las medidas de control interno utilizadas en las empresas de e-commerce para preservar la seguridad de los datos. Se discuten los diferentes enfoques y medidas utilizados en el control interno, y se proporciona una visión general de las mejores prácticas para su uso efectivo.

Dentro del marco descriptivo se propone responder las siguientes preguntas: ¿Cuáles son las diferentes medidas utilizadas en el control interno y cómo se aplican para preservar la seguridad de los datos dentro de las empresas de comercio electrónico?, ¿Cuáles son los beneficios y limitaciones de las medidas de control interno en el contexto del comercio electrónico?, de esta manera proporcionar información útil para las empresas de e-commerce sobre las medidas efectivas de control interno para proteger sus datos y activos.

Metodología

Preguntas de Investigación:

Para esta revisión se busca responder las siguientes preguntas:

Preguntas de Investigación	Motivación
RQ1: ¿Cuáles son las diferentes medidas utilizadas en el control interno y cómo se aplican para preservar la seguridad de los datos dentro de las empresas de comercio electrónico?	*Proporcionar información útil para las empresas de e-commerce sobre las medidas efectivas de control interno para proteger sus datos y activos.*
RQ2: ¿Cuáles son los beneficios y limitaciones de las medidas de control interno en el contexto del comercio electrónico?	*Entender los beneficios y limitaciones de estas medidas para que las empresas puedan tomar decisiones sobre qué medidas implementar.*

Procesos de recolección de información:

Para la presente revisión sistemática se busca toda información relacionada con el objetivo general planteado que nos permite dar un conocimiento de la relación estrecha que existe entre la auditoría y la protección de datos de los e-commerce.

Para ello, se han tomado artículos de las siguientes revistas: SCOPUS y SCIENCE DIRECT, IEE EXPLORE; de las cuales han sido seleccionadas algunos artículos que cumplan con proporcionar calidad a la investigación.

Criterio de elegibilidad:

Para la presente investigación se han tomado diferentes artículos de revistas indexadas de español e inglés y se ha excluido a todo documento que presente como título de documento el término "tesis". Además, se han excluido documentos que no estén relacionados a los siguientes términos: "auditoría" o sinónimos, "control", "medidas". Así mismo se busca que las fuentes sean de los últimos 6 años.

Los documentos relacionados a política o leyes gubernamentales relacionados a la protección de datos en sus respectivos países fueron excluidos de las fuentes recolectadas, exceptuando aquellas que se enfoquen en mencionar los controles a las cuales se hace mención. Si bien muchas normativas tomadas en los controles internos siguen estas leyes, estos artículos no se enfocan con el objetivo de la investigación, siendo este un punto primordial para tomar en cuenta.

Tipo de estudio:

Para está revisión sistemática se hizo uso de la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), la cual nos indica hacer una pregunta para establecer el rumbo de la investigación, la pregunta planteada fue: ¿Cuáles son las diferentes medidas utilizadas en el escaneo de vulnerabilidades y cómo se aplican en las empresas de comercio electrónico?

Fundamentos de la metodología:

Para Monero y otros (2018), las revisiones sistémicas son resúmenes claros y estructurados de la información disponible orientada a responder una pregunta clínica específica. Dado que están constituidas por múltiples artículos y fuentes de información, representan el más alto nivel de evidencia dentro de la jerarquía de la evidencia. Las revisiones sistemáticas se caracterizan por tener y describir el proceso de elaboración transparente y comprensible para recolectar, seleccionar, evaluar críticamente y resumir toda la evidencia disponible con respecto a la efectividad de un tratamiento, diagnóstico, pronóstico, etc.
Teniendo en cuenta esta definición se realizaron los siguientes pasos:

1. Se identificó el título de la revisión sistemática y justificación de la revisión sistemática.
2. Se especificaron los criterios de inclusión y exclusión para la búsqueda.
3. Se describieron los resultados de los procesos de búsqueda y selección de la misma.
4. Se interpretaron los datos para dar respuesta a las preguntas anteriormente planteadas.

Proceso de búsqueda:

Para la recolección de artículos en las diferentes bases de datos se utilizaron diferentes fórmulas que aseguren una calidad óptima en los artículos seleccionados.

En "SCOPUS":

Para la presente revista se han recolectado 14 artículos siguiendo la fórmula:

(TITLE-ABS-KEY (" control") AND TITLE-ABS-KEY ("e-commerce") AND TITLE-ABS-KEY ("data protection") AND NOT TITLE-ABS-KEY ("law") AND NOT TITLE-ABS-KEY ("politic*")) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp"))

En Sciencie of Direct:

En la presente base de datos se realizó una búsqueda con aplicación de filtros, donde la fórmula principal fue: ""e-commerce"+"data protection "+" control"" y los filtros aplicados fueron: Año de publicación (2017-2022), Tipo de artículo (Artículos de revisión y artículos de investigación), Áreas de tema (Ciencias de la computación); dándonos un total de 281 artículos encontrados.

En IEEE xplore:

En esta base de datos se usó la fórmula: ("All Metadata": e-commerce) AND ("All Metadata": control) NOT ("All Metadata": law*) AND ("All Metadata":data protection), desde el año 2018 hasta el 2023 encontrándose 11 publicaciones (10 conferencias y 1 revista)

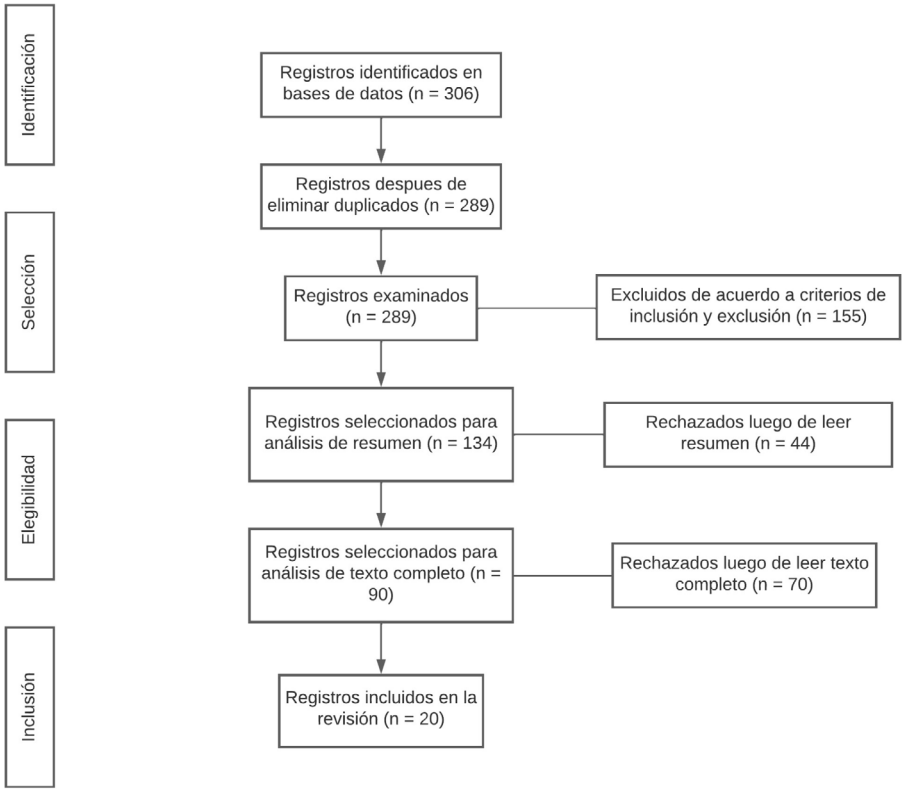


Fig.1 *Diagrama de selección de los artículos tomados para la presente revisión sistemática*

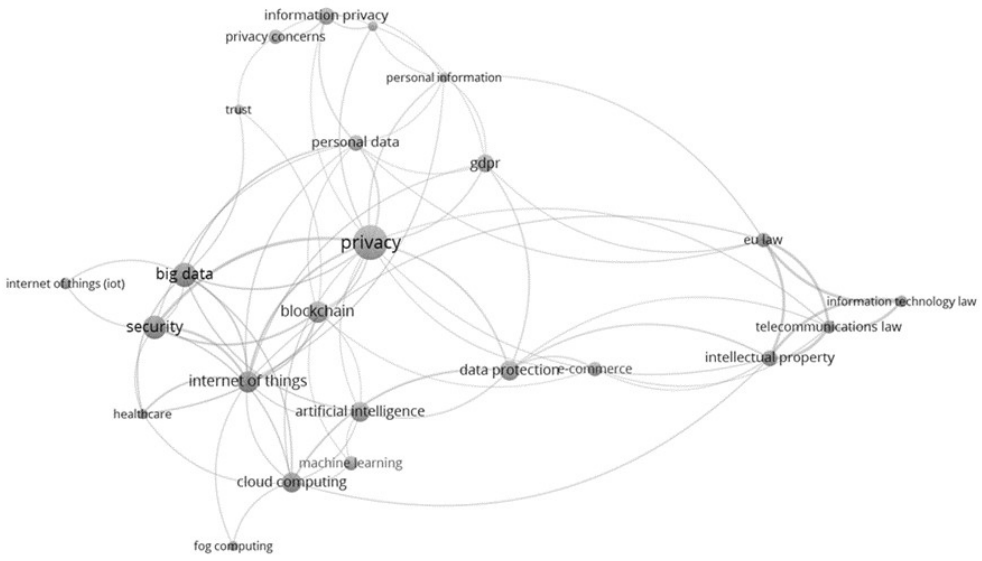


Fig.2 *Mapa de coocurrencia de palabras clave de un total de 281 artículos encontrados en Science Direct*

En la Fig.2 se logra observar todas las diferentes palabras clave que el software VosViewer puede recolectar de las 281 fuentes de los artículos de Science Direct, encontrándose muchos términos tecnológicos que se han tomado en cuenta en los últimos 5 años, siendo el principal nodo de todos estos la palabra "privacidad" que se extiende en 4 ramas, dejándonos en claro la relación estrecha de estos términos con los temas de privacidad de datos en las empresas de e-commerce de la actualidad.

Resultados

Luego de la recolección de todas las fuentes podemos encontrar las siguientes características de las fuentes:

Tabla 1. Tabla de autores y títulos de los artículos seleccionados:

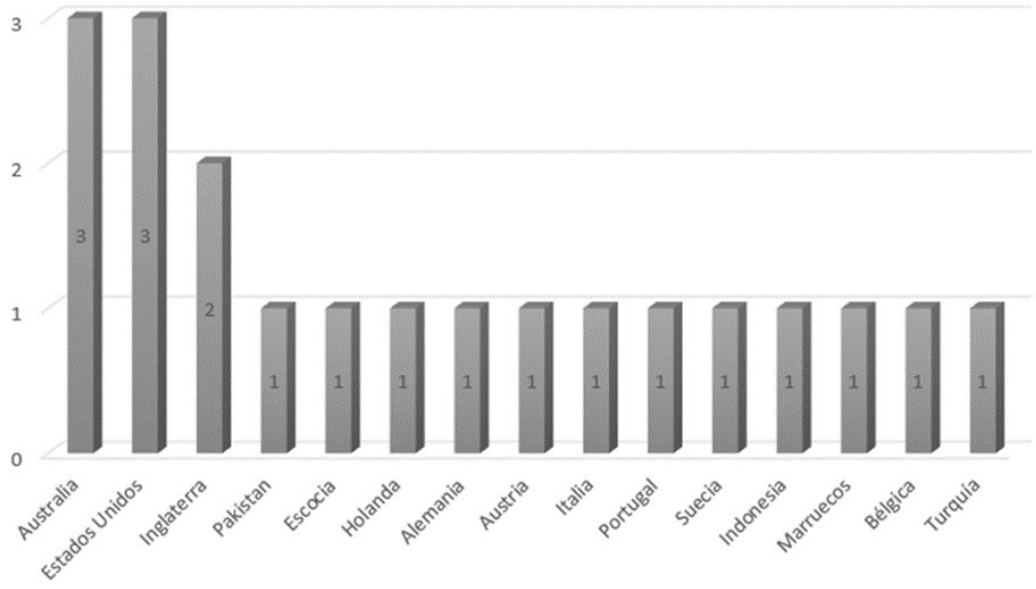
N°	Autor	País	Título de publicación	Año
1	*Fagioli, Alex*	*Inglaterra*	*Recuperación de día cero: la clave para mitigar la amenaza del ransomware*	*2019*
2	*Walee, Abdul; Jamali, Abdul Fareed; Masood, Amar*	*Pakistan*	*¿Qué IDS de código abierto? Snort, Suricata o Zeek*	*2022*
3	*Mackenzie, Lewis; Omoronyia, Inah; Olukoya, Oluwafemi*	*Escocia*	*Hacia el uso de solicitudes de entrada de usuario no estructuradas para la detección de malware*	*2020*
4	*Slokom, Manel; Hanjalic, Alan; Larson, Martha*	*Holanda*	*Hacia una privacidad orientada al usuario para los datos del sistema de recomendación: Un enfoque basado en la personalización para la ofuscación del género para los perfiles de usuario*	*2021*
5	*Lueck, Marc*	*Inglaterra*	*Los siete mitos de la exploración del tráfico cifrado*	*2021*

Continuación Tabla 1

Tabla 1. Tabla de autores y títulos de los artículos seleccionados:

N°	Autor	País	Título de publicación	Año
6	Frick Nicholas, R. J.; Wilms, Konstantin L.; Brachten, Florian; Hetjens, Teresa; Stieglitz, Stefan; Ross, Björn	Alemania	La percepción de la vigilancia de las conversaciones a través de los dispositivos inteligentes	2021
7	Treiblmaier, Horst; Sillaber, Christian	Austria	El impacto de blockchain en el comercio electrónico: Un marco para los temas de investigación más destacados	2021
8	Tam, Tracy; Rao, Asha; Hall, Joanne	Australia	Lo bueno, lo malo y lo que falta: Una revisión narrativa de las implicaciones de la ciberseguridad para las pequeñas empresas australianas	2021
9	Sicari, Sabrina; Rizzardi, Alessandra; Coen-Porisini Alberto	Italia	Problemas y desafíos de seguridad y privacidad en las bases de datos NoSQL	2022
10	Sobitha, Ahila S.; Shunmuganathan, K.L.	Estados Unidos	Papel de la tecnología de agentes en la minería del uso de la web: Recomendación basada en la encriptación homomórfica para aplicaciones de comercio electrónico	2018
11	Fernandes, Teresa; Pereira, Nuno	Portugal	Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online?	2021
12	Makhdoom I.; Zhou I.; Abolhasan M.; Lipman J.; Ni W.	Australia	PrivySharing: Un marco basado en blockchain para la preservación de la privacidad y el intercambio seguro de datos en las ciudades inteligentes	2020
13	Lwakatare, Lucy Ellen; Raj, Aiswarya; Crnkovic, Ivica; Bosch, Jan; Olsson, Helena Holmström	Suecia	Sistemas de aprendizaje automático a gran escala en entornos industriales reales: Una revisión de los desafíos y soluciones	2020
14	Akanfe, Oluwafemi; Valecha Rohit; Rao H. Raghav	Estados Unidos	Evaluación del riesgo de privacidad a nivel de país para los sistemas de pago digitales	2020
15	Mulia Rafiqa, Amini; Azzahro, Fatimah; Handayani Putu Wuri	Indonesia	Análisis de los factores internos y externos que afectan a la preocupación por la privacidad en línea en el comercio electrónico: Estudio comparativo por género	2020
16	Gahi, Youssef; Alaoui, Imane El	Marruecos	Un enfoque seguro de base de datos como servicio para la privacidad de la computación en nube	2019
17	Van Looy Amy	Bélgica	Un estudio cuantitativo y cualitativo del vínculo entre la gestión de los procesos empresariales y la innovación digital	2021
18	Formosa, Paul; Wilson, Michael; Richards Deborah	Australia	Un marco principista para la ética de la ciberseguridad	2021
19	Osman, Ibrahim H.; Anouze, Abdel Latef; Irani Zahir; Lee, Habin; Medeni Tunç D.; Weerakkody, Vishanth	Turquía	Un marco de gestión de análisis cognitivo para la transformación de los servicios de la administración electrónica desde la perspectiva de los usuarios para crear valores compartidos sostenibles	2019
20	Yun Haejung; Lee Gwanhoo; Kim Dan J	Estados Unidos	Una revisión cronológica de la investigación empírica sobre la preocupación por la privacidad de la información personal: Un análisis de los contextos y los constructos de investigación	2020

Fig.3 *Distribución del número de publicaciones según cada país*



Entidades del estado y empresas en la actualidad utilizan redes para una variedad de tecnologías, como el uso compartido de archivos, el acceso remoto, la protección de datos y demás tecnologías informáticas. Firewall y detección y prevención de intrusión son soluciones de seguridad más populares que se usan en conjunto (Waleed et al., 2022).

Las soluciones de ciberseguridad diseñadas para probar la respuesta a eventos debilitantes requieren un entorno de prueba seguro. (Tam Tracy et al., 2021)

De acuerdo a (Sicari Sabrina et al., 2022) refiriéndose a las bases de datos NoSQL que se están implementando en la actualidad en muchas empresas para mejorar su arquitectura interna en los datos que la fragmentación de bases de datos plantea muchos riesgos de seguridad debido a su naturaleza distribuida y estas están relacionadas con el almacenamiento no cifrado, la exposición no autorizada, las copias de seguridad y la inseguridad a través de la red.

Así mismo en la actualidad los dispositivos IoT tienen una vulnerabilidad a un gran número de ataques a la seguridad y la privacidad, aunque los mismos fabricantes conocen estas amenazas, desafortunadamente la seguridad en los dispositivos IoT es descuidada, en este sentido, si hablamos de una red de ciudad inteligente, esta misma, sufre numerosos problemas de seguridad y privacidad que atentan contra lo primordial que debe de proteger las empresas del sector e-commerce, los datos.(Makhdoom I. et al., 2020)

Tabla 2. Tabla de amenazas y medidas aplicadas según fuentes

Fuente	Amenaza	Tipo de Control interno informático	Medida referenciada
1, 2, 3, 5,7,9, 16, 18	*Ransomware o robo de información*	*Detección*	*Ejecución de software de detección de intrusiones*
4, 7, 10, 15	*Toma de control del sistema*	*Prevención*	*La ofuscación de código*

Continuación Tabla 2

Fuente	Amenaza	Tipo de Control interno informático	Medida referenciada
6, 11	*Ransomware o robo de información*	*Prevención*	*Vigilancia en el uso de los sistemas*
8, 9, 15, 20	*Ransomware o robo de información*	*Prevención*	*Entorno de prueba de software*
14, 17	*Uso indebido de la información*	*Prevención*	*Aplicación de nuevas políticas de uso de datos*

Discusión

En esta revisión sistemática se analizó el uso de medidas de control interno en empresas de comercio electrónico para preservar la seguridad de los datos. Se identificaron varias medidas de control interno que son ampliamente utilizadas en la industria.

A continuación, se responderá a la pregunta de investigación planteada:

RQ1: ¿Cuáles son las diferentes medidas utilizadas en el control interno y cómo se aplican para preservar la seguridad de los datos dentro de las empresas de comercio electrónico?

Una de las medidas más comunes es la ejecución de software de detección de intrusiones. Esta medida es esencial en la protección de los datos en las empresas de comercio electrónico. Este tipo de software puede ser utilizado para monitorear la actividad en tiempo real en los sistemas y detectar cualquier actividad sospechosa que pueda indicar una posible violación de seguridad.

El software de detección de intrusiones también puede utilizar técnicas de aprendizaje automático para identificar patrones de comportamiento malicioso y predecir posibles ataques en el futuro. Además, este tipo de software puede ayudar a los equipos de seguridad de la empresa a responder rápidamente a las amenazas de seguridad y tomar medidas para minimizar el daño potencial.

Otra medida es la ofuscación de código; esta técnica es utilizada para dificultar la lectura y la comprensión del código fuente de un software por parte de personas no autorizadas, lo que puede ayudar a proteger la propiedad intelectual, evitar la ingeniería inversa y dificultar el análisis de vulnerabilidades por parte de posibles atacantes.

Existen varias técnicas de ofuscación de código, desde simples reemplazos de nombres de variables hasta técnicas más avanzadas como la transformación de código a través de algoritmos matemáticos. En general, la idea es hacer que el código fuente sea lo más difícil posible de leer y entender sin afectar su funcionalidad.

Otra medida es la vigilancia en el uso de los sistemas. Esto puede incluir el monitoreo de las transacciones de los clientes, el monitoreo del tráfico de red y el análisis de registros de eventos.

Al monitorear la actividad en los sistemas, las empresas pueden detectar patrones sospechosos o inusuales que puedan indicar una posible amenaza de seguridad, como un intento de acceso no autorizado o una actividad de phishing. Una vez que se detecta la actividad sospechosa, la empresa puede tomar medidas para mitigar cualquier posible riesgo, como bloquear el acceso de la fuente sospechosa o notificar a los equipos de seguridad para que investiguen más a fondo.

Además, la vigilancia en el uso de los sistemas también puede ayudar a identificar cualquier comportamiento inusual por parte de los empleados, lo que puede indicar un problema de seguridad interno. Al monitorear la actividad de los empleados en los sistemas de la empresa, las empresas pueden detectar comportamientos sospechosos, como la descarga de grandes

cantidades de datos o el acceso a áreas del sistema que no están relacionadas con su trabajo. Estas señales pueden ser indicativas de una posible violación de seguridad por parte de un empleado y la empresa puede tomar medidas para investigar y remediar la situación.

Otra medida es los entornos de prueba de software, estos son un componente esencial en el ciclo de vida del desarrollo de software en el comercio electrónico. Estos entornos proporcionan un ambiente controlado donde se pueden probar las aplicaciones y sistemas antes de su implementación en producción. En los entornos de prueba, se pueden simular diferentes escenarios y situaciones que permiten identificar problemas y riesgos de seguridad antes de que el software se lance al mercado. Por ejemplo, se pueden realizar pruebas de penetración para evaluar la capacidad de la aplicación para resistir ataques externos, así como pruebas de vulnerabilidad para identificar posibles vulnerabilidades en el sistema.

Además, los entornos de prueba también son útiles para la identificación de problemas de calidad del software, lo que incluye errores de programación y fallos de seguridad. Los equipos de desarrollo pueden usar los resultados de estas pruebas para corregir los problemas identificados antes de que la aplicación sea lanzada al público.

Por último, se encontró que la aplicación de políticas de uso de datos es una parte crucial de la gestión de la seguridad de los datos en el comercio electrónico. Estas políticas deben especificar claramente cómo se recopilan, utilizan y protegen los datos del cliente. También deben especificar quién tiene acceso a estos datos y cómo se pueden utilizar.

Además, las políticas de uso de datos deben ser actualizadas regularmente para asegurarse de que se adapten a los cambios en el negocio y en el entorno de seguridad. Esto puede incluir cambios en las regulaciones de privacidad de datos, nuevas amenazas de seguridad o cambios en la forma en que se utilizan los datos.

Es importante que estas políticas se comuniquen claramente a todos los empleados y se implementen de manera efectiva. Esto puede incluir la formación de los empleados sobre las políticas y la realización de auditorías regulares para garantizar el cumplimiento.

En general, estas medidas de control interno son esenciales para garantizar la seguridad y privacidad de los datos en el comercio electrónico.

Las empresas de comercio electrónico deben implementar medidas de control interno efectivas y actualizarse regularmente para mitigar los riesgos de seguridad y garantizar una experiencia segura y confiable para sus clientes.
RQ2: ¿Cuáles son los beneficios y limitaciones de las medidas de control interno en el contexto del comercio electrónico?

En cuanto a los beneficios, las medidas de control interno pueden ayudar a proteger la información confidencial, reducir el riesgo de fraude y mejorar la calidad del servicio ofrecido por la empresa de comercio electrónico.

Además, la implementación de medidas de control interno también puede ayudar a las empresas de comercio electrónico a cumplir con los requisitos legales y regulatorios, lo que puede ser especialmente importante en el contexto de la privacidad de datos y la protección del consumidor.

Sin embargo, es importante tener en cuenta que también existen limitaciones en la implementación de medidas de control interno en el contexto del comercio electrónico. Por ejemplo, la aplicación de medidas de control interno puede requerir una inversión significativa en recursos, como tecnología y personal capacitado en seguridad informática.

Además, algunas medidas de control interno pueden afectar negativamente la experiencia del usuario, como la introducción de controles

de seguridad adicionales que puedan ralentizar el proceso de compra. También puede haber limitaciones en la capacidad de las medidas de control interno para proteger contra amenazas emergentes y sofisticadas, como los ataques de hackers más avanzados.

En resumen, la implementación de medidas de control interno puede brindar numerosos beneficios a las empresas de comercio electrónico en términos de protección de datos y cumplimiento normativo, pero también pueden tener algunas limitaciones, incluyendo costos y posibles impactos negativos en la experiencia del usuario. Es importante que las empresas de comercio electrónico consideren cuidadosamente las medidas de control interno que implementan y evalúen regularmente su efectividad y eficiencia.

Conclusiones

Podemos concluir que es importante tener en cuenta una variedad de enfoques para garantizar la seguridad de los datos y la protección de la privacidad del cliente.

La ejecución de software de detección de intrusiones, la ofuscación de código, la vigilancia en el uso de los sistemas, el entorno de prueba de software y la aplicación de nuevas políticas de uso de datos son algunas de las medidas de control interno más comunes utilizadas en el comercio electrónico. Cada una de estas medidas aborda diferentes aspectos de la seguridad de los datos y puede ser efectiva cuando se implementa correctamente.

Es importante destacar que la seguridad en el comercio electrónico es un tema crítico que requiere atención constante. Los avances en tecnología y la evolución de las amenazas de seguridad hacen que la implementación de medidas de control interno sea cada vez más compleja y es necesario estar al día con las últimas tendencias y mejores prácticas.

Es importante destacar que el control interno no solo es importante para el comercio electrónico, sino también para el "digital commerce" en general. El "digital commerce" puede incluir una amplia gama de actividades comerciales, como el marketing digital, la publicidad en línea y la venta de productos digitales. Todas estas actividades también requieren medidas adecuadas de control interno para garantizar la seguridad de los datos y la privacidad de los clientes.

Por lo tanto, se invita a otros investigadores a explorar las medidas de control interno en el "digital commerce" y su importancia para garantizar la seguridad de los datos en un mundo cada vez más digital.

Referencias bibliográficas

Akanfe Oluwafemi, Valecha Rohit, & Rao H. Raghav. (2020). Assessing country-level privacy risk for digital payment systems. Computers & Security, 99, 102065. https://doi.org/10.1016/j.cose.2020.102065

OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264245471-en

Fagioli, A. (2019). Zero-day recovery: The key to mitigating the ransomware threat. Computer Fraud & Security, 2019(1), 6-9. https://doi.org/10.1016/S1361-3723(19)30006-5

Fernandes Teresa & Pereira Nuno. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? Telematics and Informatics, 65, 101717. https://doi.org/10.1016/j.tele.2021.101717

Formosa Paul, Wilson Michael, & Richards Deborah. (2021). A principlist framework for cybersecurity ethics. Computers & Security, 109, 102382. https://doi.org/10.1016/j.cose.2021.102382

Frick Nicholas R. J., Wilms Konstantin L., Brachten Florian, Hetjens Teresa, Stieglitz Stefan, & Ross Björn. (2021). The perceived surveillance of conversations through smart devices. Electronic Commerce Research and Applications, 47, 101046. https://doi.org/10.1016/j.elerap.2021.101046

Gahi Youssef & Alaoui Imane El. (2019). A Secure Multi-User Database-as-a-Service Approach for Cloud Computing Privacy. Procedia Computer Science, 160, 811-818. https://doi.org/10.1016/j.procs.2019.11.006

Lueck Marc. (2021). The seven myths of encrypted traffic scanning. Network Security, 2021(7), 9-12. https://doi.org/10.1016/S1353-4858(21)00075-1

Lwakatare Lucy Ellen, Raj Aiswarya, Crnkovic Ivica, Bosch Jan, & Olsson Helena Holmström. (2020). Large-scale machine learning systems in real-world industrial settings: A review of challenges and solutions. Information and Software Technology, 127, 106368. https://doi.org/10.1016/j.infsof.2020.106368

Mackenzie Lewis & Omoronyia Inah. (2020). Towards using unstructured user input request for malware detection. Computers & Security, 93, 101783. https://doi.org/10.1016/j.cose.2020.101783

Makhdoom I., Zhou I., Abolhasan M., Lipman J., & Ni W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers and Security, 88. Scopus. https://doi.org/10.1016/j.cose.2019.101653

Moreno, Begoña, Muñoz, Maximiliano, Cuellar, Javier, Domancic, Stefan, & Villanueva, Julio. (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

Mulia Rafiqa Amini, Azzahro Fatimah, & Handayani Putu Wuri. (2020). Analysis of Internal and External Factors Affecting Online Privacy Concern in E-commerce: Comparative Study by Gender. 2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS), 187-192. https://doi.org/10.1109/ICACSIS51025.2020.9263227

Osman Ibrahim H., Anouze Abdel Latef, Irani Zahir, Lee Habin, Medeni Tunç D., & Weerakkody Vishanth. (2019). A cognitive analytics management framework for the transformation of electronic government services from users' perspective to create sustainable shared values. European Journal of Operational Research, 278(2), 514-532. https://doi.org/10.1016/j.ejor.2019.02.018

Sicari Sabrina, Rizzardi Alessandra, & Coen-Porisini Alberto. (2022). Security&privacy issues and challenges in NoSQL databases. Computer Networks, 206, 108828. https://doi.org/10.1016/j.comnet.2022.108828

Slokom Manel, Hanjalic Alan, & Larson Martha. (2021). Towards user-oriented privacy for recommender system data: A personalization-based approach to gender obfuscation for user profiles. Information Processing & Management, 58(6), 102722. https://doi.org/10.1016/j.ipm.2021.102722

Sobitha Ahila S. & Shunmuganathan K.L. (2016). Role of Agent Technology in Web Usage Mining: Homomorphic Encryption Based Recommendation for E-commerce Applications. Wireless Personal Communications, 87(2), 499-512. Scopus. https://doi.org/10.1007/s11277-015-3082-y

Tam Tracy, Rao Asha, & Hall Joanne. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security, 109, 102385. https://doi.org/10.1016/j.cose.2021.102385

Treiblmaier Horst & Sillaber Christian. (2021). The impact of blockchain on e-commerce: A framework for salient research

topics. Electronic Commerce Research and Applications, 48, 101054. https://doi.org/10.1016/j.elerap.2021.101054

Van Looy Amy. (2021). A quantitative and qualitative study of the link between business process management and digital innovation. Information & Management, 58(2), 103413. https://doi.org/10.1016/j.im.2020.103413

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS? Snort, Suricata or Zeek. Computer Networks, 213, 109116. https://doi.org/10.1016/j.comnet.2022.109116

Yun Haejung, Lee Gwanhoo, & Kim Dan J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. Information & Management, 56(4), 570-601. https://doi.org/10.1016/j.im.2018.10.001