Impacto de los marcos de gobierno de TI en la seguridad de la información de las organizaciones

Impact of IT governance frameworks on information security in organizations

Luis Rolando Lecca-Rengifo[1], Harrison Jordi Paz-Medrano[2], Alberto Carlos Mendoza de los Santos[3]

Fecha de recepción: 6 de febrero, 2024
Fecha de aprobación: 28 de mayo, 2024

Lecca-Rengifo, L.R; Paz-Medrano, H.J; Mendoza de los Santos, A.C. Impacto de los marcos de gobierno de TI en la seguridad de la información de las organizaciones. *Tecnología en Marcha*. Vol. 38, Nº 1. Enero-Marzo, 2025. Pág. 93-103.

https://doi.org/10.18845/tm.v38i1.7048

1 Escuela de Ingeniería. Universidad Nacional de Trujillo, Perú.
llecca@unitru.edu.pe
https://orcid.org/0000-0003-1005-1744
2 Escuela de Ingeniería. Universidad Nacional de Trujillo, Perú.
hpazm@unitru.edu.pe
https://orcid.org/0000-0003-3201-109X
3 Departamento de Ingeniería. Universidad Nacional de Trujillo, Perú.
amendozad@unitru.edu.pe
https://orcid.org/0000-0002-0469-915X

Palabras clave

Efecto; impacto; marco de gobierno de TI; organización; seguridad de información.

Resumen

Proteger los activos de la empresa es una labor imprescindible de toda organización; realizar planificaciones, controles y todo un despliegue de actividades para salvaguardar la información de las empresas es una función que todo encargado del área tecnológica tiene que estar en constante monitoreo, para ello los marcos de gobierno de TI trazan un rumbo para poder realizar actividades que mejoren todos las áreas de una organización en cuanto al uso de recursos tecnológicos, pero es necesario tener claro en cuanto se mejora. En la presente investigación se evalúa el impacto de los marcos de gobierno de TI en la seguridad de la información de las organizaciones, así como la comparativa entre los marcos de gobierno para poder llegar a la conclusión de que marcos de gobierno de TI son los que mejor ayudan para la preservación de la seguridad de la información.

Keywords

Effect; impact; IT governance framework; organization; information security.

Abstract

Protecting the company's assets is an essential task for any organization; planning, controls and a whole deployment of activities to safeguard the company's information is a function that every person in charge of the technological area has to be constantly monitoring, for this purpose the IT governance frameworks outline a course to be able to carry out activities that improve all the areas of an organization in terms of the use of technological resources, but it is necessary to be clear about how much it is improved. This research evaluates the impact of IT governance frameworks on information security in organizations, as well as the comparative between governance frameworks in order to reach the conclusion that IT governance frameworks are the ones that best help to preserve information security.

Introducción

Las tecnologías de información (TI) son los procesos que se utilizan para poder procesar la información que una organización o empresa maneja para su respectivo análisis y que esto ayude en la toma de decisiones en las acciones que la empresa esté pensando en realizar o implementar, a dicho proceso se le conoce como integración, en donde una organización realiza distintas acciones con el fin de desarrollar un plan que reúna a todos los procesos involucrados en el negocio [1]. Las TI también son un apartado importante con el cual se logra la integración de los procesos de la empresa, la flexibilidad con los procesos de cambio de datos entre otros puntos importantes los cuales nos dan a conocer cómo es que la tecnología al implementarse puede mejorar considerablemente las empresas; otro punto importante de las TI para las empresas es que crezcan en relación a la globalización y digitalización por la que el mundo está atravesando.

El gobierno de TI se describe como una estructura que dirige las relaciones y procesos que se dan dentro de una organización que permiten encaminar dichos procesos hacia el cumplimiento de sus objetivos, para que una empresa pueda implementar TI se debe de seguir como se comentó un marco referencial en el cual basarse para tener un mejor manejo del área de TI en este caso y de los servicios que se pueden presentar en estos; principalmente

tiene algunos marcos referenciales principales que son : COBIT, ITIL ,ISO, TOGAF, etc. [2]. Todos estos marcos tienen características similares en algunos aspectos mientras que en otros son completamente distintas estas decisiones tiene que regirse concretamente de cuáles son los requerimientos que la organización quiere resolver y como es que se va a sustentar económicamente para que se empiece con la adaptación y el control respectivo.

En este sentido, el gobierno de TI tiene un impacto directo e indirecto en la seguridad de la información, ya que contribuye a establecer una cultura de seguridad, a definir una estrategia y una política de seguridad, a asignar recursos y competencias para la seguridad, a evaluar y gestionar los riesgos de seguridad, a monitorear y auditar el desempeño de la seguridad, y a mejorar continuamente la seguridad. En esta revisión se analiza el impacto de los marcos de gobierno de TI en la seguridad de la información de las organizaciones, basándose en los conceptos teóricos y en las evidencias empíricas disponibles.

En esta revisión se analiza el impacto que genera la implementación de los marcos de gobierno de TI en la seguridad de la información de las organizaciones.

Metodología

Preguntas de investigación

En esta revisión se busca responder las siguientes preguntas:

Preguntas de Investigación	Motivación
RQ1: ¿Cuál es el nivel de impacto positivo de la aplicación de los marcos de TI en la seguridad de la información en las organizaciones?	Identificar el nivel de impacto positivo que ha tenido los marcos de TI en la seguridad de la información de las empresas
RQ2: ¿Qué marcos de TI son los más usados para preservar la seguridad de la información las organizaciones?	Identificar que marcos son los más utilizados para la preservación de la seguridad de la información en las empresas

Objetivo general

Determinar el nivel de impacto de los marcos de gobierno de TI en el campo de la seguridad de las organizaciones

Objetivos específicos

- Determinar el impacto positivo de los marcos de gobierno de TI en la preservación de la seguridad de la información de las organizaciones
- Determinar los marcos de gobierno de TI más utilizados para la preservación de la seguridad de la información

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 del impacto que tienen los marcos de gobierno de TI en la seguridad de la información de las organizaciones.

Criterios de elegibilidad

Para la presente investigación se han tomado diferentes artículos de revistas indexadas de español e inglés y se han tomado artículos que sean revisiones sistemáticas e investigaciones. Así mismo se han tomado en cuenta criterios para para su exclusión adicionales:

- Los artículos deben de poseer al menos un término que se relacione con la investigación
- Los artículos tienen que al menos responder a alguna de las preguntas de investigación
- Los artículos deben de tener indicadores cuantitativos y resultados visibles

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: ¿Cuál es el impacto que tienen los marcos de gobierno de TI en la seguridad de la información de las organizaciones?

Fundamentos de la metodología

Las revisiones sistémicas son resúmenes concisos y metódicos de información que tienen como objetivo responder a una pregunta clínica específica. Como constan de varios artículos y fuentes de información, son la forma de evidencia más elevada en una jerarquía. Al utilizar un proceso de desarrollo claro y comprensible, las revisiones sistemáticas tienen como objetivo recopilar, seleccionar para evaluación mediante análisis crítico y resumir toda la evidencia disponible sobre la efectividad del tratamiento (incluida, entre otras, la precisión del diagnóstico), el pronóstico, etc. [3]

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.

Procesos de búsqueda

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 los marcos de TI y su impacto en la seguridad de la información de las organizaciones

Para ello, se han tomado artículos de las siguientes revistas: DOAJ, REDALYC, DIALNET, SCOPUS, SCIENCE DIRECT de las cuales han sido seleccionadas algunos artículos que cumplan con proporcionar calidad a la investigación. Dicha selección se muestra en el siguiente diagrama de embudo que sigue el modelo prisma.

El gráfico de la Fig.01 muestra las etapas de selección los artículos, en la etapa 1 se seleccionan todos aquellos que nos trajeron como resultados de aplicar una fórmula de búsqueda en las diferentes bases de datos, en la etapa 2 se quitaron de la lista inicial aquellos artículos donde el título no tenga relación con el tema de investigación y los elementos duplicados si existiesen, en la etapa 3 se excluyeron aquellos artículos donde el resumen no tenga relación alguna con el tema a investigar, dándonos como resultado un total de 24 artículos seleccionados para realizar la revisión.

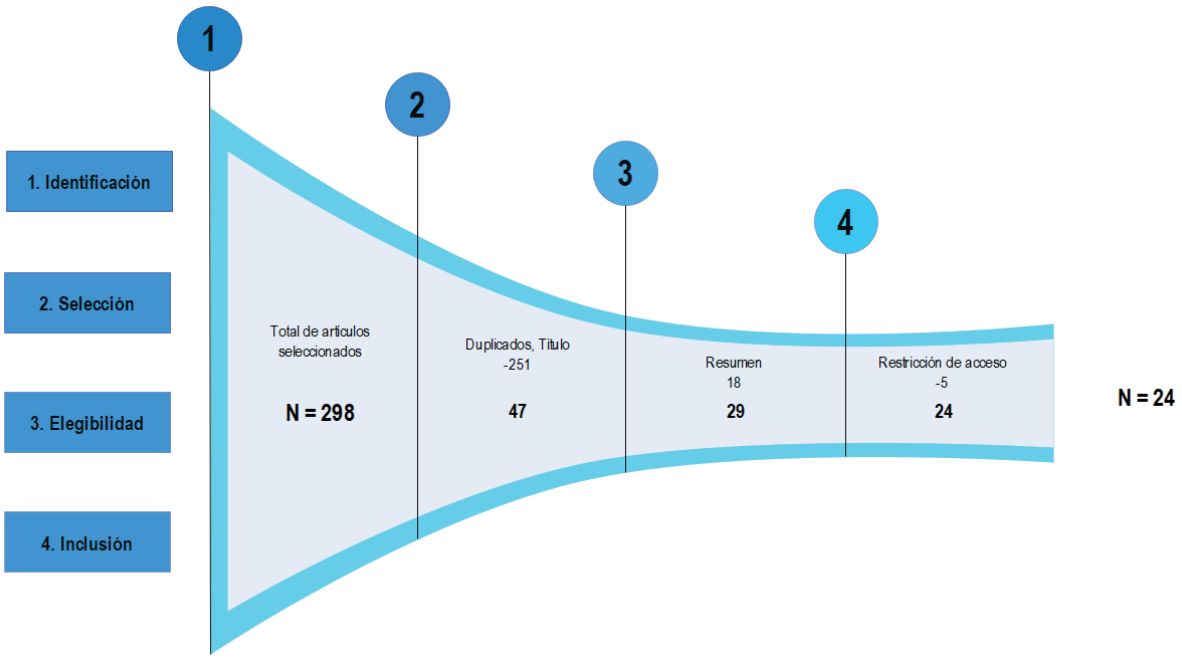

Figura 1. Diagrama de embudo del proceso de selección de los artículos tomados para la presente revisión sistemática

Criterio de elegibilidad

Para la presente investigación se han tomado diferentes artículos de revistas indexadas de español e inglés y se han tomado artículos que sean revisiones sistemáticas e investigaciones. Así mismo se han tomado en cuenta criterios para para su exclusión adicionales:

- Los artículos deben de poseer al menos un término que se relacione con la investigación
- Los artículos tienen que al menos responder a alguna de las preguntas de investigación
- Los artículos deben de tener indicadores cuantitativos y resultados visibles

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.

DOAJ

“IT governance” AND “challenges” AND “organization”

“IT governance” AND “challenges” AND “information security”

REDALYC

“IT governance” AND “challenges” AND “information security” AND “organization” AND “data processing”.

Aplicando filtro (disciplina de ingeniería y computación)

SCIENCE DIRECT

"IT governance" AND "challenges" AND "information security" AND "organization" AND "data processing" AND "effects".

Aplicando algunos filtros a los resultados

- Primer filtro (Área: Computer Science)
- Segundo filtro (Open access & Open archive)
- Tercer filtro (Artículos de investigación)

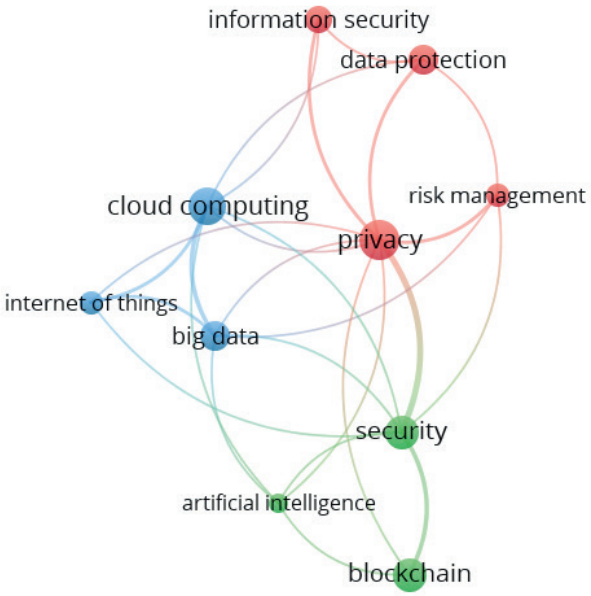

Figura 2: Mapa de coocurrencia de palabras clave de un total de 218 artículos encontrados en Science Direct.

SCOPUS

Las fórmulas utilizadas para la búsqueda en Scopus fueron:

TITLE-ABS-KEY ("its government" AND "challenges")

TITLE-ABS-KEY ("IT governance" AND "challenges" AND "information security" AND "organization")

TITLE-ABS-KEY ("IT governance" AND "challenges" AND "information security" AND "effects")

TITLE-ABS-KEY ("IT governance" AND "challenges" AND "information security")

Resultados

N°	Título	Año	Autor (es)	País
1	A software gateway to affordable and effective Information Security Governance in SMMEs	(2013)	J. Coertze, R. Von Solms	Sudáfrica
2	A systems-of-systems security framework for requirements definition in cloud environment	(2019)	S.B.O.G. Carturan, D.H. Goya	Brasil
3	A web-based information security management toolbox for small-to-medium enterprises in Southern Africa	(2011)	J. Coertze, J. Van Niekerk, R. Von Solms	Sudáfrica
4	Analisis Tata Kelola Sistem Informasi Dengan Framework COBIT-5: Studi Kasus Pada PT. Batu Karang	(2020)	Raissa Amanda Putri, Fadhlan Hussaini Srg, Sinta Dewi, Tania Yulindra, Wahyu Herlambang	Indonesia
5	Analyzes and solves the top enterprise network data security issues with the web data mining technology	(2009)	W. Chai	China
6	Cloud Computing and Information Technology Strategy	(2013)	Antonio Mariano Carlos Junior, Cesar Augusto Biancolino, Emerson Antonio Maccari	Chile
7	Cloud Sourcing and Paradigm Shift in IT Governance: Evidence from the Financial Sector	(2020)	N. Kazemargi, P. Spagnoletti	Italia
8	Digital certification in the Brazilian e-government	(2011)	Edilson Ferneda, Luiza Beth Nunes Alonso, Lamartine Vieira Braga	Brasil
9	Enterprise information security, a review of architectures and frameworks from interoperability perspective	(2011)	Marzieh Shariati, Faezeh Bahmani, Fereidoon Shams	Iran
10	Ict Strategic Planning at Public Higher Educational Organizations: Building an Approach Through Action Research at Unirio	(2015)	Luiza Goncalves de Paula, Renata Mendes Araujo, Asterio Kiyoshi Tanaka, Claudia Cappelli	Brasil
11	Improving information exchange processes when implementing the State's information function on the internal level	(2021)	Anatoliy Valerievich Tsaregorodtsev, Sergey Dmitrievich Volkov	Rusia
12	Information security control centralization and IT governance for enterprises	(2008)	R.J. Robles, J.-Y. Park, T.-H. Kim	Korea del Sur
13	Information security governance in big data environments: A systematic mapping	(2018)	Reza Saneei Moghadam, Ricardo Colomo-Palacios	Noruega
14	Information Technology Service Management Processes Maturity in the Brazilian Federal Direct Administration	(2015)	Maria Albeti Vieira Vitoriano, João Souza Neto	Brasil
15	Integration of IT governance and security risk management: A systematic literature review	(2017)	D. De Smet, N. Mayer	Luxemburgo
16	IT governance and IT application orchestration capability role on organization performance during the COVID-19 pandemic: An intervening of business-IT alignment	(2021)	Afrizal Tahar, Hafiez Sofyani, Detra Putri Kunimasari	Indonesia
17	IT Governance restructuring challenges in cloud computing utilizing governmental enterprises	(2020)	Mohammad Reza Taghva, Kamran Feizi, Sayed Gholam hasan Tabatabaei, Mostafa Tamtaji	Irán
18	Major Challenges of Systems-of-Systems with Cloud and DevOps - A Financial Experience Report	(2019)	S.B.O.G. Caraturan, D.H. Goya	Brasil
19	Ontology based modeling for information security management	(2011)	P. Saha, N. Parameswaran, P. Ray, A. Mahanti	India
20	Perceived information security of internal users in Indian IT services industry	(2014)	N.R. Mukundan, L. Prakash Sai	India
21	Performance Measurem Ent of Information Technology Governance in Brazilian Financial Institutions	(2014)	Sara C. Boni Barbosa, Ildeberto Aparecido Rodello, Silvia Inês Dallavalle de Pádua	Brasil
22	Resultados Do 9º Contecsi - Congresso Internacional De Gestão Da Tecnologia E Sistemas De Informação	(2012)	Edson Luiz Riccio, Marici Cristine G. Sakata	Brasil
23	Security in organisations: Governance, risks and vulnerabilities in moving to the cloud	(2017)	M.O. Alassafi, R.K. Hussain,	Reino Unido
24	Should we wear a velvet glove to enforce Information security policies in higher education?	(2022)	H.-J. Kam, D.J. Kim, W. He	Estados Unidos

Posterior a haber revisado los 24 artículos seleccionados, se obtuvieron resultados muy claros con respecto a las preguntas de investigación. Primero observemos la fig.03 que nos indica los países de donde más se han obtenido la información recolectada.

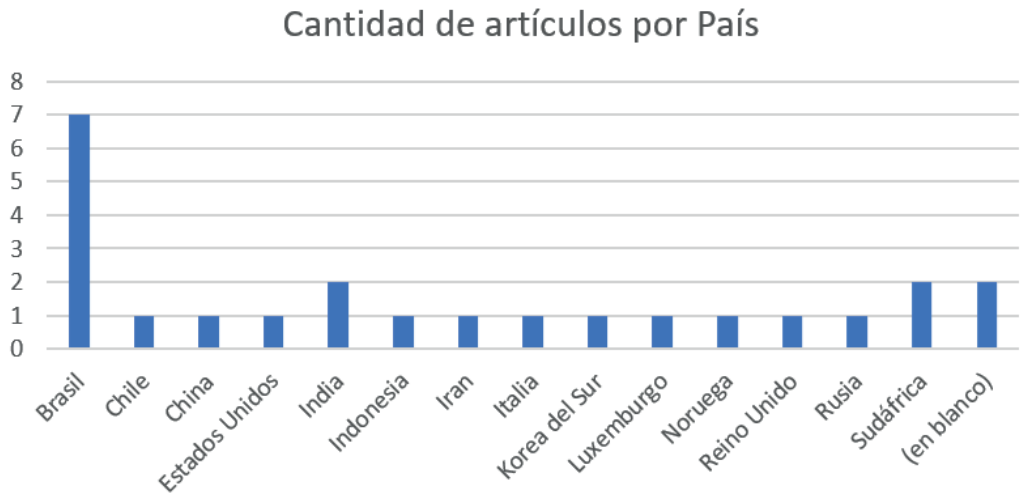

Figura 3. Frecuencia de los artículos por cada país de la lista de artículos seleccionados.

Se puede apreciar de la Fig.03 que el país que más aporto para el presente artículo de revisión es Brasil, con un total de 7 artículos, y luego los demás países tienen al menos 1 articulo seleccionado para su revisión de literatura.

Discusión

Ahora respondiendo a la primera pregunta de la revisión: ¿Cuál es el nivel de impacto positivo de la aplicación de los marcos de TI en la seguridad de la información en las organizaciones?

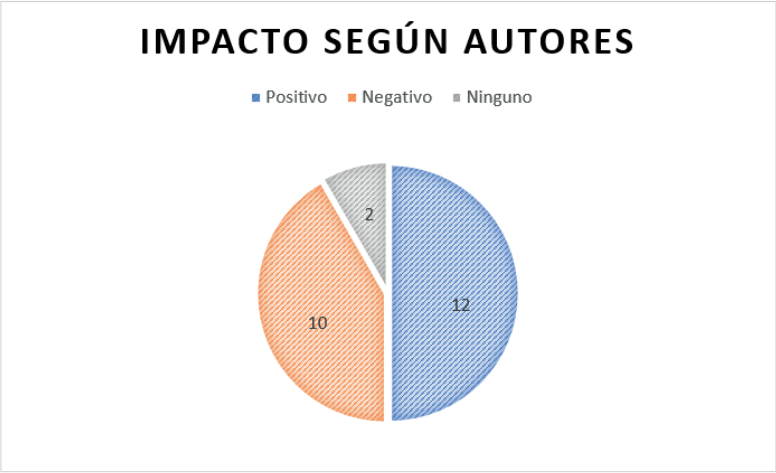

Figura 4. Impacto de los marcos de gobierno de TI según cantidad de artículos.

De acuerdo a la figura 4 se puede inferir que la mayoría de autores indican que la implementación de la guía de seguridad que contiene todo marco de gobierno de TI da un impacto positivo en el manejo interno de todo tipo de organización, así mismo da mecanismos para poder controlarlos y monitorearlos para su futura mejora de acuerdo a cada necesidad.

La implementación de marcos de gobierno de TI conlleva una serie de ventajas sustanciales para las organizaciones. En primer lugar, se destaca la optimización y eficiencia operativa que proporcionan. Estos marcos optimizan procesos internos y la asignación de recursos, lo que se traduce en una notable mejora en la productividad y en la entrega eficiente de servicios de TI. Al estandarizar prácticas y procedimientos, se eliminan redundancias y se logra una gestión más eficaz de los activos de TI.

Además, la seguridad de la información se ve fortalecida significativamente. Los marcos de gobierno de TI suelen incluir directrices y buenas prácticas en materia de seguridad, lo que contribuye a mitigar riesgos y a garantizar la protección de los activos críticos de la organización. La seguridad se convierte en un componente integral de las operaciones de TI, brindando confianza y tranquilidad tanto a la organización como a sus partes interesadas.

Otro aspecto positivo crucial es la alineación estratégica. Estos marcos permiten una alineación efectiva entre las estrategias de TI y los objetivos globales del negocio. Así, la tecnología se utiliza de manera óptima para apoyar y avanzar en la visión y metas organizativas. La TI se convierte en un facilitador estratégico, garantizando que cada acción tecnológica esté alineada con la dirección general de la empresa.

A pesar de los beneficios evidentes, la implementación de marcos de gobierno de TI no está exenta de desafíos. Uno de los aspectos negativos notables es la resistencia al cambio dentro de la organización. La introducción de nuevos procesos y prácticas puede encontrar resistencia por parte de los empleados, lo que puede obstaculizar la adopción exitosa del marco de gobierno de TI.

Otro aspecto negativo se refiere a la inversión inicial requerida. La implementación efectiva de estos marcos puede demandar inversiones considerables en términos de tiempo, recursos financieros y capacitación. Esto puede generar preocupaciones iniciales sobre la rentabilidad y viabilidad a largo plazo de la inversión.

Es fundamental abordar estos desafíos de manera proactiva y planificada para garantizar una adopción exitosa y duradera de los marcos de gobierno de TI en la organización.

Para la segunda pregunta: ¿Qué marcos de TI son los más usados para preservar la seguridad de la información las organizaciones?

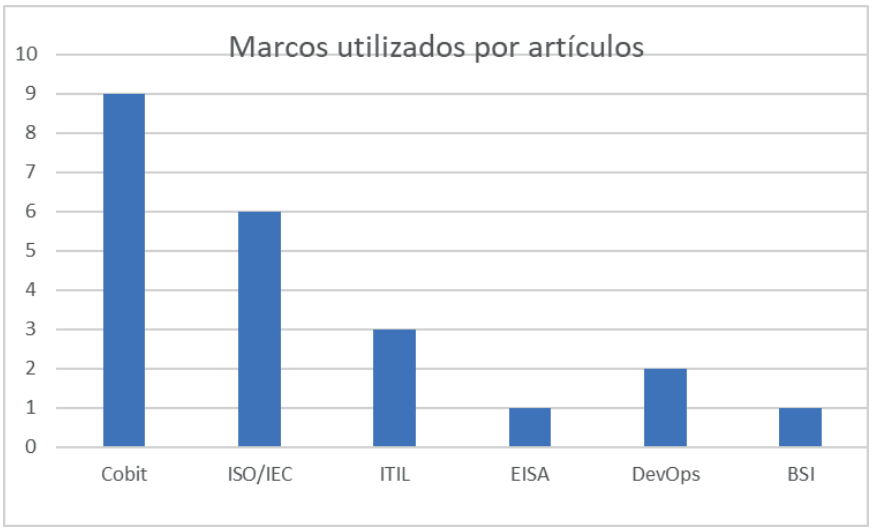

Figura 5. Uso de los framework en los artículos seleccionados.

De acuerdo a la Fig.05 se puede ver que la mayoría de artículos revisados utiliza muchos en particular, algunos usan COBIT 2019, que es el más utilizado. Pero existen otras opciones, así como el marco ISO/IEC, ITIL, etc. que en su mayoría son utilizadas por empresas del rubro tecnológico.

Conclusiones

- Se logró concluir que las implementaciones de los gobiernos de TI en las organizaciones impactan significativamente en la seguridad de los activos de la misma organización.
- Algunos autores refieres que si bien es cierto los marcos de TI son una guía para las buenas prácticas de seguridad de información, estas no son implementadas en todas las organizaciones, debido a que las medianas y pequeñas empresas optan por mejorar sus ingresos y alcanzar sus metas.
- Existe aún poca literatura de qué softwares en específico son las más utilizadas en las empresas para dar soporte a la seguridad en el ámbito gerencial, pero podemos inferir que en la actualidad la gran parte de estas organizaciones están mudando a la computación en la nube para tercerizarla protección de sus activos.

Referencias

[1] C. Ávila, E. J. Chinchilla y T. Velásquez Pérez, «It governance model for state entities, as support for compliance with the information security and privacy component in the framework of the digital government policy,» *Journal of Physics: Conference Series,* vol. 1409, nº 1, 2019.

[2] H. A. F. Cano y D. P. Domínguez, «Modelo de gobierno de tecnología de la información para mejorar el desempeño de proyectos de negocio minorista. Investigación Administrativa,» *Investigación Administrativa,* vol. 47, nº 122, pp. 1-15, 2018.

[3] B. Moreno, M. Muñoz, J. Cuellar, S. Domancic y J. Villanueva, «Revisiones Sistemáticas: definición y nociones básicas,» *Revista clínica de periodoncia, implantología y rehabilitación oral,* vol. 11, nº 3, pp. 184-186, 2018.

[4] M. A. Vieira Vitoriano y J. Souza Neto, «Information Technology Service Management Processes Maturity in the Brazilian Federal Direct Administration,» *Journal of Information Systems and Technology Management,* vol. 12, nº 3, pp. 663-686, 2015.

[5] A. Valerievich Tsaregorodtsev y V. Sergey Dmitrievich, «Improving information exchange processes when implementing the State's information function on the internal level,» *Revista Cubana de Ciencias Informáticas,* vol. 15, pp. 181-198, 2021.

[6] A. Tahar, S. Hafiez y D. Putri Kunisamari, «IT governance and IT application orchestration capability role on organization performance during the COVID-19 pandemic: An intervening of business-IT alignment,» *Jurnal Ilmiah Bidang Akuntansi Dan Manajemen,* vol. 18, nº 1, pp. 1-20, 2021.

[7] M. Shariati, F. Bahmani y F. Shams, «Enterprise information security, a review of architectures and frameworks from interoperability perspective,» *Procedia Computer Science,* vol. 3, pp. 537-543, 2011.

[8] R. Saneei Moghadam y R. Colomo Palacios, «Information security governance in big data environments: A systematic mapping,» *Procedia Computer Science,* vol. 138, pp. 401-408, 2018.

[9] P. Saha, N. Parameswaran, P. Ray y A. Mahanti, «Ontology based modeling for information security management,» Sydney, 2011.

[10] E. L. Riccio y M. C. G. Sakata, «Resultados Do 9o Contecsi—Congresso Internacional De Gestão Da Tecnologia E Sistemas De Informação,» *Journal of Information Systems and Technology Management,* vol. 9, nº 2, pp. 391-436, 2012.

[11] M. Reza Taghva, K. Feizi, S. G. Hasan Tabatabaei y M. Tamtaji, «IT Governance restructuring challenges in cloud computing utilizing governmental enterprises,» *Iranian Journal of Information Processing & Management,* vol. 35, nº 3, pp. 785-816, 2020.

[12] N. R. Mukundan y L. Prakash Sai, «Perceived information security of internal users in Indian IT services industry. Information Technology and Management,» *Information Technology and Management ,* vol. 15, nº 1, pp. 1-8, 2014.

[13] N. Kazemargi y P. Spagnoletti, «Cloud Sourcing and Paradigm Shift in IT Governance: Evidence from the Financial Sector,» *Digital Business Transformation,* vol. 38, pp. 47-61, 2020.

[14] H. J. Kam, D. J. Kim y W. He, «Should we wear a velvet glove to enforce Information security policies in higher education? Behaviour and Information Technology,» vol. 41, nº 10, pp. 2259-2273, 2022.

[15] L. Goncalves de Paula, R. Mendes Araujo, A. Kiyoshi Tanaka y C. Cappelli, «Ict Strategic Planning at Public Higher Educational Organizations: Building an Approach Through Action Research at Unirio,» *Journal of Information Systems and Technology Management,* vol. 12, nº 2, pp. 351-370, 2015.

[16] E. Ferneda, L. B. Nunes Alonso y L. Vieira Braga, «Digital certification in the Brazilian e-government,» *JISTEM: Journal of Information Systems and Technology Management,* vol. 8, nº 2, pp. 331-346, 2011.

[17] D. De Smet y N. Mayer, «Integration of IT governance and security risk management: A systematic literature review,» *International Conference on Information Society (i-Society),* pp. 143-148, 2016.

[18] J. Coertze y R. Von Solms, «A Software Gateway to Affordable and Effective Information Security Governance in SMMEs,» de *Information Security South Africa*, Johannesburg, 2013.

[19] W. Chai, «Analyzes and solves the top enterprise network data security issues with the web data mining technology,» de *2009 First International Workshop on Database Technology and Applications*, Wuhan, 2009.

[20] S. Carturan y D. Goya, «A systems-of-systems security framework for requirements definition in cloud environment,» de *ECSA '19: Proceedings of the 13th European Conference on Software Architecture*, Paris, 2019.

[21] A. M. Carlos Junior, C. A. Biancolino y E. A. Maccari, «Cloud Computing and Information Technology Strategy,» *Journal of Technology Management & Innovation,* vol. 8, nº 1, pp. 178-188, 2013.

[22] S. Caraturan y D. Goya, «Major Challenges of Systems-of-Systems with Cloud and DevOps—A Financial Experience Report,» de *2019 IEEE/ACM 7th International Workshop on Software Engineering for Systems-of-Systems (SESoS) and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (WDES)*, Montreal, 2019.

[23] S. C. Boni Barbosa, I. Aparecido Rodello y S. I. Dallavalle de Padua, «Performance Measurem Ent of Information Technology Governance in Brazilian Financial Institutions,» *Journal of Information Systems and Technology Management,* vol. 11, nº 2, pp. 397-414, 2014.

[24] R. Amanda Putri y F. Hussaini Srg, «Analisis Tata Kelola Sistem Informasi Dengan Framework COBIT-5: Studi Kasus Pada PT. Batu Karang,» *Jurnal Sistem Informasi ,* vol. 4, nº 1, 2020.

[25] M. O. Alassafi, R. K. Hussain, G. Ghashgari, R. J. Walters y G. B. Wills, «Security in organisations: Governance, risks and vulnerabilities in moving to the cloud,» de *Enterprise Security Springer*, 2017, pp. 241-258.

Declaración sobre uso de Inteligencia Artificial (IA)

El autor aquí firmante declara que no se utilizó ninguna herramienta de IA para la conceptualización, traducción o redacción de este artículo.