ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES / Index A LOS AUTORES / To the AUTORS

Vol. 40 (Nº 25) Año 2019. Pág. 5

Importancia de los modelos para el gobierno de la seguridad de la información en las empresas: una revisión sistemática de la literatura

Importance of models for government of information security in companies: a systematic review of the literature

ESPINOZA Mina, Marcos Antonio 1

Recibido: 03/02/2019 • Aprobado: 01/07/2019 • Publicado 22/07/2019

Contenido

RESUMEN:
Uno de los activos más importantes de toda organización actualmente es la información, por lo cual el gobierno de la seguridad de la información (GSI) es cada vez más crucial a medida que aumenta la dependencia de la misma, siendo responsabilidad de la junta directiva y la dirección ejecutiva asegurar este valioso bien. En este artículo se busca, a través de una revisión sistemática, conocer los modelos para el GSI, su aplicación y administración en la organización, y finalmente las herramientas tecnológicas propuestas. Se muestran los niveles jerárquicos en la organización a los que va dirigida esta práctica y los nuevos modelos propuestos.
Palabras clave: Estándares, modelos, tecnología, gobierno corporativo

ABSTRACT:
One of the most important assets of any organization is currently information, which is why the government of information security (GIS) is increasingly crucial as the dependence on it increases, being the responsibility of the board of directors and Executive management ensure this valuable good. This article seeks, through a systematic review, to know the models for the GIS, its application and administration in the organization, and finally the technological tools proposed. The hierarchical levels in the organization to which this practice is directed and the new proposed models are shown.
Keywords: Standards, models, technology, corporate governance

1. Introducción

Las organizaciones han sufrido transformaciones radicales al llegar la era de la información, las diferentes actividades realizadas por las mismas generan permanentemente grupos de información almacenados digitalmente. Es difícil considerar que exista una empresa u

organización que haya permanecido ajena a este avance, el de la tecnología de la información. Por lo cual, cualquier daño a la reserva o integridad de la información puede ser devastador; también puede serlo el hecho de no contar con la información en forma oportuna. Así lo considera Kusumah, Sutikno, & Rosmansyah (2014), al indicar que: las dimensiones de la seguridad de la información en el contexto de la confidencialidad, la integridad y la disponibilidad de la información están siempre en el logro de los objetivos comerciales o los objetivos de la empresa / organización. El diseño e implementación del control de riesgos de seguridad de la información evita la filtración de información, la destrucción de información o la falta de disponibilidad de información.

La seguridad de la información es un asunto corporativo y es por esta razón que la perspectiva correcta para llegar a un cumplimiento regulatorio satisfactorio, es tratando a esta actividad desde un enfoque de gobierno, el cual es transversal en toda la organización no solamente un enfoque hacia los sistemas de información. Será fundamental que un gerente de seguridad de la información incorpore los amplios conocimientos para un gobierno de la seguridad efectiva, así como los elementos y las acciones necesarias para desarrollar una estrategia de seguridad de la información y un plan de acción para su puesta en práctica. Para garantizar la seguridad de la información en una organización, el GSI podría ser una de las estrategias que se pueden implementar (Laksono & Supriyadi, 2015).

La seguridad de la información implica un sistema de gestión y un gobierno efectivo, este gobierno debe presentarse meramente desde el punto de vista de su implementación, ya que el GSI es una parte del gobierno corporativo de las organizaciones. Bajo este contexto, la aplicación de mejores prácticas y modelos, tales como: ISO (International Organization for Standardization), COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library), CMMI (Capability Maturity Model Integration), PMBOK (Project Management Body of Knowledge), OSSTMM (Open Source Security Testing Methodology Manual), entre otros; nos dan los lineamientos claros para establecer el alcance de la implementación. Los problemas de seguridad de la información deben resolverse a fondo. Por lo tanto, resolver estos problemas no debe ser parcial y limitado (Setiawan, Syamsudin, & Sastrosubroto, 2016).

En este artículo se presenta una revisión sistemática (RS) de la literatura acerca del tópico de importancia de los modelos para el GSI, siguiendo el proceso de Kitchenham (2004), en el que indica que las revisiones sistemáticas se basan en una estrategia de búsqueda definida que apunta a detectar la mayor cantidad posible de literatura relevante, por lo cual, el propósito de este trabajo es comprender la importancia de los modelos para el GSI en la literatura de investigación; la investigación no será delimitada y los términos de búsqueda se mantienen amplios a fin de no limitar la investigación a un área determinada dentro de la temática.

La estructura de este trabajo es la siguiente: en primer lugar, se discuten cuestiones metodológicas; luego, se consideran las características de la investigación existente sobre GSI, con respecto a las temáticas tratadas y la relación entre ellas, a través de los resultados del examen sistemático y la discusión. La última sección presenta las conclusiones y se discuten las implicaciones para futuras investigaciones.

2. Desarrollo

Dado que las disciplinas de computación tienen una trayectoria relativamente nueva, se encuentra que Kitchenham (2004) propone un método para realizar revisiones sistemáticas de esta importante área, en el cual, se señala que una revisión sistemática se define como una manera de evaluar e interpretar toda la investigación disponible relevante respecto de una interrogante de investigación particular, en un área temática o fenómeno de interés y que los estudios individuales que contribuyen a una revisión sistemática se denominan estudios primarios, una revisión sistemática se considera un estudio secundario. El presente trabajo usa la metodología descrita, para despejar la interrogante planteada a continuación.

2.1. Definición de la pregunta de investigación

Para conocer los modelos usados para el GSI, se ha definido la siguiente pregunta: ¿Cuáles son los modelos disponibles para el GSI que apoyan a las labores corporativas?

Como palabras claves se utilizaron: estándares, modelos, tecnología, gobierno corporativo.

Con el objeto de concretarla un poco más la pregunta de investigación planteada se subdivide en las siguientes interrogantes:

- ¿De los modelos encontrados cuál es el que más ha sido propuesto?
- ¿Qué herramientas de seguridad de información han sido estudiadas?
- ¿Existen estudios de la aplicación de gobierno de seguridad de la información?

2.2. Selección de fuentes

Para identificar todos los estudios sobre los modelos para el GSI, se realizó una búsqueda sistemática en las bases de datos de EBSCOhost (EBS), IEEE Xplore (IEEEX), Google Scholar y Science Direct, cubriendo todos los artículos publicados desde el año 2014. Se identificaron los estudios relevantes usando las palabras claves. Además, se revisaron todos los resúmenes en los artículos para evitar la exclusión de estudios significativos. Adicionalmente, las bases de datos de las fuentes bibliográficas seleccionadas tenían que contar con un motor de búsqueda que permita ejecutar consultas de búsqueda avanzada.

2.3. Estrategias de búsqueda

La estrategia de búsqueda se basó en las palabras "information security governance", además de la expresión "information security standars".

La cadena de búsqueda estructurada fue: "information security governance" OR "information security standars".

Se aplicó la cadena de búsqueda solo al título de los artículos, en cada una de las bibliotecas electrónicas y cuando contenía las palabras definidas, se obtenía y revisaba el artículo.

La temporalidad de las publicaciones fue desde el año 2014.

Los tipos de publicaciones fueron conferencias, conferencias internacionales, workshops internacionales y artículos de revistas.

Los artículos debían ser escritos en idioma inglés.

2.4. Criterios de inclusión y exclusión

Criterios de inclusión

Artículos publicados entre los años 2014 y 2018.

Artículos cuyos títulos tuvieran la expresión "information security governance" o la expresión "information security standars".

Contenidos específicos sobre “information security”.

Artículos de conferencias, revistas y “workshops” internacionales.

Criterios de exclusión

Trabajos en diapositivas y libros.

Literatura gris, que corresponde a artículos no publicados.

De los artículos repetidos en varias bibliotecas digitales, solo se seleccionó uno de ellos.

2.5. Extracción de información y revisión de trabajos para selección de artículos

Una vez realizada la búsqueda que se llevó a cabo en las publicaciones indexadas de todas

las bases ya mencionadas, durante los meses de septiembre y octubre del 2018, y aplicando la cadena de búsqueda para todas las bases de datos se procedió a la selección de la muestra, se utilizó el siguiente procedimiento: a) revisión general de los títulos, resúmenes y evaluación de los contenidos, y; b) lectura de cada documento y extracción de los datos principales. Adicionalmente, se excluyeron aquellos estudios en los que, aunque aparecía el término, no era el tema central del escrito o no se mencionaban de manera específica sus características, a los que no se tuvo acceso de texto completo y a los que estaban escritos en un idioma diferente al inglés.

Se seleccionaron originalmente 117 documentos potenciales, de los cuales se excluyeron 71 en base a la revisión del título y resumen, resultando un total de 46 estudios para una revisión posterior. Después de leer los artículos completos y verificar su pertinencia para el presente estudio, se seleccionaron un total de 23 escritos, ver tabla 1.

Tabla 1
Selección de artículos

Detalle de selección	**No. de artículos**
Artículos potenciales identificados en las bases de datos	117
Estudios excluidos en base a título y resumen, por no ser texto completo, sin acceso al artículo y por ser irrelevantes	71
Escritos considerados para una revisión de texto completo	46
Excluidos tras la lectura de textos completo	23
Total de textos incluidos	23

Fuente: elaboración propia

3. Resultados del examen sistemático

Después de analizar los títulos y los resúmenes de los artículos seleccionados para esta revisión, el autor obtuvo los siguientes grupos correspondientes a aspectos tales como: modelos propuestos, evaluación de herramientas de seguridad, casos de estudios de la aplicación de GSI, modelos adaptados y niveles organizativos a los que más afecta.

Cuando no era suficientemente claro el resultado, se leía parte o la totalidad de la descripción o formulación del estudio realizado. En muchos casos no era necesario leer el artículo completo. En la sección de conclusiones se buscaba también la descripción de trabajos futuros con el fin de conocer nuevos problemas abiertos o nuevas direcciones de investigación. Después de leer todos los estudios, se organizaron para facilitar nuevamente su lectura y análisis.

La tabla 2 muestra los estudios seleccionados en este trabajo, así como un resumen de sus características y lo encontrado en ellos, están ordenados alfabéticamente y su orden no determina su importancia con respecto a los objetivos del presente trabajo. Además, se detallan los modelos y estándares relacionados junto con el nivel organizativo que interviene.

Tabla 2
Resumen de artículos seleccionados con modelos y estándares referidos

Artículo	**Año publicación**	**Autor**	**Modelos y estándares referidos**	**NOQI**

A Framework for Information Security Governance and Management	2016	Marian Carcary	ISGM framework, COBIT 5, ISO 27002	G
A Proposed Best-practice Framework for Information Security Governance	2017	Ghada Gashgari	ISO / IEC 27014 y COBIT	G
A Study on E-Taiwan Promotion Information Security Governance Programs with E-government Implementation of Information Security Management Standardization	2016	Chien-Cheng Huang	ISO/IEC 27001:2005, ISO/IEC 27003:2010	G-O
An Analysis of the Information Security Governance in the State Owned Enterprises (Soe) In Zimbabwe.	2015	Joseph Sigauke		O
An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas	2014	Dr. Winfred Yaokumah		G
An Evaluation of Security Governance Model in Organizational Information Technology or Information Systems Security Implementation	2018	Dayang Hanani Abang Ibrahim		O
An Overview of Information Security Governance	2017	Mehdi Asgarkhani	ISO27001, BS7799, Payment Card Industry Data Security Standard (PCIDSS), Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Technology (COBIT), ISO27002: 2007/ ISO 7799:2005, ANSI/ISA-99.02.01-2009	G
Design and Implementation Information Security Governance Using Analytic Network Process and COBIT 5 For Information Security A Case Study of Unit XYZ	2015	Haryo Laksono	COBIT 5	
Empirical Evaluation of a Cloud Computing Information Security Governance Framework	2015	Oscar Rebollo	ISO / IEC 38500 o COBIT 5, norma ISO / IEC 27036	O
Exploring Information Security Governance in Cloud Computing	2015	Hemlata Gangwar		O

Organisation				
Exploring the Link Between Behavioural Information Security Governance and Employee Information Security Awareness	2015	W. Flores		O
Information Security Governance for the Nonsecurity Business Executive	2014	Michael Whitman	COBIT 5	G
Information security governance in big data environments: A systematic mapping	2018	Reza Saneei Moghadam	ISO / IEC 27014 y COBIT	G
Information Security Governance in Colleges and Universities	2017	Jia WANG		G
Information Security Governance model to enhance zakat information management in Malaysian Zakat Institutions	2014	Hidayah Sulaiman		O
Information Security Governance on National Cyber Physical Systems	2016	Ahmad Budi Setiawan	ISO / IEC 38500, COBIT 5	O
Information Security Governance: A Case Study of the Strategic Context of Information Security	2017	Terrence Tan	ISO 27000	O
Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture	2014	Waldo Rocha Flores		O
Information Security: Risk, Governance and Implementation Setback	2015	M.R, Fazlida	ISO 27001 and COBIT. COSO, COBIT, ISO 27001 y el Estándar de Declaración de Auditoría No.70	G
Information System Security Commitment: A Study of External Influences on Senior Management	2016	Kevin A. Barton		G
MAVEN Information Security Governance, Risk Management, and Compliance (GRC): Lessons Learned	2014	Eduardo Takamura		O
Model Design of Information Security Governance Assessment with Collaborative Integration of COBIT 5 and ITIL	2014	Perdana Kusumah	ISO / IEC 27001: 2009 e ISO / IEC 27002: 2005	

Obstacles to Implementation of Information Security Governance	2018	William W. Lidster, Ph.D. Candidate	COBIT, ISO	G

NOQI: Nivel organizativo que interviene / G: gerencial O: operativo
Fuente: elaboración propia

3.1. Modelo más referido o propuesto para el GSI

En la actualidad es necesario conocer soluciones que permitan proteger los datos generados día a día, por lo cual se debe contemplar no solo el hardware como elemento a resguardar, sino involucrar aspectos tales como: los análisis de riesgos, asignación de roles con sus responsabilidades y marcos normativos, lo cual permitirá a una organización poder estar "segura". Debido a esto se deben conocer, analizar y revisar los modelos GSI; para cumplir con esta necesidad, se procedió a la revisión de los artículos seleccionados y a identificar el modelo más nombrado o relacionado en los mismos.

La revisión arroja que 13 artículos sugieren modelos para el tema revisado; en la tabla 3, se muestran los artículos con los modelos propuestos.

Tabla 3
Consolidado del número de artículos y modelos referenciados

Modelo	**Número de artículos**	**Artículos**
Solo COBIT	2	(Laksono & Supriyadi, 2015) y (Whitman & Mattord, 2014)
Solo ISO	3	(Kusumah et al., 2014), (Tan, Maynard, Ahmad, & Ruighaver, 2017), (Huang & Farn, 2016)
COBIT, ISO, otros	8	(Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015), (Asgarkhani, Correia, & Sarkar, 2017), (LIdster & Rahman, 2018), (Carcary, Renaud, McLaughlin, & O'Brien, 2016), (Moghadam & Colomo-Palacios, 2018), (Gashgari, Walters, & Wills, 2017), (Setiawan et al., 2016), (Fazlida & Said, 2015)

Fuente: elaboración propia

Se encuentra que en tres artículos basan sus estudios solo en la norma ISO, la misma que proporciona orientación sobre conceptos y principios para la GSI, mediante la cual las organizaciones pueden evaluar, dirigir, monitorear y comunicar las actividades relacionadas con la seguridad de la información dentro de la organización y con otras normas ISO27k es aplicable a todos los tipos y tamaños de organizaciones. La correcta GSI garantiza la alineación de la seguridad de la información con las estrategias y los objetivos empresariales, la entrega de valores y la responsabilidad; apoya el logro de visibilidad, agilidad, eficiencia, efectividad y cumplimiento.

Señalan Setiawan, Syamsudin, & Sastrosubroto (2016), que la norma ISO/IEC 38500:2013 tiene un marco que se basa en seis principios para ser utilizados como referencia por el gobierno de tecnología de la información (TI), entre otros: responsabilidad, estrategia, adquisición, rendimiento, adecuación, comportamiento humano. La declaración de cada principio se refiere a lo que debería suceder, pero no especifica cómo, cuándo o a quién se aplicarán.

En dos artículos del total de evaluados se encuentra que hacen uso de COBIT; así lo indican Laksono & Supriyadi, (2015) que COBIT 5 para la seguridad de la información se puede utilizar para implementar procesos de seguridad de la información en la organización, ya que, proporciona procesos y habilitadores necesarios para generar valor a través del uso de TI.

En su artículo indican Carcary, Renaud, McLaughlin, & O'Brien (2016), que utilizando un enfoque de investigación colaborativa de innovación abierta en un marco de madurez de capacidad para information security governance and management (ISGM), se han utilizado comparaciones con estándares y marcos de seguridad de la información, entre ellos: COBIT 5.0 para la seguridad de la información, el modelo de madurez de la GSI de Open Group, el cuerpo de conocimientos esencial de seguridad de TI, e ISO 27002.

En el artículo de Rebollo, Mellado, Fernández-Medina, & Mouratidis (2015), se indica que el marco propuesto por ellos mantiene un enfoque de gobierno de seguridad continuo, alineándose con las propuestas existentes, como la norma ISO/IEC 38500 o COBIT 5.

3.2. Herramientas propuestas para GSI

Se encuentra que en solo un artículo se mencionan las herramientas que han analizado, es así que indica Asgarkhani et al. (2017), algunas de las soluciones tecnológicas relacionadas con la seguridad de internet más amplia y la seguridad de la información más específica pueden incluir pruebas de penetración y se mencionan a las herramientas siguientes: Honeynets, Simulated Attacks (Wargames), Access Control, Cryptographic System, Firewalls, Intrusion Detection Systems (IDS), Anti-Malware Software and Scanners, Internet Protocol Security (IPsec) y Secure Socket Layer (SSL).

A medida que aumenta el interés por proteger la información, sea en los equipos locales, en la red o en la nube, ya que cada vez más los sistemas de almacenamiento se han universalizado y son más rápidos, han surgido nuevas aplicaciones que permiten explotarlos al máximo. Asimismo, con cada avance tecnológico se van creando nuevas herramientas, definidas por la necesidad de los usuarios de hacer alguna tarea concreta. Estos programas, aplicaciones o simplemente instrucciones son usados para efectuar las tareas de modo más sencillo.

La cartera de prácticas que guían las estrategias de evaluación, el establecimiento de una dirección y la decisión sobre las herramientas de TI a menudo se denomina Gobernabilidad de la Tecnología de la Información (ITG). ITG involucra elementos tanto estratégicos como operativos (Asgarkhani et al., 2017).

3.3. Estudios en los que se aplican modelos establecidos de GSI

El GSI es el sistema mediante el cual una organización dirige y controla la seguridad de TI utilizando algunos de los modelos propuestos. El GSI no debe confundirse con la administración de seguridad de TI. El gobierno determina quién está autorizado para tomar decisiones. El gobierno, o también llamado gobernanza, especifica el marco de responsabilidad y proporciona supervisión para garantizar que los riesgos se mitigan adecuadamente. La gobernabilidad garantiza que las estrategias de seguridad estén alineadas con los objetivos comerciales y que sean coherentes con las regulaciones.

En la tabla 4 se incluyen los artículos en los cuales se hace un seguimiento a la aplicación de los modelos de gobiernos de seguridad de la información.

Tabla 4
Tipos de organización que aplicaron y estudiaron al GSI

Tipo de organización	Artículos
Pequeñas, medianas y grandes	(Flores & Ekstedt, 2015)

Sin definir	(Gangwar & Date, 2015), (Laksono & Supriyadi, 2015)
Gubernamental	(Sigauke, Mupfiga, & Tsokota, 2015)
Servicios	(Rebollo et al., 2015), (Kusumah et al., 2014), (Tan et al., 2017)
Agencia espacial	(Takamura, Gomez-Rosa, Mangum, & Wasiak, 2014)

Fuente: elaboración propia

En su artículo Flores & Ekstedt (2015), indican que los resultados de su estudio realizado en 24 empresas revelan que tener una unidad formal con responsabilidad explícita para la seguridad de la información, utilizar comités de coordinación y compartir el conocimiento de seguridad a través de un sitio de intranet se correlaciona significativamente con las dimensiones de la conciencia de seguridad de la información de los empleados, ya que, la administración y el apoyo de los empleados son el componente crítico de la implementación efectiva del marco de gobierno de la seguridad de la información, Gangwar & Date, (2015).

De acuerdo con Sigauke et al. (2015), algunas características de la GSI, considera que la información debe estar protegida contra daños por amenazas que conducen a diferentes tipos de impactos, como pérdida, inaccesibilidad, alteración o divulgación errónea, es por esto que los estudios antes señalados se han enfocado en la aplicación del Gobierno de la seguridad de la información en algunos tipos de organizaciones.

Señalan Moghadam & Colomo-Palacios (2018), que el 58% de las organizaciones que informaron tener esfuerzos activos de big data incluyeron procesos de seguridad y gobierno, y que existe cada vez más la necesidad de un marco general de seguridad de la información que pueda proporcionar contexto y coherencia a la actividad de cumplimiento en todo el mundo.

Para Tan et al. (2017), luego de su revisión concluyen que en lugar de un enfoque basado en el riesgo y los controles, las organizaciones deben abordar los objetivos y las estrategias a través del desarrollo de su contexto estratégico de seguridad, ya que ninguna tecnología es capaz de eliminar los riesgos de seguridad de TI. Es por eso que se deben administrar los riesgos para que a medida que se reduzcan las vulnerabilidades, se incremente la seguridad del sistema. El aseguramiento de la información es tan importante como el aseguramiento de una misión (Takamura et al., 2014).

Queda en claro que una buena implementación del GSI proporciona alineación estratégica, gestión de riesgos, gestión de recursos, medición del rendimiento y entrega de valor (Gashgari et al., 2017) y que el GSI requiere un control constante asociado con el uso de técnicas de gobernabilidad como la gestión de riesgos, la gestión de procesos empresariales y la gestión de procesos de seguridad para garantizar el valor empresarial (Moghadam & Colomo-Palacios, 2018).

Consideran Whitman & Mattord (2014) que cuando la administración ejecutiva no planifica el éxito y no diseña e implementa programas y estructuras de gobierno altamente funcionales, los activos de información estarán expuestos a niveles más altos de riesgo y la información utilizada en la organización puede verse comprometida y tener un valor reducido, por lo cual las organizaciones pueden transformar su enfoque de la seguridad. En lugar de un enfoque basado en el riesgo y los controles, los investigadores abogan por que las organizaciones aborden los objetivos y las estrategias a través del desarrollo de su contexto estratégico de seguridad, se espera que las políticas de seguridad y las pautas desarrolladas permitan a los responsables de la toma de decisiones entender el fundamento de los controles, en lugar de simplemente realizar la función de controles de seguridad (Tan et al., 2017).

3.4. Estudios en los que se proponen modelos adaptados al GSI

El éxito en la implementación de un modelo ya establecido, sea ISO/IEC 27001, COBIT, o cualquiera de los conocidos, se fundamenta en que fue adoptada la norma y alineada a los objetivos y a lineamientos y necesidades específicas de una organización, lo cual es un fundamento muy importante para el GSI.

A pesar de tener estos modelos ya establecidos, se demuestra que son necesarios nuevos modelos que permitan llegar a la reducción de los riesgos al ayudar a gestionarlos en forma segura y acorde a los requerimientos de la organización una vez que fueron establecidos los criterios contra los cuales se los evaluaría.

En la revisión realizada se encuentra que cuatro autores proponen nuevos modelos, es así que señalan Kusumah et al. (2014), que hay tres tareas principales para preparar el GSI, las cuales consisten en determinar el alcance del proceso, hacer el modelo de referencia del proceso y hacer el modelo de evaluación. Por lo cual indica que el propósito de su estudio es desarrollar un modelo de evaluación para el GSI integral e integrado en el sistema de gestión de servicios para la empresa, especialmente de su caso de estudio: INTRAC.

En el artículo "Information security governance model to enhance zakat information management in Malaysian zakat institutions" de Sulaiman & Jamil (2014), se encuentra que con la implementación de un GSI sólido, esto mejorará los beneficios del receptor de zakat (% de bienes a ser entregados), aumentará el rendimiento comercial y la productividad de las instituciones de zakat y brindará mayor seguridad a los pagadores de zakat sobre la transparencia de la administración de zakat. Por lo tanto, el modelo propuesto para el GSI entre la institución zakat y los fideicomisarios del fondo zakat, a fin de contar con información precisa que se utilizará para una mejor toma de decisiones y la gestión de zakat, ha identificado 7 factores que contribuyen a la alineación de los objetivos del GSI y la asimetría de la información, estos son: confianza, integridad, ética, auténtico, proceso, relacional y estructural.

Indica Gashgari et al. (2017), que como no se han identificado los factores críticos de éxito (CSF, por sus siglas en inglés) que aseguran la mejora de un nivel alto en las áreas de gobernabilidad esenciales para una gobernabilidad efectiva, se ha propuesto un marco de mejores prácticas para GSI en las áreas de gobernanza esenciales para una gobernanza efectiva de los SI que apoye a las organizaciones para sobrevivir y prosperar. La principal contribución de este artículo es que establece un marco para GSI, basado en estándares y marcos reconocidos internacionalmente de GSI que puede ser utilizado por todos los tipos y tamaños de organizaciones, en él se contempla lo siguiente: alineación estratégica, medición del desempeño, entrega de valor, gestión de riesgos y administración de recursos.

Rebollo et al, (2015), muestran que ya en una investigación anterior las propuestas existentes relacionadas con la seguridad de la computación en la nube tienen deficiencias en cuanto a su cumplimiento de los aspectos de gobernabilidad y que tales sistemas tienen características diferenciadoras claras, lo que sugiere la necesidad de metodologías de gestión de seguridad adaptada; por lo cual el modelo propuesto mantiene un enfoque de gobernanza de seguridad continuo, alineándose con las propuestas existentes, como la norma ISO/IEC 38500 o COBIT 5, señalan que el modelo ISGcloud incluye cuatro procesos de gobierno centrales: a) Evaluar el uso actual y futuro de TI; b) Preparación directa e implementación de planes y políticas para asegurar que el uso de TI cumpla con los objetivos comerciales; c) Monitorear la conformidad con las políticas y el desempeño contra los planes; y d) Comunicar el conocimiento y las políticas que se requieren en ISG.

3.5. Niveles organizacionales a los que se han dirigido los estudios revisados

La pirámide organizacional muestra tres niveles en su estructura jerárquica, de los cuales el estratégico y operativo se encuentran relacionados en casi todos los artículos seleccionados; establecen parámetros que garanticen que se logren los objetivos, determinando que los riesgos se administran en forma apropiada y verificando que los recursos de la empresa se utilizan con responsabilidad.

La implementación de GSI se puede lograr si a) La junta directiva y la gerencia ejecutiva

ponen atención adicional en los asuntos de seguridad de la información en lugar de tratarlos como problemas tecnológicos bajo las responsabilidades de los gerentes técnicos; b) la medida de seguridad de la información se comunica claramente desde la alta dirección al personal de nivel inferior; c) el personal de bajo nivel participa en la formulación de las políticas de seguridad de la información para evitar el retroceso o el rechazo de la implementación de la política y, por último, d) todas las partes interesadas están conscientes del valor agregado ofrecido por la implementación del GSI que resulta en una mayor inversión en el control de la seguridad de la información, así lo indican Fazlida & Said, (2015).

Un sistema de seguridad de la información en la empresa fomenta los entornos de trabajos seguros al ofrecer un marco que permite a la organización identificar y controlar coherentemente sus riesgos de la información, reducir el potencial de accidentes y mejorar el rendimiento en general; Gangwar & Date (2015), señalan que las empresas deben centrarse en la sensibilización a través de la educación y la formación de los empleados. Además, la administración y el apoyo de los empleados son el componente crítico de la implementación efectiva del marco de gobierno de la seguridad de la información.

Consideran Tan et al. (2017) que comprender cómo ciertas características de la gobernanza de la seguridad, a nivel empresarial y por debajo, influyen en la calidad de la toma de decisiones estratégicas en la seguridad de la información es un paso esencial para garantizar que las inversiones en seguridad no se desperdicien, por lo que la ejecución de estrategias de seguridad y las decisiones oportunas en torno a estas estrategias se producen, según los autores, en el nivel de operaciones de la organización.

4. Discusión

Esta investigación se ha realizado sobre la base del método de revisión sistemática explicado en la sección 2. El propósito fue conocer la importancia en la administración de los modelos para el gobierno de la seguridad de la información y que sirvan de guía a los directivos de las organizaciones en asuntos relacionados con este tema.

En varios artículos se menciona el uso de COBIT, al que se conoce como una guía de mejores prácticas, presentada como framework, y considera la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos, y finalmente permita una evaluación sobre los procesos involucrados en la organización.

En cuanto a ISO/IEC 38500:2008 al ser una norma internacional que trata sobre el concepto de Gobierno TI en las organizaciones, fija los estándares para el buen gobierno de los procesos y decisiones empresariales relacionados con los sistemas y tecnologías de la información; está dirigida principalmente a la alta dirección de las organizaciones para hacerles entender y ayudarles a cumplir sus obligaciones legales, regulatorias y éticas respecto al uso de las TIC en sus organizaciones.

COBIT e ISO son los modelos y estándares más utilizados y revisados en los artículos de la investigación realizada. Así lo señala Asgarkhani et al. (2017) al indicar que el personal es el eslabón más débil de seguridad, por lo que la falta de comprensión y conciencia de las consecuencias de los compromisos de seguridad, una cultura relajada en la que la confiabilidad del sistema no se considera seria, hacen necesario lograr un gobierno eficiente a través de procedimientos estandarizados haciendo uso de COBIT, ISO e ITIL. Laksono & Supriyadi, (2015) manifiestan que COBIT 5 es compatible con los activos de TI y los objetivos comerciales para ayudar a garantizar que los sistemas de información cumplan con los controles de riesgo necesarios.

Los profesionales informáticos utilizan herramientas técnicas con fines tácticos específicos cuando se trata de seguridad o garantía dentro de sus entornos, que pueden ser de código abierto o comercial. Pero, cuando se trata de GSI, a menudo puede ser más difícil encontrar herramientas específicas, las razones de esto no son difíciles de entender. El gobierno es por definición, un ejercicio que requiere una personalización significativa de la organización para

la organización, y cómo puede una herramienta personalizada de gobierno implementarse en una organización que es muy diferente de la de otra organización, ya que tienen objetivos diferentes. Esto, a su vez, hace que sea difícil encontrar y usar herramientas de talla única que puedan soportar transversalmente las implementaciones en varias organizaciones.

Por lo antes expuesto, Flores & Ekstedt (2015), señalan que el soporte para la transferencia de conocimientos sobre seguridad mediante el uso de tecnología como el sitio de intranet dedicado a la seguridad de la información (por ejemplo, amenazas y procedimientos generales, políticas y directrices) parece ser beneficioso, ya que influye en la percepción de la seguridad de la información de los empleados, incluso al parecer, los empleados están dispuestos a usar la tecnología para aprender sobre la seguridad de la información y estar conscientes de las amenazas comunes.

A pesar de que COBIT y las ISO son los modelos más usados y han sido una guía en muchas implementaciones para la seguridad realizadas, es importante recalcar que los modelos en sí no bastan para tener un correcto gobierno de TI, ya que ello solo se puede alcanzar cuando existe todo el marco compuesto por políticas, procedimientos, informes, registros, instructivos ajustados según el ámbito de la organización. En el artículo de Asgarkhani et al. (2017), se señalan los siguientes modelos: ISO27001, BS7799, Estándar de seguridad de datos de la industria de tarjetas de pago (PCIDSS), biblioteca de infraestructura de tecnología de la información (ITIL), Objetivos de Control para la Información y la Tecnología (COBIT), ISO27002: 2007 / ISO 7799: 2005, ANSI / ISA-99.02.01-2009; Sigauke et al. (2015), recomiendan que las empresas de propiedad estatal utilicen los siguientes modelos COBIT, ITIL y BS17009.

El proceso de implementación requiere empatía y razonamiento, la empatía se refiere a ponerse uno mismo en los zapatos de los creadores del estándar, y viendo el modelo en su totalidad (Huang & Farn, 2016).

Se encontró que algunos autores proponen nuevos modelos que en muchos casos parten de los ya nombrados anteriormente pero que debido a algunas condiciones deben ser ajustados. Gashgari et al. (2017), indican que el marco propuesto deberá revisarse para su aplicación en regiones particulares, a fin de confirmar que es adecuado para las estructuras y cultura organizativas locales, en particular porque el marco está sujeto a las leyes y regulaciones locales.

Al ser los niveles estratégicos y operativos a los que más está dirigido el GSI, se encuentra que esto se logra cuando los miembros de la organización a cargo de esa responsabilidad saben qué hacer, quién debe hacerlo y cómo debe hacerse. Cuando la administración ejecutiva no planifica el éxito y no diseña e implementa programas y estructuras de gobierno altamente funcionales, los activos de información estarán expuestos a niveles más altos de riesgo y la información utilizada en la organización puede verse comprometida y tener un valor reducido (Whitman & Mattord, 2014). Por lo tanto, los factores formales, técnicos e informales incluyen: visión y objetivos de negocios, cultura organizacional, estrategia de gestión, ajuste tecnológico y valores y creencias de los empleados (Ibrahim et al., 2018)

---

5. Conclusiones

Se conoce que las revisiones sistemáticas permiten sintetizar la información existente sobre un fenómeno de forma minuciosa y empírica y al final permite obtener como resultado una conclusión general sobre los estudios individuales del fenómeno en cuestión.

Es así que se encuentra que los modelos COBIT y las ISO son los más usados dentro del GSI en las organizaciones que han realizado estas implementaciones, aun cuando existen otros modelos tales como: ISO27001, BS7799, estándar de seguridad de datos de la industria de tarjetas de pago (PCIDSS), biblioteca de infraestructura de tecnología de la información (ITIL), ISO27002: 2007 / ISO 7799: 2005, ANSI / ISA-99.02.01-2009.

No se definían en los artículos las herramientas tecnológicas utilizadas para realizar la implementación de los modelos propuestos, solo en un artículo se sugerían las siguientes:

Honeynets, Simulated Attacks (Wargames), Access Control, Cryptographic System, Firewalls, Intrusion Detection Systems (IDS), Anti-Malware Software and Scanners, Internet Protocol Security (IPsec) y Secure Socket Layer (SSL).

Muchas organizaciones han adoptado modelos ya establecidos para el GSI y su aplicación va a pequeñas, medianas, grandes, gubernamentales, de servicios e inclusive en una agencia espacial.

Los nuevos modelos propuestos por algunos autores tienen como partida los modelos ya establecidos y reconocidos para esta actividad y resultan de una serie de ajustes necesarios por el tipo de giro de negocios que realizan y que no son iguales en todas las organizaciones.

Se indica en la misma magnitud que los niveles organizaciones estratégicos y operativos son los que más intervienen en el proceso de implementación, aplicación y administración del GSI.

Es necesario realizar más investigaciones para abordar cuestiones relacionadas con la evolución de la aplicación de los modelos de GSI en distintas organizaciones, sean privadas, públicas o mixtas, además de la aplicación de las herramientas tecnológicas.

Referencias bibliográficas

Asgarkhani, M., Correia, E., & Sarkar, A. (2017). An overview of information security governance. 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 1–4. https://doi.org/10.1109/ICAMMAET.2017.8186666

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. Computers & Security, 59, 9–25. https://doi.org/10.1016/j.cose.2016.02.007

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A Framework for Information Security Governance and Management. IT Professional, 18(2), 22–30. https://doi.org/10.1109/MITP.2016.27

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. Procedia Economics and Finance, 28, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

Flores, W., & Ekstedt, M. (2015). Exploring the Link Between Behavioural Information Security Governance and Employee Information Security Awareness. 13.

Gangwar, H., & Date, H. (2015). Exploring Information Security Governance in Cloud Computing Organisation: International Journal of Applied Management Sciences and Engineering, 2(1), 44–61. https://doi.org/10.4018/ijamse.2015010104

Gashgari, G., Walters, R., & Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, 295–301. https://doi.org/10.5220/0006303102950301

Huang, C.-C., & Farn, K.-J. (2016). A Study on E-Taiwan Promotion Information Security Governance Programs with E-government Implementation of Information Security Management Standardization. 14.

Ibrahim, D. H. A., Musa, N., & Leng, C. K. (2018). An Evaluation of Security Governance Model in Organizational Information Technology or Information Systems Security Implementation. 10(2), 5.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Joint Technical Report, 1–33. Recuperado de http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.

Kusumah, P., Sutikno, S., & Rosmansyah, Y. (2014). Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC). 2014 International Conference on ICT For Smart Society (ICISS), 1–6. https://doi.org/10.1109/ICTSS.2014.7013193

Laksono, H., & Supriyadi, Y. (2015). Design and implementation information security governance using Analytic Network Process and cobit 5 for Information Security a case study of unit XYZ. 2015 International Conference on Information Technology Systems and Innovation (ICITSI), 1–6. https://doi.org/10.1109/ICITSI.2015.7437689

LIdster, W., & Rahman, S. S. M. (2018). Obstacles to Implementation of Information Security Governance. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1826–1831. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00276

Moghadam, R. S., & Colomo-Palacios, R. (2018). Information security governance in big data environments: A systematic mapping. Procedia Computer Science, 138, 401–408. https://doi.org/10.1016/j.procs.2018.10.057

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, 58, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Setiawan, A. B., Syamsudin, A., & Sastrosubroto, A. S. (2016). Information security governance on national cyber physical systems. 2016 International Conference on Information Technology Systems and Innovation (ICITSI), 1–6. https://doi.org/10.1109/ICITSI.2016.7858210

Sigauke, J., Mupfiga, P., & Tsokota, T. (2015). An Analysis of the Information Security Governance in the State Owned Enterprises (Soe) In Zimbabwe. 5.

Sulaiman, H., & Jamil, N. (2014). Information security governance model to enhance zakat information management in Malaysian zakat institutions. Proceedings of the 6th International Conference on Information Technology and Multimedia, 200–205. https://doi.org/10.1109/ICIMU.2014.7066630

Takamura, E., Gomez-Rosa, C., Mangum, K., & Wasiak, F. (2014). MAVEN information security governance, risk management, and compliance (GRC): Lessons learned. 2014 IEEE Aerospace Conference, 1–12. https://doi.org/10.1109/AERO.2014.6836516

Tan, T., Maynard, S., Ahmad, A., & Ruighaver, T. (2017). Information Security Governance: A Case Study of the Strategic Context of Information Security. Information Security Governance, 15.

Wang, J. (2017). Information Security Governance in Colleges and Universities. DEStech Transactions on Economics, Business and Management, (icem). https://doi.org/10.12783/dtem/icem2017/13206

Whitman, M., & Mattord, H. J. (2014). Information Security Governance for the Non-security Business Executive. 17.

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. Journal of Business Systems, Governance and Ethics, 9(2). https://doi.org/10.15209/jbsge.v9i2.718

---

1. Universidad Ecotec, Universidad Agraria del Ecuador. Ingeniero en Sistemas, Magister en Negocios Internacionales, Doctorando en Administración UCA. mespinoza@ecotec.edu.ec , mespinoza@uagraria.edu.ec

---