MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN: UNA REVISIÓN SISTEMÁTICA DE SU CONCEPTO.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Aida Diana ORMAZA VINTIMILLA

Bajo la dirección de:
Francisco Joshep BOLAÑOS BURGOS.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Junio del 2016

Política de Seguridad de la Información: Una revisión sistemática de su concepto

Information Security Policy: A systematic review of its concepts

Aida Diana ORMAZA VINTIMILLA[1]
Francisco Joseph BOLAÑOS BURGOS[2]

Resumen

El objetivo de este artículo es establecer un concepto de Políticas de Seguridad de la Información (PSI) con base en su clasificación, características y objetivos, a través de una revisión sistemática de literatura tomando como fuente de información la base Web of Knowledge en un período de diez años, comprendidos entre el 2006 y el 2016. Se concluye que las PSI son documentos o mecanismos que especifican reglas que no sólo involucran el aspecto tecnológico sino también al humano y que se enfocan en la Seguridad de la Información y la Gestión de Seguridad de la Información. Como trabajo futuro se plantea realizar la misma investigación en base de datos no estructuradas aplicando técnicas de vigilancia tecnológica para contrastar el nivel de acuerdo en la conceptualización de las PSI entre las empresas auditoras y la academia.

Palabras clave: Políticas de Seguridad de la Información, Seguridad de la Información, Revisión sistemáticas, auditoría de TI.

Abstract

The aim of this article is to establish the concept of Information Security Policy (ISP) based on its classificaction, features and objectives through a systematic review taking as reference the database Web of Knowledge between the years 2006 and 2016. Findings define ISP as documents or mechanisms which specifies rules and involve human and tecnological aspects, it focuses in information security and information secuirty management. As future work the same research can be executed, but in non structured databases using tecnological survilliance Techniques. The obtained results could be compared with the definition of this research and establish the concordance level between IT auditing companies and the academia.

Key words Information Security Policies, Information Security, systematic review, IT auditing.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail aidaormaza@uees.edu.ec.
[2] Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

INTRODUCCIÓN

La información es un activo de vital importancia para cualquier organización (Lim Thow-Chang, n.d.); adopta diferentes formas y está disponible en ambientes cada vez más interconectados por lo que está expuesta a amenazas y vulnerabilidades (Baldecchi, 2014), que están provocando preocupación por la seguridad, dado que el fracaso de ésta traerá consecuencias de gran alcance para la economía, los negocios y la sociedad mundial (BBVA, 2016). Von Solms (1999), afirma que la seguridad de la información ya no es sólo un asunto interno, sino que también afecta a las partes externas; las organizaciones intentan proteger su propio entorno, pero no tienen control sobre los sistemas con los que se vinculan. PricewaterhouseCoopers (2016), indica que existe un incremento del 38% de incidentes que afectan a la seguridad de la información a nivel global en el año 2015, con un impacto del 50% a causa de estos incidentes. Además, se ha registrado un aumento notable de incidentes de seguridad, dado que de 10 organizaciones 9 han sufrido infracciones de seguridad (HM Government, 2015).

Para proporcionar seguridad de información adecuada y con el fin de reducir el riesgo contra infracciones a los datos, es importante contar con una política de seguridad (Lineman, 2011), que aporte instrucciones generales elaboradas a la medida de las organizaciones y cuyo cumplimiento sea obligatorio (Wood, 2002). Sin embargo, definir el contenido de una política de seguridad de la información, asociada a controles de seguridad es un problema (Von Solms, 1999); su aplicación no garantiza que una organización esté completamente protegida; si la política de seguridad es mal entendida existirá incumplimiento por parte del personal (HM Government, 2015), puesto que a pesar de tener conocimientos sobre sus funciones en el proceso de seguridad éstos no se adhieren a la política establecida (Niekerk & Solms, 2006) debido al conflicto generado entre sus creencias y valores (Schlienger & Teufel, 2003); una política que no proyecte y dé valor a los activos atraerá intrusos; éstas infracciones no representativas pueden volverse severas si es que los responsables están acostumbrados a no cumplir con ella, explotando las debilidades de las políticas (Control Data, 1999), amplificando los riesgos por políticas inefectivas (Deloitte, 2016). Por otro lado, las políticas de seguridad que dictan el comportamiento de los usuarios a nivel interno, no tienen influencia en usuarios externos(Von Solms, 1999).

The Institute of Internal Auditors (2012), indica que sin declaraciones claras de políticas, las organizaciones pueden desorientarse y actuar de manera ineficaz. Una política mal diseñada a pesar de que se encuentre documentada, presentará algunas debilidades. De acuerdo con Lineman (2006), la falta de formación y educación formal de los usuarios, el no cumplimiento de las directrices de seguridad (ISACA, 2010) y la ausencia de un claro entendimiento de la política, no permite al personal ejecutar correctamente sus responsabilidades(West-Brown et al., 2003). Así mismo, una política de seguridad demasiado compleja reduce la satisfacción de los usuarios (Mattord & Whitman, 2004), impidiendo que los empleados operen de manera efectiva(Anderson, 2013).

Debido a que las directrices sobre seguridad deben ser ideadas y aprobadas por la Dirección (The Institute of Internal Auditors, 2012), la falta de apoyo de la misma y una política que no esté alineada en todo momento con los objetivos de la organización, dará como resultado una política de seguridad confusa y contraproducente (Mattord & Whitman, 2004).

Por otro lado, una política no actualizada, no revisada, poco estructurada que se ha ido ajustando a una necesidad percibida en un momento determinado dentro de la organización, que no tiene claro las sanciones establecidas ante su incumplimiento, así como la falta de transparencia y de coherencia entre política, procedimiento y norma, dará como resultado políticas de seguridad peligrosas (Edwards, 2012).

Es así que las políticas de seguridad se han convertido en elementos importantes para

garantizar la seguridad informática (Wood, 2002). Por esta razón el objetivo del presente trabajo es definir el concepto de Políticas de Seguridad de la Información (PSI) con base en su clasificación, características y objetivos por medio de una revisión sistemática. Con la finalidad de establecer un marco de referencia teórico y que la investigaciones relacionadas a la gestión de las políticas de seguridad basen sus trabajos en esta definición teórica académica.

MARCO TEÓRICO

Seguridad

De acuerdo con Whitman & Mattord (2012) la seguridad consiste en protegerse contra los adversarios, es decir estar libre de peligro; es una condición que resulta de establecer medidas de protección que pueden incluir una combinación de disuasión, prevención, detección, recuperación y corrección; que permiten a la empresa cumplir con su misión y llevar a cabo sus funciones críticas a pesar de los riesgos que plantean las amenazas(NIST, 2004). Para Laudon & Laudon (2012) la seguridad consiste en "Políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso no autorizado, la alteración, el robo o el daño físico a los sistemas de información" (p. 586)

Seguridad de la Información

Según Von Solms & Von Solms (2004), la Seguridad de la Información es una disciplina multidimensional que garantiza un entorno adecuado y seguro para los activos de información de una empresa, protegiéndolos de debilidades, vulnerabilidades, ataques, amenazas e incidentes emergentes (Myler & Broadbent, 2006). Además, la seguridad de la información protege a la información y a los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción (NIST, 2004). Esta definición implica que la seguridad de la información no es sólo una cuestión estrictamente tecnológica (Wood, 1995), sino que involucra también a personas y procesos(Montesino & Fenz, 2011).

Por otro lado, es importante mencionar que cuando se habla de Seguridad de la Información se hace referencia a tres aspectos claves: Confidencialidad, Integridad y Disponibilidad (Baumann & Schmid, 2006; Whitman & Mattord, 2012; Yusufovna & Kim, 2007; Montesino & Fenz, 2011); los cuales se logran a través de la aplicación de políticas, educación, formación, conocimiento y la tecnología (Whitman & Mattord, 2012).

Confidencialidad

La confidencialidad se refiere a la protección de la información contra accesos no autorizados (Chris Hare, 2001; Paar & Pelzl, 2010; Whitman & Mattord, 2012), evitando que la información sensible sea divulgada a entidades del sistema como usuarios, procesos y dispositivos (Whitman & Mattord, 2012).

Whitman & Mattord (2012) indican que la confidencialidad está estrechamente relacionada con la privacidad. Asi mismo, sostenienen que para proteger la confidencialidad de la información se pueden emplear diferentes, medidas entre las que se incluyen: clasificación de la información, almacenamiento seguro de documentos, aplicación de políticas generales de seguridad y educación a usuarios finales y custodios de la información.

Integridad

Kissel (2013) la integridad consiste en proteger la información contra modificaciones o destrucciones inadecuadas, asegurando el no repudio y la autenticidad; proporciona a la información la característica de ser oportuna, precisa, completa(Jonnaganti, 2009) y que llegue al receptor cuando éste la solicite(Chris Hare, 2001). Es así que, hay dos categorías de integridad: a) la integridad de la fuente, que garantiza que los datos provienen del remitente correcto y; b) la integridad de los datos(Baumann & Schmid, 2006).

Garantiza la confianza de que la información no ha sido alterada (Baumann & Schmid, 2006), que los datos son válidos y que es un

requisito para que la información y los programas se cambien sólo de manera específica y autorizada. La integridad se suele aplicar mediante un conjunto de reglas o restricciones propias de cualquier sistema de información (Jonnaganti, 2009).

Disponibilidad

La disponibilidad garantiza el acceso inmediato a los recursos de información (Farooq, Waseem, Khairi, & Mazhar, 2015; Baumann & Schmid, 2006; Yusufovna & Kim, 2007), no sólo en condiciones normales sino también en condiciones de desastre. Permite a los usuarios o sistemas informáticos autorizados acceder a la información sin interferencias u obstrucción y en el formato requerido (Whitman & Mattord, 2012). Por otro lado, la disponibilidad significa que los sistemas utilizados para almacenar y procesar la información, los controles de seguridad empleados como protección y los canales de comunicación funcionen correctamente (Yusufovna & Kim, 2007).

Gestión de la Seguridad de la Información

Es un proceso que define cómo se deben gestionar los problemas de la seguridad de la información en la empresa y/o la organización; debe ser establecida e implementada de modo que apoye las operaciones de la organización y se logren las metas estratégicas (Toivanen, 2015). La gestión de seguridad de la información no es simplemente la instalación de soluciones técnicas; está formada por muchos componentes que incluyen personas, políticas, procedimientos, procesos, estándares y tecnologías (Bhaskar & Ahson, 2008).

Así mismo y de acuerdo a lo expresado por Kazemi, Khajouei, & Nasrabadi (2012) la gestión de la seguridad de la información es el conjunto de actividades cuyo objetivo es proteger los activos de información minimizando los riesgos; por lo tanto la gestión de riesgos es una parte esencial de la gestión de la seguridad de la información, ya que permite identificar sistemáticamente los riesgos de seguridad de los activos, analizarlos y evaluarlos (Brunner, 2016), adoptando el enfoque de mejora continua (Humphreys, 2008). De acuerdo con (Kazemi et al., 2012), los objetivos de la gestión de la seguridad de la información son los mismos que persigue la seguridad de la información; sin embargo y debido al incremento en el procesamiento y almacenamiento de la información, también es importante considerar nuevos conceptos (Lim Thow-Chang, n.d.) y expandir el triángulo de seguridad con términos como: no repudio, responsabilidad y autenticidad (Rantonen, 2014).

No repudio

El no repudio implica la garantía de que el remitente de la información y el destinatario prueban su identidad, haciendo imposible más tarde que puedan negar haber procesado la información (Kissel, 2013).

Autenticidad

Es la propiedad que tienen los datos, transacciones, comunicaciones o documentos de ser genuinos; además, valida que las partes involucradas sean las que dicen ser (Yusufovna & Kim, 2007).

Responsabilidad

Especifica que todos los que participan en la seguridad de la información tienen responsabilidad específica por sus operaciones (Chris Hare, 2001), asegurando que las acciones de una entidad pueden ser rastreadas únicamente a la entidad (Lim Thow-Chang, n.d.) y que todas las acciones en el sistema pueden atribuirse a una identidad autenticada (Rantonen, 2014).

METODOLOGÍA.

El desarrollo de este artículo se basó en la revisión sistemática de literatura planteada por (Kitchenham, 2004), los pasos son descritos a continuación:

1. Planeación

1.1 Necesidad de una revisión sistemática

En esta etapa se consideran las razones para realizar una revisión sistemática; ésta generalmente surge como una necesidad de los investigadores para resumir la información existente sobre un tema o fenómeno de manera completa e imparcial, con el objetivo de sacar conclusiones más generales sobre un fenómeno o como preludio de nuevas actividades de investigación.

1.2 Desarrollo de un protocolo de revisión

Especifica los métodos que se utilizarán para el proceso de revisión; además reduce la posibilidad de sesgo del investigador. Un protocolo debe incluir:

- Razón de ser del estudio.
- Pregunta de investigación que pretende ser respondida.
- Estrategias de búsqueda en la que se incluyen los términos de búsqueda y los recursos a buscar como: revistas específicas, bases de datos y actas de congresos.
- Estudiar procedimientos y criterios de selección, para determinar cuales se van a incluir o excluir en la revisión.
- Evaluar la calidad de los estudios.
- Definir una estrategia de extracción de datos.
- Especificar plan de revisión.

1.2.1 Formular la pregunta de investigación

La pregunta de investigación debe ser significativa e importante tanto para los profesionales como para los investigadores. Esta debe estar estructurada desde tres puntos de vista: población, intervención y resultados.

1.3 Revisión del protocolo

El protocolo es un elemento crítico que debe ser sometido a procedimientos de revisión.

2. Revisión

Una vez finalizado el protocolo inicia el proceso de revisión. Los pasos en esta fase son documentados a continuación:

2.1 Identificación de la Investigación

El objetivo de esta etapa es encontrar tantos estudios primarios sobre el tema de investigación como sea posible, utilizando una estrategia de búsqueda imparcial.

2.1.1 Generación de una estrategia de búsqueda

En una revisión de literatura es necesario elaborar una estrategia de búsqueda a través de la combinación de términos derivados de la pregunta de investigación, revisiones de resultados y consultas con expertos. Además, se pueden construir cadenas de búsqueda empleando los operadores Booleanos AND y OR. Inicialmente esta búsqueda utiliza bases de datos electrónicas, sin embargo esta puede ampliarse incluyendo listas de referencia de estudios primarios relevantes, revistas, literatura gris, registros de investigación e internet.

2.1.2 Sesgo de publicación

Esta etapa aborda el problema del sesgo de publicación, el cual crea una tendencia a publicar aquellas investigaciones con resultados positivos, menoscabando aquellas cuyos resultados no son significativos.

2.1.3 Gestión bibliográfica y recuperación de documentos

Las referencias bibliográficas de la revisión sistemática deben ser administradas adecuadamente a través de paquetes bibliográficos.

2.1.4 Documentación de la búsqueda

El proceso de búsqueda debe ser transparente y replicable de modo que los lectores puedan evaluarla.

2.2 Selección del estudio

2.2.1 Criterios de selección del estudio

En esta fase se pretende identificar los estudios primarios que provean evidencia directa sobre la pregunta de investigación y deberían decidirse en el protocolo de revisión. Además, se deben probar los criterios de inclusión y exclusión para asegurar que sean interpretados de manera confiable y que los estudios sean clasificados correctamente.

2.2.2 Proceso de selección de estudios

En el proceso de selección los resultados deben ser evaluados y los criterios de inclusión y exclusión deben ser considerados una vez se han obtenido los textos completos de los documentos; así mismo, es de utilidad mantener una lista de estudios excluidos debidamente identificados.

2.2.3 Confiabilidad de las decisiones de inclusión

La inclusión y la exclusión de los estudios debe ser investigada por más de un investigador a través del análisis de sensibilidad.

2.3 Evaluación de la calidad del estudio

Además de evaluar los criterios de inclusión y exclusión, se debe evaluar la calidad de los estudios primarios a través de: criterios de inclusión y exclusión más detallados, investigar y explicar las diferencias de resultados, orientar la interpretación de los resultados y encaminar a investigaciones futuras.

2.3.1 Umbrales de calidad

Se debe realizar una evaluación del diseño del estudio para garantizar un mínimo de calidad.

2.3.2 Desarrollo de instrumentos de calidad

La evaluación de la calidad suele basarse en instrumentos de calidad, que permiten a los investigadores evaluar las diferencias en las ejecuciones de los estudios dentro de las categorías de diseño. Para la evaluación se utilizan listas de verificación a las que se les asigna escalas numéricas, de modo que se obtienen evaluaciones numéricas de calidad.

2.4 Extracción de los datos

En esta etapa se deben diseñar formularios que registren la información obtenida de las fuentes primarias, de modo que se reduzca la posibilidad del sesgo.

2.4.1 Diseño del formulario de extracción de datos

Los formularios deben ser diseñados para recopilar toda la información, abordar la pregunta de investigación y los criterios de calidad del estudio. En la mayoría de los casos la extracción de datos definirá un conjunto de datos numéricos para cada estudio. Los datos numéricos son importantes al momento de resumir los resultados.

2.4.2 Contenido de los formularios de extracción

Además de incluir los datos para responder la pregunta de investigación y los criterios de evaluación de calidad, los formularios deben incluir: nombre de la revisión, fecha de extracción de los datos, título, autores, publicación, detalles de la publicación y espacio para datos adicionales.

2.4.3 Procedimiento de extracción de los datos

La extracción de los datos debe ser realizada independientemente por varios investigadores, los datos deben ser comparados y en caso de desacuerdos éstos deben ser resueltos a través de consensos o por arbitraje de un investigador independiente.

2.4.4 Publicaciones múltiples de los mismos datos

Cuando existen publicaciones duplicadas, se deben incluir las más recientes, evitando incorporar múltiples publicaciones de los mismos datos.

2.4.5 Datos no publicados, datos faltantes y datos que requieren manipulación

En el caso de existir estudios que se están realizando, éstos deben ser incluidos; además se puede obtener información de calidad de los propios autores porque en los informes no siempre se incluyen todos los datos relevantes.

2.5 Síntesis de los datos

Esta etapa se centra en recopilar y resumir los resultados de los estudios. La síntesis de los datos puede ser descriptiva que puede ser complementada con un resumen cuantitativo. El uso de técnicas estadísticas para la síntesis cuantitativa se conoce como *metaanálisis*.

2.5.1 Síntesis descriptiva

La información extraída debe tabularse de manera coherente con la pregunta de revisión. Las tablas deben estructurarse para resaltar similitudes y diferencias entre los resultados del estudio; es importante identificar si los resultados son consistentes o inconsistentes.

2.5.2 Síntesis cuantitativa

Los resultados cuantitativos deben ser presentados de manera comparable.

2.5.3 Presentación de resultados cuantitativos

Uno de los mecanismos más comunes para presentar datos cuantitativos es un gráfico forestal.

2.5.4 Análisis de sensibilidad

El análisis de sensibilidad es importante cuando se realiza un metaanálisis completo.

2.5.5 Sesgo de publicación

Los gráficos en embudo son empleados como medio para evaluar la posibilidad de que una revisión sistemática es vulnerable al sesgo de publicación.

2.6 Presentación del informe de la revisión

Las revisiones sistemáticas pueden ser reportadas en dos formatos: como sección en una tesis doctoral, en una revista o en una conferencia.

ANÁLISIS DE RESULTADOS

1. Pregunta de Investigación

La pregunta de investigación abordada para este estudio es:

¿Cuál es el concepto de Políticas de Seguridad de la Información con base en su clasificación, características y objetivos?

2. Proceso de Búsqueda

El proceso de búsqueda en la base de datos ISI Web of Knowledge. El criterio de selección establecido incluía términos en el título y en el abstract como: *information, security, policies, guideline, guidance, management, assurance*; además se incluyó el operador booleano OR para combinar los criterios de búsqueda en una sola expresión que pueda ser interpretada por el buscador, es así que, la exploración se realizó con la instrucción: *((information security policy) or (information security guideline) or (information assurance guideline) or (Information security policies) or (Policy protection information) or (information security guidance) or (information security guide) or (information security management))*, obteniéndose inicialmente un total de 7342 resultados.

3. Criterios de inclusión y exclusión

La búsqueda de la información se limitó a Políticas de Seguridad de la Información, ya que lo que se pretende elaborar es un concepto sobre estas con base en su clasificación, características y objetivos. Para la revisión de la literatura, se estableció un periodo de 10 años (2006 – 2016).

La extracción de los datos y debido a la gran cantidad de resultados obtenidos, la búsqueda se limitó a la categoría *Computer Science*

Information Systems, excluyéndose categorías como *Medical Informatics, Automation Control Systems, Health case sciences services, Geography, Engineering electrical electronic, Business, Engineering aerospace, remote sensing, metereology, geochemistry geophysics, Mathematics applied, Communication, Astronomy, Astrophysics, Engineering multidisciplinary, Telecomunications, Computer science cybernetics, Computer science Artificial Intelligence, Computer science theory methods or computer science interdisciplinary applications or computer science software engineering or computer science hardware architecture,* obteniendo un total de 306 resultados.

Para la clasificación de la información se examinaron revistas en cuyo resumen y conclusiones incluía términos del tema de investigación, encontrándose un total de 33 documentos categorizados de acuerdo a su factor de impacto (ver Tabla 1).

Tabla 1
Artículos clasificados

Factor de impacto	Artículos
Q1	7
Q2	22
Q3	2
Q4	2
Total	**33**

Los documentos clasificados fueron sometidos a una nueva revisión por tres expertos en al área para identificar únicamente aquellos que aportaban a las PSI, recabando información de 17 artículos de los cuales 3 son Q1, 10 tienen un factor impacto Q2, 2 artículos corresponden a Q3 y 2 a Q4.

4. Recopilación de los datos

El criterio de selección de los artículos fue por la indexación de las revistas en Web of Science, inicialmente se consideraron aquellas revistas categorizadas en cuartil 1 (Q1) y en cuartil 2 (Q2). Luego se incluyeron las ubicadas en cuartil 3 (Q3) y cuartil 4 (Q4) con la finalidad de ampliar la información. No se consideró tesis doctorales, conferencias, libros ni otro tipo de fuentes, porque se consultó referencias de alto impacto sometidas a procesos de valoración para medir su calidad, factibilidad y rigurosidad científica (Michele, Hincapié, Jackman, Uribe, & Carlo, 2008), como es el caso de los artículos de las revistas científicas, que para su aprobación y publicación deben sujetarse a la revisión por pares como un mecanismo que controla la importancia de la evidencia científica (Plaséncia, García, & Fernández, 2001).

5. Análisis de Resultados

Con base en la información obtenida (ver Apéndice 1), los datos se clasificaron en tres tablas: 1) clasificación, 2) características y 3) objetivos. En cada una de las tablas se buscaba determinar qué criterios se repetían y qué autores los mencionaban.

La Tabla 2 revela que de los 19 autores citados, el 45,16% es decir 11 de ellos, determinan que las PSI son un documento, aclarando que se excluyó a los autores Doherty y Fulford debido a que se referencian nuevamente en el año 2009. Por otro lado, el 32,26% de los autores consideran a las políticas de seguridad de la información como un mecanismo.

Tabla 2. Clasificación de las Políticas de Seguridad de la Información

	AUTORES – AÑOS																					Porcentajes
CLASIFICACIÓN	Wadlow, T. A. 2000	Dhillon G 2001	Backhouse J. 2001	Baskerville, R. 2002	Siponen, M. 2002	Stephen Hinde 2002	Hone K 2002	Eloff JHP. 2002	von Solms, B 2004	von Solms, R. 2004	Whitman 2004	Doherty, N.F. 2005	Fulford, H. 2005	I.S.O. 2005	Boss Sr. 2007	Kirsch L J 2007	Doherty, N.F.2009	Anastasakis, L. 2009	Fulford, H. 2009	Herath T 2009	Rao HG. 2009	
Documento		1	1	1	1							1	1	1	1	1	1	1	1	1	1	45,16%
Comercial				1	1																	6,45%
Negocio												1	1									6,45%
Trabajo																	1	1	1			9,68%
Mecanismo	1					1	1	1	1	1	1						1	1	1			32,26%

Para determinar las características de las políticas de seguridad, se incluyeron los criterios de la Tabla 3 que en su frecuencia son mayores al 5%. Dando como resultado que los criterios: define reglas (5,77%), involucra personas (6,73%), implementa la gestión de cambios (7,69%), establece derechos (8,65%), establece el canal de comunicación (8,65%), define accesos (9,62%) y establece límites del comportamiento (13,46%). Mientras que el objetivo de las mismas es garantizar la gestión de la seguridad de la información (44,23%) o la seguridad de la información (38.46%) [Ver Tabla 4].

Tabla 3. Características de la Seguridad de la Información

CARACTERÍSTICAS DE LAS POLÍTICAS DE SEGURIDAD	AUTORES- AÑOS																																																Porcentajes
	Davis GB 1985	Olson MH. 1985	Lindup, K. R. 1995	Hone, K 2002	Eloff, J. H. P. 2002	Richards, N.2002	Rees, J 2003	Bandyopadhyay, S 2003	Spafford, E. H. 2003	Whitman 2004	Hong, K. 2006	Chi, Y. 2006	Chao, L. 2006	Tang, J. 2006	Ding Guoli 2006	Chen Jianhua 2006	Lax R.F. 2006	Chen Peter 2006	Wahsheh L. A. 2006	Alves-Foss J. 2006	Da Veiga A. 2007	Eloff J. H. P. 2007	White G. 2009	Hedstrom K 2011	Kolkowska E 2011	Karlsson F 2011	Allen J. 2011	Kolkowska Ella 2012	Dhillon Gurpreet 2012	Anthor Peter 2014	Kuhnhauser W. E. 2014	Polck Anja 2014	Chen H 2014	Li W. 2014	Solic Kresimir 2015	Ocevcic Hrvoje 2015	Golub Marin 2015	Tsohou Aggeliki 2015	Karyda Maria 2015	Kokolakis Spyros 2015	Horcas J. M. 2015	Pinto Mónica 2015	Fuentes L. 2015	Mallouli W. 2015	Montes de Oca E.2015	Al Hogail Areej 2015	Lee Chunghun 2016	Lee Choong C. 2016	Kim Suhyun 2016	
Establece responsabilidades										1																																								0,96%
Define accesos										1					1	1	1	1	1	1	1	1																								1				9,62%
Establece los espacios de notificaciones										1													1																											1,92%
Define sanciones										1																							1	1																2,88%
Define mecanismo de actualización										1																																								0,96%
Establece derechos				1	1		1	1	1		1	1	1	1																																				8,65%
Establece el canal de comunicación				1	1		1	1	1		1	1	1	1																																				8,65%
Se basa en Riesgos			1																			1	1																											2,88%
Estudia problemas de seguridad							1	1	1																																									2,88%
Implementa controles de seguridad				1	1																																													1,92%
Definida en contexto de planificación y control	1	1																																																1,92%
Establece límites de comportamiento	1	1				1																		1	1	1	1						1	1							1	1	1	1	1					13,46%
Establece límites en la toma de decisiones	1	1																																																1,92%
Establece límites en el uso de estándares	1	1																																																1,92%
Define reglas																				1								1	1	1	1	1																		5,77%
Protege la información																												1	1																					1,92%
Implementa la gestión de cambios																							1					1	1												1	1	1	1	1					7,69%
Involucra personas																						1													1	1	1	1	1	1										6,73%
Involucra Procesos																						1													1	1	1													3,85%
Involucra Tecnología																						1													1	1	1													3,85%
Controla de cumplimiento de seguridad																				1																											1	1	1	3,85%
Concientiza a los usuarios por políticas																						1																												0,96%
Compatible con leyes internas y externas																							1																											0,96%
Deben abordar temas de privacidad																							1																											0,96%
Establece controles de seguridad																				1																														0,96%
Administra recursos																				1																														0,96%
Especifica el qué, cómo y por qué los datos/recursos deben ser protegidos																				1																														0,96%

Tabla 4. Objetivos de las Políticas de Seguridad de la Información

OBJETIVO	AUTORES – AÑOS																																													
	Straub DW. 1990	Lindup, K. R. 1995	Dhillon, G. 1997	Higgins Huong Nao 1999	Dhillon, G. 2000	Backhouse, J. 2000	Wadlow, T. A. 2000	Stephen Hinde 2002	Baskerville, R. 2002	Siponen, M. 2002	Rees, J., 2003	Bandyopadhyay, S. 2003	Spafford, E. H. 2003	von Solms, B. 2004	von Solms, R. 2004	Whitman 2004	I.S.O. 2005	Doherty, N.F. 2005	Fulford, H. 2005	Wahsheh Lu'ay A. 2006	Alves-Foss Jim 2006	Ashenden D. 2008	Doherty, N.F. 2009	Anastasakis, L. 2009	Fulford, H., 2009	Herath, T. 2009	Rao, H.R. 2009	Hone K.2009	Eloff JHP. 2009	White Garry 2009	Kolkowska Ella 2012	Dhillon Gurpreet 2012	ISO/IEC 27002.2013	Tsohou Aggeliki 2015	Karyda Maria 2015	Kokolakis Spyros 2015	Areej Al Hogail 2015	**Porcentaje**
Salvaguardar activos de conocimiento organizacional								1															1	1	1																				7,69%
Seguridad de la Información	1				1	1	1		1	1						1	1	1	1				1	1	1	1	1	1	1		1	1	1											38,46%
Gestionar la seguridad de la información		1	1	1							1	1	1	1	1		1	1	1	1	1	1	1	1	1	1	1							1	1	1	1								44,23%
Difusión y aplicación de prácticas sólidas de seguridad dentro de la organización									1	1								1	1																										7,69%
Asegurar que los sistemas se desarrollen y operen de manera segura																													1																1,92%

Con base en la evidencia de las Tablas 2,3 y 4 se puede definir a las políticas de seguridad como un documento o mecanismo que define accesos y reglas, que involucra a personas y establece derechos, canales de comunicación y límites de comportamiento; además de implementar la gestión de cambios y tienen como objetivo garantizar la seguridad de la información o la gestión de la seguridad de la información.

CONCLUSIONES

Los resultados de esta revisión sistemática integran la información existente sobre PSI, logrando conceptualizar su definición con base a su clasificación, características y objetivos. Para ello se realizó el análisis de diferentes artículos científicos en los que se abordaba términos relacionados al tema de investigación, tomando como referente para el desarrollo la metodología propuesta por Kitchenham.

Este trabajo contribuye significativamente a la teoría de la Gestión de Seguridad de la Información debido a que establece las bases teóricas para que las metodologías de la Gestión de PSI actualicen sus procesos y buenas prácticas. Para los profesionales específicamente en el área de auditoria de Tecnologías de la Información, la definición establecida les permitirá a los auditores alinear sus informes de las buenas prácticas como la ISO 2007:2001, ITIL, COBIT o COSO, con una visión integradora y holística con fundamentos teóricos y no solamente con juicios de expertos.

Existen algunas limitaciones al presente trabajo. Una de ellas es que la única fuente de búsqueda fue Web of Knowledge sin embargo, los trabajos indizados en esta base de datos tienen un alto impacto y calidad académica. Por otro lado, no se consideraron artículos de conferencias o tesis doctorales que pueden ampliar o ratificar el concepto construido. Otra limitación es el periodo de búsqueda debido a que el tiempo de búsqueda fue sólo de diez años.

Con base en este trabajo científico surge la necesidad de realizar la misma investigación, pero en fuentes no estructuradas aplicando técnicas de vigilancia tecnológica enfocadas en las compañías auditoras y contrastar el concepto profesional que se pueda obtener con el concepto académico de esta revisión sistemática. Los resultados de este contraste permitirían conocer el grado de acuerdo entre la empresa y la academia con respecto a PSI.

Referencias Bibliográficas

Al Hogail, A. (2015). Cultivating and Assessing an Organizational Information Security Culture ; an Empirical Study. *International Journal of Security and Its Applications*, *9*(7), 163–178.

Anderson, J. (2013). Information Security for SME's (pp. 11–14).

Baldecchi, R. (2014). *Implementación efectiva de un SGSI ISO 27001*. *2014*. Retrieved from http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014 - Exposición 2 CIGRAS ISO 27001 - rbq.pdf

Baumann, R., & Schmid, S. (2006). Voice Over IP - Security and SPIT Swiss Army, FU Br 41, KryptDet Report. *Challenges*, 1–33.

BBVA. (2016). *Situación Economía Digital*.

Bhaskar, S. M., & Ahson, S. I. (2008). Information Security A Practical Approach, 276.

Brunner, M. (2016). RiskFlows – Continuous Risk-driven Workflows and Decision Support in Information Security Management Systems.

Chris Hare. (2001). INFORMATION SECURITY POLICIES, PROCEDURES, AND STANDARDS: ESTABLISHING AN ESSENTIAL CODE OF CONDUCT. *Auerbach Publications*, 31.

Control Data. (1999). *Why Security Policies Fail*. *Policy*.

Deloitte. (2016). Los Riesgos de la Tecnología de la información en los servicios financieros : Lo que los miembros de la junta necesitan saber – y hacer.

Edwards, B. W. (2012). Implementing Information Security Policies and Standards A Real Life Example, (November).

Farooq, M., Waseem, M., Khairi, A., & Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, *111*(7), 1–6. https://doi.org/10.5120/19547-1280

HM Government. (2015). *INFORMATION SECURITY BREACHES SURVEY 2015*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010

ISACA. (2010). IT Standards , Guidelines , and Tools and Techniques for Audit and Assurance and Control Professionals Current as of 16 August 2010. *Professional Ethics*, (August), 329.

Jonnaganti, V. (2009). *An Integrated Security Model for the Management of SOA Improving the attractiveness of SOA Environments through a strong Architectural Integrity*. University of Gothenburg. Retrieved from https://gupea.ub.gu.se/bitstream/2077/20518/1/gupea_2077_20518_1.pdf

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors : Case study of Municipal organization, *6*(14), 4982–4989. https://doi.org/10.5897/AJBM11.2323

Kissel, R. (2013). Glossary of Key Information Security Terms Glossary of Key Information Security Terms. *Nist*, *NISTIR 729*(Revision 2). https://doi.org/10.6028/NIST.IR.7298r2

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(TR/SE-0401), 28. https://doi.org/10.1.1.122.3308

Laudon, K. C., & Laudon, J. P. (2012). *Sistemas de información gerencial* (Décimo seg). México.

Lim Thow-Chang, K. S.-M. and A. F. (n.d.). Information Security Management Systems and standards.

Lineman, D. J. (2006). Information Security Policy Concerns for Laptops and Portable Devices.

Lineman, D. J. (2011). The Total Cost of Information Security Policy Management. *Solution Brief*, 1–11.

Mattord, H. J., & Whitman, M. E. (2004). Teaching Information Security Policy, (June).

Michele, L. D. G. C., Hincapié, J., Jackman, J., Uribe, C., & Carlo, V. (2008). Revisión por pares : ¿ Qué es y para qué sirve ? Peer Review : what it ' s and what it ' s for ? *Redalyc*, *24*(2), 258–272.

Montesino, R., & Fenz, S. (2011). Information security automation: How far can we go? *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, 280–285. https://doi.org/10.1109/ARES.2011.48

Myler, E., & Broadbent, G. (2006). Standard for Security. *The Information Management Journal*, (December).

Niekerk, J. Van, & Solms, R. Von. (2006). Understanding Information Security Culture. *Proceedings of the ISSA 2006 from Insight to Foresight Conference*.

NIST. (2004). FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. *Fips*, *199*(February 2004), 13.

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography* (Springer). Berlin.

Plaséncia, a, García, A., & Fernández, E. (2001). La revisión por pares: ¿buena, mala o todo contrario? *Gaceta Sanitaria*, *15*(1), 378–379.

PricewaterhouseCoopers. (2016). *Encuesta Global de Información*.

Rantonen, K. (2014). Explaining Information Security Behavior – Case of the Home User.

Schlienger, T., & Teufel, S. (2003). Information security culture: from analysis to change. *South African Computer Journal*, *31*(31), 46–52.

The Institute of Internal Auditors. (2012). Information Technology Risk and Controls. *Global Technology Audit Guide*, *2nd editio*, 36. Retrieved from http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag12nded.pdf

Toivanen, H. (2015). Case Study of Why Information Security Investment Decision Fail ?

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50–58. https://doi.org/10.1108/09685229910255223

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). *SEI Digital Library*, (April), 223. https://doi.org/CMU/SEI-2003-HB-002

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information Security*. (C. Technology, Ed.) (Fourth). Boston. https://doi.org/http://dx.doi.org/10.1016/B978-0-12-381972-7.00002-6

Wood, C. C. (1995). Writing infosec policies. *Computers & Security*, *14*(8), 667–674. https://doi.org/10.1016/0167-4048(96)81706-8

Wood, C. C. (2002). *Políticas de Seguridad Informática - Mejores Prácticas Internacionales*. (NetIQ, Ed.).

Yusufovna, S. F., & Kim, T. (2007). IT Security Review : Privacy , Protection , Access Control , Assurance and System Security, *2*(2), 17–32.

Apéndice 1. Datos Bibliográficos

#	AUTORES					Título	Revista	Año de Publicación	Factor de Impacto
	Autor 1	Autor 2	Autor 3	Autor 4	Autor 5				
1	Ding, Guoli	Chen, Jianhua	Lax, R.F	Chen, Peter		Graph-theoretic method for merging security system specifications	Information Sciences an International Journal	2007	Q1
2	Doherty, Neil	Anastasakis, L	Fulford, Heather			The information security policy unpacked: A critical study of the content of university policies	International Journal of Information Management	2009	Q1
3	Stahl, Bernd C	Doherty, Neil	Shaw, Mark			Information security policies in the UK healthcare sector: a critical evaluation	Information System Journal	2011	Q1
4	Doherty, Neil	Fulford, Heather				Aligning the information security policy with the strategic information systems plan	Computers & Security	2006	Q2
5	Knappa, Kenneth J	Morris, Franklin Jr.	Marshall, Thomas E	Byrd, Terry Anthony		Information security policy: An organizational-level process model	Computers & Security	2009	Q2
6	Kolkowska, Ella	Dhillon, Gurpreet				Organizational power and information security rule compliance	Computers & Security	2013	Q2
7	Amthor, Peter	Kuhnhauser, Winfried E.	Polck, Anja			WorSE: A Workbench for Model-based Security Engineering	Computers & Security	2014	Q2
8	Solic, Kresimir	Ocevcic, Hrvoje	Golub, Marin			The information systems' security level assessment model based on an ontology and evidential reasoning approach	Computers & Security	2015	Q2
9	Zimmermann Montesdioca, Gustavo Percio	Gastaud Macada, Antonio Carlos				Measuring user satisfaction with information security practices	Computers & Security	2015	Q2
10	Tsohou, Aggelik	Karyda, Maria	Kokolakis, Spyros			Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs	Computers & Security	2015	Q2
11	Flowerday, Stephen V	Tuyikeze, Tite				Information security policy development and implementation: The what, how and who	Computers & Security	2016	Q2
12	Lee, Chunghun	Lee, Choong C	Kim, Suhyun			Understanding information security stress: Focusing on the type of information security compliance activity	Computers & Security	2016	Q2
13	Horcas, Jose-Miguel	Pinto, Mónica	Fuentes, Lidia	Mallouli, Wissam	Montes de Oca, Edgardo	An approach for deploying and monitoring dynamic security policies	Computers & Security	2016	Q2
14	White, Garry					Strategic, Tactical, & Operational Management Security Model	Journal of Computer Information Systems	2009	Q3
15	Da Veiga, A	Eloff, J.H.P				An Information Security Governance Framework	Information Systems Management	2007	Q3
16	Wahsheh, Lu'ay A	Alves-Foss, Jim				Specifying and enforcing a multi-policy paradigm for high assurance multi-enclave systems	Journal of High Speed Networks	2006	Q4
17	Al Hogail, Areej					Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study	International Journal of Security and Its Applications	2015	Q4