Disponible en línea en www.sciencedirect.com

CienciaDirecta
CienciaDirecta

000–000 Disponible en línea en www.sciencedirect.com
Procedia Informática 00 (2019) 000–000

CienciaDirecta

Procedia Informática 161 (2019) 1216–1224

www.elsevier.com/locate/procedia
www.elsevier.com/locate/procedia

Procedia
Computer Science

www.elsevier.com/locate/procedia

La Quinta Conferencia Internacional de Sistemas de Información 2019
La Quinta Conferencia Internacional de Sistemas de Información 2019

Cumplimiento de la política de seguridad de la información: literatura sistemática
Cumplimiento de la política de seguridad de la información: literatura sistemática
Revisar
Revisar

Angrainia,d,*, Rose Alinda Alisa,b Okfalisac
Angrainia,d,*, Rose Alinda Alisa,b Okfalisac

a Escuela de Informática, Facultad de Ingeniería, Universiti Teknologi Malaysia, 81310 Johor, Malasia a Escuela
[b]Departamento de Sistemas de Información, Facultad de Ingeniería, Universiti Teknologi Malaysia, 81310 Johor, Malasia
[b]Departamento de Sistemas de Información, Facultad de Ciencias y Tecnología, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau c
[d]Departamento de Sistemas de Información, Facultad de Ciencias y Tecnología, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau c
[c]Departamento de Sistemas de Información, Facultad de Ciencias y Tecnología, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau

Resumen
Resumen

El crecimiento de la investigación en seguridad de las tecnologías de la información se ha ampliado en los últimos años. Investigaciones en seguridad de la información. El crecimiento de la investigación en seguridad de la tecnología de la información se ha incrementado en los últimos años. Las investigaciones en seguridad de la información además de discutir problemas técnicos, también consideran cuestiones de políticas, el comportamiento y las cuestiones de cumplimiento del usuario. Por lo tanto, se necesita una revisión sistemática para informar el desarrollo de la investigación en el cumplimiento de las políticas de seguridad de la información. Esta revisión de la literatura tiene como objetivo encontrar los desafíos y explorar el estado actual del arte del cumplimiento de la política de seguridad de la información. Identificamos 309 trabajos de investigación publicados sobre temas de cumplimiento de política de seguridad de la información entre 2014 y 2019, y extrajimos 53 documentos de discusiones con criterios de inclusión y exclusión. Esta revisión de la literatura encontró que hay una falta de estudio sobre una evaluación del cumplimiento de la política de seguridad de la información usando una métrica específica y la necesidad de mejorar el modelo de cumplimiento de la política de seguridad de la información con teorías organizacionales.

conformidad con las teorías organizacionales. © 2019 Los autores. Publicado por Elsevier BV © 2019 Los autores. Publicado por Elsevier BV
© 2019 Los autores. Publicado por Elsevier BV
Este es un artículo de acceso abierto bajo la licencia CC BY-NC-ND (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Este es un artículo de acceso abierto bajo la licencia CC BY-NC-ND (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Revisión por pares bajo la responsabilidad del comité científico de The Fifth Information Systems International Conference 2019.
Peer-review bajo responsabilidad del comité científico de The Fifth Information Systems International Conference 2019 Palabras clave:
Política de seguridad de la información; Cumplimiento; Revisión de literatura; Evaluación Palabras clave: Política de seguridad de la información; Cumplimiento; Revisión de literatura; Evaluación

1. Introducción
1. Introducción

La política de seguridad de la información es un documento para garantizar los activos de información y la información de tecnología segura con un procedimiento específico para respaldar los objetivos de la organización [1]. La política de seguridad de la información garantiza un procedimiento específico de activos de información para respaldar los objetivos de la organización [1]. La política de seguridad de la información garantiz

* Autor correspondiente. Tel.: +62-813-2636-8388.
Dirección de correo electrónico: angraini@uin-suska.ac.id

1877-0509 © 2019 Los autores. Publicado por Elsevier BV

Revisión por pares bajo la responsabilidad del comité científico de The Fifth Information Systems International Conference 2019

1877-0509 © 2019 Los autores. Publicado por Elsevier BV
Este es un artículo de acceso abierto bajo la licencia CC BY-NC-ND (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Revisión por pares bajo la responsabilidad del comité científico de The Fifth Information Systems International Conference 2019.
10.1016/j.procs.2019.11.235

y tecnología de la información segura con un procedimiento específico para respaldar el objetivo y la meta de una organización. un tema importante es el apoyo de la gerencia durante la implementación de las políticas de seguridad de la información. Cuando se obtiene el apoyo, otro desafío que se enfrenta es garantizar que las políticas sean realmente capaces de mejorar la seguridad [2]. La gestión será comparada con productos técnicos; la eficiencia de las políticas de valor es más difícil de lograr. Esto siempre es más fácil para los productos técnicos, porque a menudo pueden debatir la eficiencia en función de las estadísticas. Aunque la organización implementó la política de valores, el empleado ignoró la regla y el comportamiento inesperado. Sin cumplimiento, las políticas solo están en el papel en el que están impresas o en los bits en los que están almacenadas. El cumplimiento de las políticas tiene como objetivo garantizar la aplicación de los estándares de seguridad organizacionales [3]. Investigadores anteriores han investigado para formular el modelo de cumplimiento del usuario con las políticas de seguridad de la información. Bulgurcu (2010) investiga los factores basados en la racionalidad que alientan a un empleado a cumplir con los requisitos del ISP en relación con la protección de los recursos de información y la tecnología organizacional y argumenta que las actitudes de los empleados están influenciadas por los beneficios de cumplimiento, los costos de cumplimiento y los costos de incumplimiento, que son creencias sobre la valoración. como consecuencia del cumplimiento o incumplimiento[4] . Los usuarios no se dieron cuenta de la importancia del cumplimiento de la política de seguridad hasta que ocurren incidentes y las organizaciones tienen un impacto y deben incurrir en costos adicionales debido al comportamiento de incumplimiento. Phamz (2015) explora la literatura para descubrir la relevancia de la motivación del usuario, la regulación y la orientación del usuario hacia el cumplimiento de la seguridad de la información [5]. Se han realizado varias investigaciones para aprender sobre el cumplimiento de la seguridad de la información, la mayoría de las investigaciones se realizan para averiguar qué factores influyen en el comportamiento de cumplimiento del usuario. Claramente existe un enfoque de insuficiencia y falta de soluciones para mejorar el comportamiento de cumplimiento de los usuarios con las políticas de seguridad de la información. Todavía se puede explorar más información para aumentar la comprensión del cumplimiento Por lo tanto, es necesario realizar una revisión sistemática de la literatura para encontrar tendencias y desafíos de investigaciones anteriores. Una revisión sistemática eficaz de la literatura requiere preguntas de investigación específicas para mantenerse enfocado. Por lo tanto, esta revisión de la literatura identifica las revistas más importantes en el campo del cumplimiento de la seguridad de la información y encuentra tendencias y desafíos en el cumplimiento de la seguridad de la información. Este documento está estructurado: la sección 2 presenta el método de investigación utilizado para producir una revisión de la literatura sistemáticamente y discute las estrategias para estudios primarios y criterios de selección de estudios. La sección 3 presenta los datos extraídos de la revisión de datos que se ha llevado a cabo en forma de estadísticas. La sección 4 presenta un análisis de los hallazgos y directrices para futuras investigaciones. Finalmente, la Sección 5 presenta las conclusiones.

2. Metodología

El procedimiento de revisión de la literatura utilizado en este estudio es una revisión sistemática de la literatura. Una revisión sistemática de la literatura es un proceso sistemático, explícito y completo para identificar, evaluar y sintetizar los resultados de los trabajos producidos por investigadores, académicos y profesionales. El proceso de revisión de literatura tiene cuatro etapas antes de escribir una reseña; planificación, selección, extracción y ejecución [6]. La etapa de planificación es la primera etapa que definirá el propósito de la revisión de la literatura y el protocolo que se llevará a cabo para obtener la literatura por las preguntas de investigación. Luego se realiza la búsqueda bibliográfica utilizando las palabras clave y se aplica a la biblioteca digital. Explica la calidad de los resultados de la búsqueda para garantizar los resultados encontrados antes de realizar la extracción de datos. Realizó análisis cuantitativos y cualitativos para analizar los hallazgos y conclusiones arrojados a causa de la revisión. Una revisión sistemática eficaz de la literatura requiere preguntas de investigación específicas para mantenerse enfocado. Las preguntas de investigación para esta revisión de la literatura se explican en la Tabla 1.

Tabla 1. Pregunta de investigación para la revisión de la literatura.

——	Pregunta de investigación	Apuntar
RQ 1	¿Qué revista es el tema de cumplimiento de seguridad de la información más importante publicado?	Identificar las revistas más importantes en el campo del cumplimiento de la seguridad de la información
RQ 2	¿Qué tipos de tendencias y desafíos en el campo de cumplimiento de la seguridad de la información seleccionan?	Identificar tendencias y desafíos en el cumplimiento de la seguridad de la información
RQ 3	¿Qué tipo de teorías se utilizan en el cumplimiento de las políticas de seguridad de la información?	Identificar las tendencias de las teorías utilizadas en el modelo de cumplimiento de políticas de seguridad de la información

La estrategia de búsqueda bibliográfica tiene una función significativa en la extracción de información en el artículo de revisión. Las etapas del proceso de búsqueda consisten en determinar la base de datos, definir las palabras clave y los términos a buscar, determinar las cadenas de búsqueda y ejecutar la palabra clave [7]. La base de datos utilizada en este estudio elegido en función de la cantidad de datos y el campo de estudio. La lista de bases de datos digitales utilizadas en el proceso de búsqueda son: Scopus (www.scopus.com), Web of Science (http://apps.webofknowledge.com), ProQuest (www.proquest.com), Springer Link (https://link.springer.com), Jstor (www.jstor.org), IEEE explore (ieeexplore.ieee.org), [illegible] biblioteca aisel.aisnet.org). La búsqueda de progreso utilizando las cadenas y la combinación de palabras clave incluyen: política/políticas de seguridad de la información, cumplimiento/conformidad [illegible] nes artículo de la revista, la tesis, la sección del libro y las actas de congresos y están escritas en inglés. Después de la fase de búsqueda, la siguiente fase seleccionó para responder a la pregunta de investigación de revisión de la literatura. Los criterios de selección del trabajo determinan y aplican en los criterios de inclusión y exclusión. Los criterios de selección de artículos debían ser explícitos por escrito porque ayuda a los investigadores a decidir y mantener el rumbo durante el proceso de búsqueda: criterios de inclusión y exclusión descritos en la Tabla 2.

Tabla 2. Tabla de criterios de inclusión y exclusión.

Criterios de inclusión	escrito en ingles
	tiempo de publicación en 2014 a 2018
	estudiar la discusión sobre el comportamiento humano en las políticas de seguridad de la información y sobre el cumplimiento de la organización en el área de seguridad de la información, tecnología de la información y sistema de información de gestión
	si se encuentra un artículo similar en una conferencia y una revista, solo se incluirá de la revista
Criterio de exclusión	estudios sin validación y resultado experimental
	estudios del informe de la organización, artículos de opinión y editoriales
	estudios circunstanciales sobre cultura organizacional, cumplimiento y psicología del comportamiento

Esta investigación utiliza el software de gestión de referencias de Mendeley (http://mendeley.com) para guardar los resultados de la búsqueda y recopilar artículos. Para el proceso de búsqueda detallada, esta investigación adopta un proceso de selección basado en las directrices PRISMA es un conjunto de elementos mínimos basados en la evidencia para informar en revisiones sistemáticas y metanálisis [8]. PRISMA es un método que se puede utilizar para informar revisiones sistemáticas de investigaciones posteriores. Para simplificar el proceso de creación de búsqueda, PRISMA proporciona una herramienta generadora de diagramas de flujo (http://prisma.thetacollaborative.ca). Los resultados del diagrama de flujo del proceso de búsqueda del artículo de este estudio se pueden ver en la Fig. 1.

El proceso de selección de artículos produjo 59 artículos, que fueron los estudios primarios en este estudio. Los criterios utilizados además de los descritos en los criterios de inclusión y exclusión también utilizan estudios de calidad, duplicación de varias bases de datos utilizadas. Además, la relevancia con la pregunta de investigación y la similitud de los estudios incluyen un proceso de selección de texto con Finalmente, se encuentra el artículo principal que será discutido en esta investigación. La siguiente etapa es extraer los datos generados a partir del proceso de selección utilizando el estándar de codificación de datos/extracción de archivos. Se extraerán los artículos principales para recopilar datos que contribuirán a responder las preguntas de investigación de esta revisión. Para cada uno de los 59 estudios principales seleccionados, solo se utilizan 52 artículos para el análisis posterior, seis artículos eliminados debido a un artículo de revisión y uno de los artículos es un artículo de patente. Solo se utilizarán trabajos de investigación con datos empíricos y el formulario de extracción de datos se haya completado. El formulario de extracción de datos está diseñado para recopilar datos de los estudios primarios necesarios para responder preguntas de investigación; esta investigación utiliza el software cualitativo NVIVO para analizar datos en una revisión sistemática de la literatura [9]. El siguiente proceso es crear un mapa conceptual para apoyar el proceso de codificación y análisis, desde los mapas conceptuales se pueden crear nodos para explorar y describir datos de patrones. El mapa conceptual comienza con la investigación del tema sobre el cumplimiento de la política de seguridad de la información, luego se determinan los nodos de acuerdo con el propósito de la pregunta de investigación. Por lo tanto, es necesario crear un nodo sobre el problema, los c

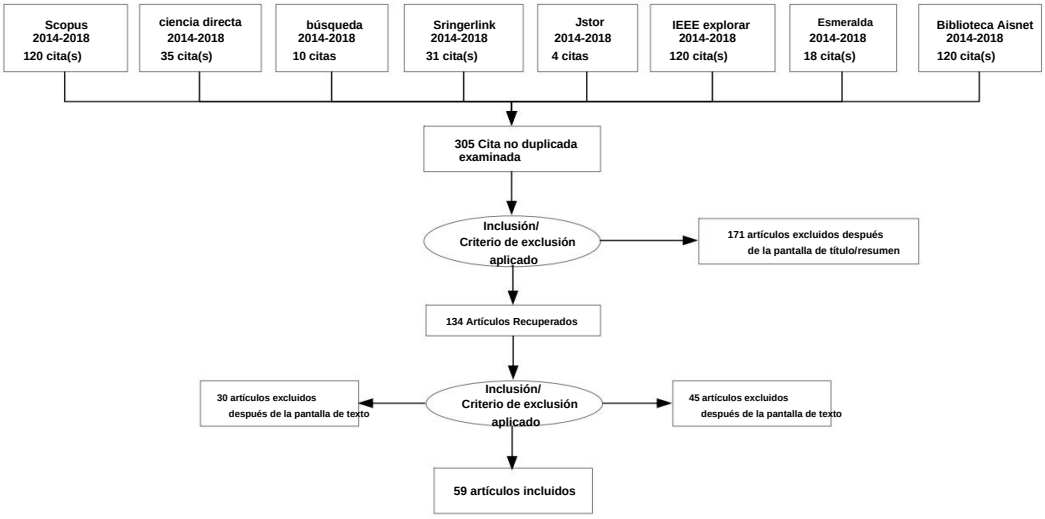

Fig. 1. Diagrama de flujo de selección de artículos.

3. Resultado y hallazgo

La última etapa de la revisión sistemática de la literatura es el análisis de hallazgos cuantitativos y cualitativos. Los hallazgos de la revisión de la literatura responderán a la pregunta de investigación de la revisión de la literatura. Los resultados de la revisión de la literatura sobre el cumplimiento de la política de seguridad de la información encontraron 59 artículos que consisten en 35 artículos de revistas, 22 artículos de actas de congresos, una sección de libro y una tesis. El cumplimiento de las políticas de seguridad de la información se ha convertido en la atención de los investigadores en los últimos cinco años. Por lo tanto, el número de investigaciones en este don Además, se publicarán dos artículos para el próximo 2019. Este tema de investigación lidera con un enfoque cuantitativo, de los cuales se encontraron 59 artículos, 64% fueron cuantitativos, 26% cualitativos y 10% utilizaron métodos mixtos.
La revista de seguridad informática y de la información es el tema de cumplimiento de la seguridad de la información publicado más importante. Además, revistas acreditadas como informática y seguridad, información y gestión, revista de sistemas de información y revistas de computación suave publicaron algunos artículos sobre este tema y otro artículo publicado en la conferencia anual. Basado en RQ 1 de una revisión sistemática de la literatura, la revista de seguridad informática y de la información es el tema de cumplimiento de seguridad de la información de la revista publicada más importante. Durante cinco años, el objetivo del investigador es encontrar los factores que influyen en el cumplimiento de la política de seguridad de la información, la intención de comportamiento y el cumplimiento de la medida. El estudio anterior estudia mayoritariamente el comportamiento humano para encontrar factores que influyan en los empleados para cumplir con las políticas de seguridad de la información. Las personas son a menudo la conexión más débil, a través de la cooperación y la coordinación, también pueden ser una fuente de gran fuerza en el desarrollo de defensas que sean efectivas y eficientes [10]. La figura 2 describe la tendencia de un objetivo de investigación de 2014 a 2019.

Figura 2. Tendencia del objetivo de la investigación.

La implementación de una política de seguridad de la información puede fracasar si los usuarios no cumplen con los requisitos de seguridad. Los factores individuales (directos o indirectos) pueden afectar la intención del comportamiento de cumplir con las políticas de seguridad y su comportamiento de seguridad general [11]. Por lo tanto, se realizaron muchas investigaciones para determinar los factores que influyen en el cumplimiento de las políticas de seguridad de la información y las intenciones de comportamiento del usuario para adherirse a las po La investigación sobre el comportamiento humano en el cumplimiento de las políticas de seguridad de la información examina los factores que hacen que los usuarios cumplan con las políticas implementadas. Según los resultados de la revisión de la literatura, hasta el 47 % de los estudios encontraron factores humanos que influyen en las intenciones del comportamiento del usuario para cumplir con la seguridad de la información y el 38 % realizó pruebas empíricas de los factores del comportamiento humano que afectan el cumplimiento de las políticas de seguridad de la información, mientras que solo el 15 % de los investigadores medir el comportamiento del usuario. Sin embargo, aún faltan investigadores que evalúen el cumplimiento de las políticas de seguridad de la información. Este hallazgo responde a la RQ 2 para identificar las tendencias y desafíos en el cumplimiento de la seguridad de la información. La Tabla 3 describe el objeto de investigación resumen de inv

Tabla 3. Objetivo de investigación del estudio anterior.

Objetivo de la investigación	Autor
Intención de comportamiento	[12, 13. 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35]
Influir en los factores humanos para cumplir	[19,24,36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55]
Evaluación y medición del cumplimiento de la política de seguridad de la información	[41,56, 57, 58, 59, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61]

La medición del cumplimiento de las políticas de seguridad de la información no puede utilizar estándares internacionales como la ISO 27001 porque las políticas de seguridad de la información desarrolladas por las organizaciones difieren según las características organizacionales [62]. Históricamente, la investigación de seguridad de IS se ha concentrado en evaluar los efectos de los fenómenos sobre las intenciones de comportamiento en lugar del comportamiento real. Merrit (2016) cree que existe una brecha entre las intenciones de comportamiento y el comportamiento real, especialmente sobre el cumplimiento de las políticas de seguridad de la información porque muchos de los que se encuentran en estudios anteriores ven una motivación de cumplimiento que tendrá un impacto en las intenciones de comportamiento [20]. Hay varios estudios publicados sobre el comportamiento humano en la seguridad de la información. Esta revisión de la literatura que encuentra 29 teorías sobre el comportamiento humano y 13 teorías organizacionales se ha utilizado en la investigación del cumplimiento de la seguridad de la información. Este hallazgo responde a la RQ 3 a las teorías que se utilizan en el cumplimiento de las políticas de seguridad de la información. La teoría que más se utiliza es la teoría del comportamiento planificado (TPB). Esta teoría es la teoría fundamental del estudio del comportamiento humano. TPB predice la intención-comportamiento en función de las actitudes personales (estado mental), la presión social de los demás (normas subjetivas) y una sensación de control (control conductual percibido) [63]. Sin embargo, las intenciones de comportamiento pueden volverse activas solo si el comportamiento está bajo control volitivo y normas. Abed (2016) afirma que la intención del usuario hace que cumpla con la política o la rechace [12]. Los investigadores usan otras teorías para explorar factores humanos significativos para proteger la información. La siguiente teoría comúnmente utilizada es la Teoría de disuasión general (GDT). La teoría de la disuasión general utilizada por los investigadores porque supone que evaluar el comportamiento preventivo eliminará las amenazas a la seguridad de la información y reducirá el riesgo. La teoría de la teoría de la motivación de protección se considera capaz de conocer el comportamiento humano para mantener la seguridad de la información. La PMT se formuló primero como una teoría comparativa del miedo antes de expandirse a una teoría más general de la comunicación persuasiva [64,65]. Esta teoría sostiene que dos procesos cognitivos pueden determinar las intenciones individuales de realizar un comportamiento protector, es decir, su motivación protectora. El estudio de moody (2018) ofrece probablemente el análisis empírico más completo de un modelo de cumplimiento de políticas de seguridad de la información con once teorías [41]. Aunque utiliza teorías complejas, la investigación de Moody todavía no tiene un elemento cultural, por lo que es posible que se necesite más investigación para poder teorizar y examinar las diferencias culturales.

4. Discusión

Una revisión sistemática de la literatura es un método de revisión que se puede utilizar para encontrar y sintetizar estudios previos. Este

El método es mejor que el método tradicional porque el proceso de búsqueda y el proceso de obtención del análisis están estructurados. Los resultados del estudio de revisión de la literatura mostraron que la cantidad de investigación en el campo de las políticas de cumplimiento de seguridad de la información está creciendo. La implementación de la política de seguridad de la información tendrá más éxito si el usuario puede cumplir con el requisito. A partir del análisis de la revisión bibliográfica se pueden encontrar dos BPA de investigación.

1. Faltan estudios sobre la evaluación del cumplimiento de las políticas de seguridad de la información.

El comportamiento interno de los empleados produce un comportamiento de seguridad que la organización debe observar y monitorear para garantizar el cumplimiento de la política aplicada. Se deben realizar evaluaciones periódicas y aleatorias para garantizar el cumplimiento. Por ejemplo, las evaluaciones de conciencia de seguridad y los programas de capacitación con métricas y producen un porcentaje de usuarios del sistema que reciben capacitación de conciencia básica, la tasa de personal de seguridad en los sistemas de información que recibe educación en seguridad y la tasa de usuarios con contraseñas que se alinean con las estrategias de seguridad. 66]. Las políticas de seguridad deben seguir revisándose y actualizándose periódicamente teniendo en cuenta los cambios en las circunstancias, el entorno, las necesidades cambiantes en el contexto empresarial y el riesgo identificado. Las organizaciones que desarrollan políticas de seguridad de la información basadas en las necesidades y tipos de organizaciones no utilizan correctamente las reglas existentes sobre estándares o mejores prácticas para evaluar sus políticas de seguridad de la información. Esta evaluación provocará calificaciones bajas porque ignoran los estándares o las mejores prácticas al desarrollar una política de seguridad de la información. En el contexto de la universidad, evaluar el cumplimiento de las políticas ayudará a la organización a conocer el nivel de cumplimiento de los usuarios de tecnologías de la información. De modo que disminuirá el nivel de amenazas a la seguridad de la información que provienen del comportamiento de los usuarios a los que no les importa.

2. Necesita mejorar el modelo de cumplimiento de las políticas de seguridad de la información con las teorías de la organización.

El comportamiento de seguridad de la información tiene la oportunidad de combinar personas, tecnología y organizaciones. Comprender el comportamiento individual mejorará el comportamiento positivo y reducirá el comportamiento dañino. Comprender el comportamiento humano podrá mejorar el cumplimiento de las políticas al conocer la motivación, la modificación y la prevención [67] y continuar investigando puede mejorar el cumplimiento del usuario [12]. Por lo tanto, es necesario estudiar otro factor que incide en los empleados para cumplir con las políticas de seguridad de la información. Su apoyo con el impacto significativo de la variable organizacional en el aumento de la efectividad durante la implementación de la gestión de la seguridad de la información [68]. La investigación sobre este tema se ha restringido principalmente a comparaciones limitadas de la teoría sobre el comportamiento humano. Por lo tanto, es necesario considerar factores humanos y factores organizacionales para evaluar el cumplimiento de las políticas de seguridad de la información [69,70].

5. Conclusión

Este documento encontró Research GAP del estudio anterior. Primero, la investigación sobre el cumplimiento de la seguridad de la información utiliza en su mayoría la teoría del comportamiento humano; necesita más estudio de otros factores que pueden influir en el cumplimiento de la teoría organizacional. En segundo lugar, la falta de estudio para evaluar el cumplimiento de la política de seguridad de la información. Es necesario seguir investigando para desarrollar instrumentos que puedan utilizarse para medir el cumplimiento de las políticas de segurida Por lo tanto, es necesario desarrollar un modelo a partir de la teoría organizacional y la teoría del comportamiento humano para medir el cumplimiento. Este modelo esperado puede ser aplicado por las organizaciones para mejorar el cumplimiento de los usuarios y conocer la efectividad de las políticas de seguridad de la información.

Referencias

[1] Doherty, NF y H. Fulford H. (2006) "Alineación de la política de seguridad de la información con el plan estratégico de sistemas de información". computar Seguridad 25: 55–63. doi:10.1016/j.cose.2005.09.009.

[2] Nohlberg, M. (2009) "Por qué los humanos son el eslabón más débil". Soc. Tararear. elemental información Seguro emergente Tendencias. pags. 22

[3] Barry, L. (2013) Desarrollo de políticas de seguridad de la información para el cumplimiento, Boca Raton, CRC Press Taylor & Francis Group.

[4] Bulgurcu, B., H. Cavusoglu e I. Benbasat. (2010) "Cumplimiento de la política de seguridad de la información: un estudio empírico de la racionalidad Creencias y conciencia sobre la seguridad de la información". MIS Q 34: 523–48. doi:10.1093/bja/aeq366.

[5] Phamz, CH y M. Nkhoma. (2015) "Cumplimiento de la seguridad: nueva perspectiva de las orientaciones de objetivos y la teoría de la autorregulación", en WMSCI 2015 - 19º Sistema Mundial de Conferencias Múltiples. cibernético Informática, Proc. 2.

[6] Okoli, C. y K. Schabram. (2010) "Una guía para realizar una revisión sistemática de la literatura sobre la investigación de sistemas de información". Papanicolaou de trabajo Inf Syst 10: 1–51. doi:10.2139/ssrn.1954824.

[7] Bandara, W., S. Miskon y E. Field. (2011) "Un método sistemático respaldado por herramientas para realizar revisiones de literatura en SI". Sistema Inf J. págs. 1 a 14.

[8] Liberati, A., DG Altman, J. Tetzlaff, C. Mulrow, PC Gøtzsche, JPA Ioannidis, et al. (2009) "La Declaración PRISMA para Reportar Revisiones sistemáticas y metanálisis de estudios que evalúan intervenciones de atención médica: explicación y elaboración". BMJ Br Med J. doi: 10.1136/bmj.b2700.

[9] O'Neill, MM, SR Booth y JT Lamb. (2018) "Uso de NVivo™ para revisiones de literatura: la pedagogía de los ocho pasos (N7+1)". El Informe Cualitativo 23 (13): 21-39. Disponible en: https://nsuworks.nova.edu/tqr/vol23/iss13/. [Consultado el 12 de agosto de 2019].

[10] Safa, NS y R. Von Solms. (2016) "Un modelo de intercambio de conocimientos sobre seguridad de la información en las organizaciones". Calcular el comportamiento humano 57: 442–51. doi:10.1016/j.chb.2015.12.037.

[11] Consolvo, S. y M. Langheinrich. (2015) "Identificación de factores que influyen en el comportamiento de seguridad de los empleados para mejorar el cumplimiento de los ISP". priv. Seguro Cómputo ACM SIGCAS. Soc. 31: 8–23. doi:10.1145/503345.503347.

[12] Abed, J., G. Dhillon y S. Ozkan. (2016) "Investigación del comportamiento de cumplimiento continuo de la seguridad: conocimientos de los sistemas de información Modelo de continuación", en Vigésimo segundo Am. Conf. Inf. Syst. San Diego. p. 1–10.

[13] Alzahrani, A., C. Johnson y S. Altamimi S. (2018) "Cumplimiento de la política de seguridad de la información: investigación del papel de la motivación intrínseca hacia el cumplimiento de la política en la organización", en 2018 4th Int. Conf. información Gerente, IEEE. pags. 125–32. doi:10.1109/INFOMAN.2018.8392822.

[14] Hwang, I., D. Kim, T. Kim y S. Kim. (2017) "¿Por qué no cumplir con la seguridad de la información? Un enfoque empírico para las causas de Incumplimiento." Online Inf Rev 41: 2–18. doi:10.1108/OIR-11-2015-0358.

[15] Ifinedo, P. (2014) "Cumplimiento de la política de seguridad de los sistemas de información: un estudio empírico de los efectos de la socialización, la influencia y la cognición". Inf Manag 51: 69–79. doi:10.1016/j.im.2013.10.001.

[16] Kajtazi, M., B. Bulgurcu, H. Cavusoglu e I. Benbasat. (2014) "Evaluación del efecto del costo hundido en las intenciones de los empleados de violar Políticas de seguridad de la información en las organizaciones", en Proc. Annu. Hawaii Int. Conf. Syst. Sci. pp. 3169–77. doi:10.1109/HICSS.2014.393.

[17] Kajtazi, M., H. Cavusoglu, I. Benbasat y D. Haftor. (2018) "Escalada de Compromiso como Antecedente de Incumplimiento de Política de seguridad de la información." Inf Comput Secur 26: 171–93. doi:10.1108/ICS-09-2017-0066.

[18] Kim, HL y J. Han. (2018) "¿Cumplen mejor los empleados de una "buena" empresa con la política de seguridad de la información? Perspectiva de responsabilidad". Inf Technol People. ITP-09-2017-0298. doi:10.1108/ITP-09-2017-0298.

[19] Lowry, PB y GD Moody. (2015) "Propuesta del modelo de cumplimiento de control-reactancia (CRCM) para explicar las motivaciones opuestas a Cumplir con las políticas de seguridad de la información de la organización". Inf Syst J 25: 433–63. doi:10.1111/isj.12043.

[20] Merritt, CD y GS Dhillon. (2016) "¿Qué interrumpe la intención de cumplir con la política de seguridad de SI?" Vigésima segunda am. Conf. información sist. pags. 1–10.

[21] Nasir, A., RA Arshah y MR Ab Hamid. (2017) "Comportamiento de cumplimiento de la política de seguridad de la información basado en dimensiones integrales de la cultura de seguridad de la información", en Proc. Internacional de 2017 Conf. información sist. Datos mín. - ICISDM '17. pags. 56–60. doi:10.1145/3077584.3077593.

[22] Rajab, M. y A. Eydgahi. (2019) "Evaluación del poder explicativo de los marcos teóricos sobre la intención de cumplir con la información Políticas de seguridad en la educación superior". Comput Secur 80: 211–23. doi:10.1016/j.cose.2018.09.016.

[23] Siponen, M., M. Adam Mahmood y S. Pahnila. (2014) "Adherencia de los empleados a las políticas de seguridad de la información: un estudio de campo exploratorio". Inf Manag 51: 217–24. doi:10.1016/j.im.2013.08.006.

[24] Amankwa, E., M. Loock y E. Kritzinger. (2018) "Establecimiento de la Cultura de Cumplimiento de Políticas de Seguridad de la Información en las Organizaciones". Inf Comput Secur 26: 420–36. doi:10.1108/ICS-09-2017-0063.

[25] Sommestad, T., H. Karlzén y J. Hallberg. (2015) "Un metaanálisis de estudios sobre la teoría de la motivación de protección y la seguridad de la información Comportamiento". Int J Inf Secur Priv 9: 26–46. doi:10.4018/IJISP.2015010102.

[26] Stewart, H. y J. Jürjens. (2017) "Gestión de la Seguridad de la Información y el Aspecto Humano en las Organizaciones". 5. doi:10.1108/ICS-07-2016-0054.

[27] Yakimin, Y. y G. Dhillon. (2015) "Intenciones de cumplimiento del ISP del empleado: una prueba empírica de empoderamiento del empleado", en Treinta Sexta Int. Conf. información sist. pags. 1–26.

[28] Yazdanmehr, A. y J. Wang. (2016) "Cumplimiento de la política de seguridad de la información de los empleados: una perspectiva de activación de normas". Decir Sistema de soporte 92: 36–46. doi:10.1016/j.dss.2016.09.009.

[29] Aurigemma, S. y T. Mattson. (2017) "Privilegio o procedimiento: evaluación del efecto del estado del empleado en la intención de cumplir con las amenazas y controles de seguridad de la información socialmente interactivos". Comput Secur 66: 218–34. doi:10.1016/j.cose.2017.02.006.

[30] Aurigemma, S. y T. Mattson. (2017) "Impactos de la experiencia de disuasión y castigo en las actitudes de cumplimiento de los ISP". Inf Comput Secur 25: 421–36. doi:10.1108/ICS-11-2016-0089.

[31] Bauer, S., EWN Bernroider y K. Chudzikowski. (2017) "¡Más vale prevenir que curar! Diseño de programas de concientización sobre seguridad de la información para superar el incumplimiento de las políticas de seguridad de la información en los bancos por parte de los usuarios". Comput Secur 68: 145–59. doi:10.1016/j.cose.2017.04.009.

[32] Doherty, NF y ST Tajuddin. (2018) "Hacia una teoría centrada en el usuario del cumplimiento de la seguridad de la información impulsada por el valor". Tecnología de información Gente 31: 348–67. doi:10.1108/ITP-08-2016-0194.

[33] Garz. V. (2015) "Asegurar BYOD: un estudio de los efectos de encuadre y neutralización en el cumplimiento de la política de seguridad de dispositivos móviles", en Proc. 36 Int. Conf. información sist. pags. 1–10.

[34] Han, JY, YJ Kim y H. Kim. (2017) "Un Modelo Integrador de Cumplimiento de la Política de Seguridad de la Información con el Contrato Psicológico: Examinando una perspectiva bilateral". Comput Secur 66: 52–65. doi:10.1016/j.cose.2016.12.016.

[35] Humaidi, N. y V. Balakrishnan. (2015) "El efecto moderador de la experiencia laboral en el comportamiento de cumplimiento de las políticas de seguridad del sistema de información de salud". Malasia J Comput Sci 28: 70–92.

[36] Alalwan, JA. (2018) "El miedo al cibercrimen y el cumplimiento de las políticas de seguridad de la información: un estudio teórico", en IC4E 2018. p. 85–7. doi:10.1145/3183586.3183590.

[37] Hina, S. y DD Dominic. (2016) "Políticas de Seguridad de la Información: Investigación del Cumplimiento en las Universidades", en el 3er Int. Conf. computar información ciencia ICCOINS 2016 - Proc., 2016. pág. 564–9. doi:10.1109/ICCOINS.2016.7783277.

[38] Huang, H., N. Parolia y KT. Cheng. (2016) "Voluntad y capacidad para realizar un comportamiento de cumplimiento de la seguridad de la información: propiedad psicológica y perspectiva de autoeficacia", en Pacific Asia Conf. información sist. doi:10.1186/1471-2334-12-S1-O4.

[39] Maphanga, GC y O. Jokonya. (2017) "El riesgo de los comportamientos negativos de los usuarios en la política de cumplimiento de seguridad de la información en Organizaciones". Risk Gov Control Financ Mark Institutions 7: 30–40. doi:10.22495/rgc7i4art4.

[40] Merhi, MI y J. Leighton. (2015) "La alta dirección puede reducir la resistencia hacia el cumplimiento de la seguridad de la información", en Thirty Sixth Int. Conf. información sist. pags. 1–11.

[41] Moody, GD, M. Siponen y S. Pahnila. (2018) "Hacia un modelo unificado de cumplimiento de políticas de seguridad de la información". MIS Q 42: 285–311. doi:10.25300/MISQ/2018/13853.

[42] Parque, M. y S. Chai. (2018) "Internalización de la política de seguridad de la información y la práctica de seguridad de la información: una comparación con Cumplimiento", en Proc. 51st Hawaii Int. Conf. Syst. Sci. 9: 4723–31. doi:10.24251/HICSS.2018.595.

[43] Razilan, M., A. Kadir, S. Norwahidah, S. Norman, SA Rahman y A. Bunawan. (2017) "Cumplimiento de Políticas de Seguridad de la Información entre Empleados en Ciberseguridad Khalid S . Soliman International Business Information Management Association (IBIMA)", en Proc. 28th Int. Bus. Inf. Manag. Assoc. Conf.

[44] Sharma, S y M. Warkentin. (2018) "¿Realmente pertenezco?: Impacto del estado de empleo en el cumplimiento de la política de seguridad de la información". Seguridad informática doi:10.1016/j.cose.2018.09.005.

[45] Sikolia, D., D. Twitchell y G. Sagers. (2016) "Adherencia de los empleados a las políticas de seguridad de la información: una réplica parcial", en Proc. Soy. Conf. información sist. pags. 1–9. doi:10.1109/ICMTMA.2009.433.

[46] Sillic, M. (2019) "Impacto crítico de la inercia organizacional e individual para explicar el comportamiento de seguridad no conforme en The Shadow Contexto de TI". Comput Secur 80: 108–19. doi:10.1016/j.cose.2018.09.012.

[47] Talib, YYA (2015) Motivación intrínseca y cumplimiento de la política de seguridad de los sistemas de información en las organizaciones.

[48] Tsohou, A. y P. Holtkamp. (2018) "¿Son los usuarios competentes para cumplir con las políticas de seguridad de la información? Un análisis de los modelos de competencia profesional". Inf Technol People 31: 1047–68. doi:10.1108/ITP-02-2017-0052.

[49] Alshare, KA, PL Lane y MR Lane. "Cumplimiento de la política de seguridad de la información: un estudio de caso de educación superior". Inf Comput Secur 26: 91–108. doi:10.1108/ICS-09-2016-0073.

[50] Arage, T., F. Belanger y T. Beshah. (2015) "Influencia de la cultura nacional en el cumplimiento de los empleados con las políticas de seguridad de los sistemas de información (ISS): hacia la cultura ISS en las empresas etíopes", en AMCIS 2015 Proc. pags. 1–7.

[51] Bansal, G. y SI Shin. (2016) "Efecto de interacción de género y técnicas de neutralización en el cumplimiento de la política de seguridad de la información: Una perspectiva ética", en AMCIS 2016 Surfing IT Innov. Wave - 22nd Am. Conf. Inf. Syst. p. 1–10.

[52] Chen, X., D. Wu, L. Chen y JKL Teng. (2018) "Severidad de las sanciones de información y gestión y cumplimiento de la política de seguridad de la información de los empleados: investigación de las variables de mediación, moderación y control". Inf Manag 55: 1049–60. doi:10.1016/j.im.2018.05.011.

[53] Choi, M. y J. Song. (2018) "Control social a través de la disuasión sobre el cumplimiento de la política de seguridad de la información". Informática blanda 22: 6765–72. doi:10.1007/s00500-018-3354-z.

[54] Chulkov, DV (2017) "Escalada del compromiso y la seguridad de la información: teorías e implicaciones". Inf Comput Secur 25: 580–92. doi:10.1108/ICS-02-2016-0015.

[55] D'Arcy, J. y PB Lowry. (2017) "Motores Cognitivo-Afectivos del Cumplimiento Diario de los Empleados con las Políticas de Seguridad de la Información: A Estudio longitudinal multinivel". Inf Syst J. pp. 1–27. doi:10.1111/isj.12173.

[56] Alkhurayyif, Y. y GRS Weir. (2017) "La legibilidad como base para la evaluación de políticas de seguridad de la información", en 2017 Seventh Int. Conf. emergente Seguro Tecnología pags. 114–21. doi:10.1109/EST.2017.8090409.

[57] Jin, J., L. Ouyang y X. Gu. (2015) "Uso de Galois Lattice para representar y analizar el cumplimiento de la política de seguridad de la información". Asia internacional Conf Ind Eng Manag Innov 1: 239–43. doi:10.2991/978-94-6239-100-0.

[58] Karlsson, F., M. Karlsson y J. Åström. (2017) "Medición del cumplimiento de los empleados: la importancia del pluralismo de valores". Cálculo de información Secur 25: 279–99. doi:10.1108/ICS-11-2016-0084.

[59] Kurowski, S. (2018) "Medir el cumplimiento de los contenidos específicos de la política: las escalas SRPC y SRPCC para una medición más detallada del cumplimiento positivo de la política", en Vigésimo sexto Eur. Conf. información sist.

[60] Ross, RS (2014) "Evaluación de los controles de seguridad y privacidad en organizaciones y sistemas de información federales: creación de Planes de evaluación". NIST Spec Publ. pp. 1–487. doi:10.6028/NIST.SP.800-53Ar4.

[61] Buthelezi, MP, JAVan Der Poll y EO Ochola. (2017) "La ambigüedad como barrera para el cumplimiento de la política de seguridad de la información: un análisis de contenido", en Proc. - 2016 Int. Conf. computar ciencia computar Intel. CSCI 2016. págs. 1360–7. doi:10.1109/CSCI.2016.0254.

[62] Calder, A. y S. Watkins. (2008) Gobernanza de TI: Guía para gerentes sobre seguridad de datos e ISO 27001/ISO27002.

[63] Ajzen, I. (1991) "La teoría del comportamiento planificado". Proceso Organ Behav Hum Decis. doi:10.1016/0749-5978(91)90020-T.

[64] Rogers, RW (1975) "Una teoría de la motivación de protección de las apelaciones del miedo y el cambio de actitud". Psicología J. doi:10.1080/00223980.1975.9915803.

[65] Maddux, JE y RW Rogers. (1983) "Motivación de protección y autoeficacia: una teoría revisada de las apelaciones al miedo y el cambio de actitud". J Exp Soc Psychol. doi:10.1016/0022-1031(83)90023-9.

[66] Knapp, KJ, RF Morris, TE Marshall y T. Anthony. (2009) "Política de seguridad de la información: un modelo de proceso a nivel organizacional". Comput Secur 28: 493–508. doi:10.1016/j.cose.2009.07.001.

[67] Crossler, RE, AC Johnston, PB Lowry, Q. Hu, M. Warkentin y R. Baskerville. (2013) "Direcciones futuras para la información del comportamiento Investigación de seguridad". Comput Secur 32: 90–101. doi:10.1016/j.cose.2012.09.010.

[68] Chang, SE. (2006) "Factores organizativos para la eficacia de la implementación de la gestión de la seguridad de la información". 106. 2006.

[69] Chang, AJT, CY Wu y HW Liu. (2012) "Los efectos de la satisfacción laboral y el compromiso de la organización en la seguridad de la información Adopción y cumplimiento de políticas", en 2012 IEEE 6th Int. Conf. Manag. Innov. Technol. ICMIT. pp. 442–6. doi:10.1109/ICMIT.2012.6225846.

[70] Alotaibi, M., S. Furnell y N. Clarke. (2016) "Políticas de seguridad de la información: una revisión de los desafíos y los factores que influyen". págs. 352–8.