risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 24/06/2017
Aceitação/Acceptance: 09/09/2017

Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento

Josue Ruben Altamirano Yupanqui[1], Sussy Bayona Oré[1]

ruben.altamirano@hotmail.com, sbayonao@hotmail.com

1 Unidad de Posgrado de la Facultad de Sistemas e Informática, Universidad Nacional Mayor de San Marcos (UNMSM), Av. Germán Amézaga s/n, Lima, Perú.

DOI: 10.17013/risti.25.112-134

Resumen: Las políticas de seguridad de la información que implementan las organizaciones para protección de su información, es quizás uno de los temas que podría generar polémicas, debido a que a pesar de su existencia se producen violaciones a la seguridad de información, originadas por el factor humano. Los diferentes roles que desempeñan las personas, como: usuario final, administrador de equipos de seguridad, administrador de la información, supervisor de las políticas de seguridad, atacante a los sistemas de información, etc., tendrá un efecto y consecuencia diferente para cada caso. A través de la revisión sistemática de la literatura se ha encontrado que las teorías más relevantes que los autores están empleando en sus investigaciones relacionadas al cumplimiento de las políticas de seguridad están enfocadas a comprender el comportamiento humano a través de teorías psicológicas o sociales, lo cual conduce a tener un enfoque interdisciplinario que permita una visión global, no solo desde la perspectiva tecnológica, sino desde la perspectiva de otras disciplinas, que en su conjunto conlleve a un enfoque real del problema.

Palabras-clave: politicas de seguridad de informaciòn, revisión sistemática, cumplimiento

Information Security Policies: A Systematic Review of Theories Explaining Their Compliance

Abstract: The information security policies implemented by organizations to protect their information is perhaps one of the issues that could generate controversy, due to the fact that despite their existence there are violations of information security, caused by the human factor . The different roles that people play, such as: end user, security team administrator, information administrator, security policy supervisor, information system attacker, etc., will have a different effect and consequence for each case. Through the systematic literature review it has been found that the most relevant theories that the authors are employing in their investigations related to compliance with security policies are focused on understanding human behavior through psychological or social theories,

which leads to an interdisciplinary approach that allows a global vision, not only from a technological perspective, but from the perspective of other disciplines, which together lead to a real approach to the problem.

***Keywords**:* Information Security Policies, Systematic review, Compliance

1. Introducción

Las organizaciones públicas o privadas, implementan políticas de seguridad informáticas con el fin de proteger su información. Marcinkowski y Stanton (2003) señalaron que la política de seguridad de la información está en el corazón de los enfoques de muchas organizaciones para reforzar las conductas deseables de seguridad de la información y reforzar las restricciones contra los comportamientos de seguridad indeseables (p.2527). Según Alnatheer (2015), una política de seguridad es una parte esencial de las prácticas de seguridad dentro de las organizaciones y podría tener un impacto sustancial en su seguridad organizacional (p.1). "Sin una política, las prácticas de seguridad se desarrollarán sin una delimitación clara de los objetivos y responsabilidades" (Higgins, 1999, p.1; citado en Alnatheer, 2015, p.1).

Sin embargo, considerar que la protección de la seguridad de la información, a través de sus políticas, se llevaría a cabo solo a través de una perspectiva tecnológica, tendría un enfoque incompleto, pues los estudios que se han realizado a la fecha, demuestran que es necesario tener una visión amplia a través de un enfoque interdisciplinario, donde el principal factor, el humano, juega un papel fundamental. Tal es así, que en un reporte de Gartner (2014), menciona que las empresas deben adoptar un enfoque multifacético, apalancando personas, procesos y tecnología juntas, para crear comunidades de confianza respaldadas por la supervisión y el análisis (Walls, 2014, p.6). La tecnología no puede garantizar únicamente un entorno seguro para la información; deben tenerse en cuenta los aspectos humanos de la seguridad de la información, además de los aspectos tecnológicos (Sohrabi Safa, Solms & Furnell, 2016, p.2). Por lo tanto, las amenazas a la seguridad de la información no pueden prevenirse, evitarse, detectarse o eliminarse concentrándose únicamente en soluciones tecnológicas (Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014, p.1). Por ejemplo, respecto a la importancia del factor humano dentro de las organizaciones, los datos del 2015 de Forrester, señalan que el 39% de los tomadores de decisiones empresariales y tecnológicas de Norteamérica y Europa en firmas con 20 o más empleados que tuvieron una violación de seguridad en los últimos 12 meses dijeron que los incidentes internos dentro de su organización eran una de las maneras más comunes en que las violaciones ocurrieron (citado en Kindervag, Shey & Mak, 2016, p.3). Afirmación que coincide con un reporte de investigación de la empresa de seguridad Imperva (2016), en la que indica que les resulta preocupante que muchas brechas significativas en los datos son en última instancia en el "trabajo interno". Los iniciados, ya sean empleados, contratistas, socios comerciales o socios, representan el mayor riesgo para los datos empresariales, ya que por definición se les otorga acceso confiable a datos confidenciales (Imperva, 2016, p.2).

Por otro lado, el objetivo de asegurar la información está, en cierta medida, en conflicto con los objetivos comerciales normales de maximizar la productividad y minimizar el costo; la seguridad se ve a menudo como perjudicial para los objetivos empresariales porque hace que los sistemas sean menos utilizables (Niekerk y Solms, 2009; citado en

Van Niekerk & Von R., 2010, p.476) el único sistema absolutamente seguro es inutilizable (Wood, 2005, p.224, citado en Van Niekerk & Von R., 2010, p.476). Por ejemplo, en un reporte de la empresa de seguridad SANS, señala que uno de los desafíos que enfrentan los profesionales de la seguridad es el desarrollo de criterios de justificación de costos para invertir en contramedidas. Imagínese escuchar esta declaración: "El año pasado te dimos dinero por seguridad, y no pasó nada. ¿Por qué deberíamos darle más el próximo año? ", "Bien… Porque no pasó nada" (Mark Hardy, G., 2014, p.9).

El incumplimiento total o parcial de las políticas de seguridad informáticas, violaciones a los sistemas de información, conllevan a pérdidas económicas o de imagen de la organización, los cuales son significativas. Por ejemplo, según AT&T Cybersecurity Insights (2017), espera que los daños causados por los delitos cibernéticos lleguen a los 6 trillones de dólares anuales para el año 2021, representando la mayor transferencia de riqueza económica de la historia y los riesgos de incentivos para la innovación y la inversión. Para IBM y Ponemon Institute (2016) el costo total promedio de una violación de datos para las 383 empresas que participaron en su investigación aumentó de $ 3,79 a $ 4 millones y el costo promedio pagado por cada registro perdido o robado que contenía información sensible y confidencial aumentó de $ 154 en 2015 a $ 158 en el estudio de este año. Kaspersky Lab (2017) sostiene que en promedio las empresas pagan US$ 551 000 para recuperarse de una violación de seguridad y que las PYMES gastan 38K. Este es el gasto directo necesario para recuperarse de un ataque.

Este escenario, pone en evidencia la importancia de las políticas de seguridad en las organizaciones, por lo que una Revisión Sistemática de la Literatura (RSL) fue desarrollada en el presente documento para recolectar y analizar documentos de investigación realizadas a la fecha. En ese sentido, el presente documento tiene la siguiente estructura: la primera parte se describe de manera general la situación, problemática e impacto en las organizaciones cuyas políticas de seguridad fueron vulneradas; la segunda parte, se presenta el marco teórico necesario para comprender las teorías o conceptos relacionadas a las políticas de seguridad; en la tercera, se presenta la revisión sistemática de la literatura (RSL) como metodología empleada, su aplicación permitió la recopilación de los artículos científicos que fueron analizados y cuyos resultados de análisis son presentados.

Este trabajo es motivado por el aporte y utilidad que puede significar a los profesionales en seguridad de la información, debido a la necesidad creciente de cerrar brechas de seguridad que se originan en ataques focalizados al usuario, como por ejemplo a través de trampas de ingeniería social y que sumados a que casi todo lo utilizado por el atacante es ahora descartable genera la percepción de que ahora los atacantes avancen a un ritmo que los defensores nunca podrán alcanzar (Arbor Networks, 2017, pp. 3-4), por lo que se hace necesaria contrarestarla a través del establecimiento de políticas de seguridad que impliquen el conocimiento del comportamiento del usuario para su cumplimiento.

Este artículo esta estructurado en 6 secciones que incluye la Introducción. En la sección 2 se presenta los temas relacionados. En la sección 3 se presenta la metodología utilizada para la revisión sistemática de la literatura. En la sección 4 se presenta los resultados de la revisión sistemática. En la sección 5 se discuten los resultados y finalmente en la sección 6 se presenta las conclusiones.

2. Marco Teórico

La mayoría de las organizaciones, tienen políticas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los recursos de información. Las organizaciones desarrollan políticas y procedimientos de seguridad de la información derivados de esas políticas con la intención de mitigar los riesgos operacionales asociados con los muchos usos de los sistemas de información dentro de la empresa (Bjork, 1975; Dorey, 1991, Madnick, 1978; Moore, 2003; Schweitzer, 1990; citado por Marcinkowski y Stanton, 2003, p.2528).

Sin embargo, aparte de los controles técnicos habituales, también existe una considerable dependencia de la participación humana y este factor humano en la seguridad de la información está directamente relacionado con el comportamiento y el conocimiento humano (Kruger, Drevin, Flowerday & Steyn, 2011, p.1). Según Ahmed et al (2012) señalaron que la comunidad de investigadores de seguridad han reconocido que el comportamiento humano tiene un papel crucial en muchos fallos de seguridad, en la literatura sobre seguridad de la información, a los humanos se les suele llamar el eslabón más débil de la cadena de seguridad. Investigadores como Vroom y von Solms (2004), Stanton et al. (2005), y Pahnila et al. (2007) señalaron que es probable que las organizaciones que presten atención a los medios técnicos y no técnicos de proteger sus activos y recursos de SI (Sistemas de Información) tengan más éxito en sus intentos de proteger sus activos clave de SI (Citado en Ifindeo, 2011, p.83).

Muchos investigadores han tratado de examinar el cumplimiento de ISP (Políticas de Seguridad de la Información) en las organizaciones mediante la aplicación de varias teorías, tales como la teoría de la disuasión general (GDT), la teoría de la protección de la motivación (PMT), la teoría del comportamiento planificado (TPB), la teoría de la agencia y la teoría de la elección racional (Han, Kim & Hyungjin Kim, 2016, p.5) entre otros. En tal sentido, describiremos brevemente conceptos o teorías de mayor uso por los autores de los documentos de investigación, con el fin de que se tenga una mejor apreciación en los resultados de la presente investigación.

2.1. Seguridad de la información y Politica de Seguridad

Según la definición del ISO-27000, una declaración de política define un compromiso general, dirección o intención. Una declaración de política de seguridad de la información debe expresar el compromiso formal de la administración para la implementación y mejora de su sistema de gestión de la seguridad de la información (SGSI) y debe incluir objetivos de seguridad de la información o facilitar su desarrollo. Según la definición del ISO-27000, el propósito de la seguridad de la información es proteger y preservar la confidencialidad, integridad y disponibilidad de la información. También puede implicar proteger y preservar la autenticidad y fiabilidad de la información y garantizar que las entidades puedan ser consideradas responsables.

2.2. Teorias que explican el cumplimiento

Diversos autores han realizado, y seguirán realizando, combinaciones de diversas teorías/técnicas para analizar las violaciones a las políticas de seguridad de los sistemas de información, que se originan por la conducta humana. Por otro lado, no podemos dejar

de considerar que a través de la investigacion se genera nuevo conocimiento, por lo que podrían establecerse nuevas teorias/tecnicas, y por consiguiente se tendrian nuevas combinaciones de teorías/técnicas, en un bucle sin fin. En ese sentido, describir todas las teorías/técnicas escaparia al objetivo del presente trabajo, por lo que solo se mencionarán las mas frecuentes y algunas de menor frecuencia a efectos de comparación de conceptos.

2.2.1. Theory of Planned Behavior (TPB)

La Teoría del Comportamiento Planificado propuesto por Ajzen (citado en Ifinedo, P., 2014, p.70), postula que el comportamiento individual está influenciado por la actitud, las normas subjetivas y el control de comportamiento percibido. La actitud se define como los sentimientos positivos o negativos del individuo hacia la participación en un comportamiento especificado. Las normas subjetivas describen la percepción de un individuo de lo que las personas importantes para ellos piensan acerca de un comportamiento dado. El control cognitivo percibido se define como las creencias del individuo con respecto a la eficacia y los recursos necesarios para facilitar un comportamiento. La TPB fue desarrollada de la Theory of Reasoned Action (Teoría de la Acción Razonada).

2.2.2. Protection motivational theory (PMT)

La University of Twente (University of Twenty, 2017) sostiene que la Teoría de Protección de motivación (PMT) originalmente proponía proporcionar claridad conceptual para la comprensión de las apelaciones al miedo. Una revisión posterior de la Teoría de Protección de motivación amplió la teoría a una teoría más general de la comunicación persuasiva, con énfasis en los procesos cognitivos que median en el cambio de comportamiento. La PMT propone que la intención de proteger a uno mismo depende de cuatro factores: (1) la percepción de la gravedad de la amenaza de un evento (por ejemplo, un ataque al corazón), (2) la probabilidad percibida de la aparición, o vulnerabilidad (en este ejemplo, la vulnerabilidad percibida del individuo al escuchar un ataque), (3) la eficacia de la conducta preventiva recomendada (la percepción de la eficacia de respuesta), y (4) la percepción de auto-eficacia (es decir, el nivel de confianza en la propia capacidad para llevar a cabo el comportamiento preventivo recomendado).

2.2.3. Social bond theory (SBT)

La Teoría del Enlace Social, (Hirschi, T., 2002; citado Ifinedo, 2014, p.70) describe las vinculaciones o vínculos sociales que las personas tienen con su grupo. Hirschi (2002; citado en Ifinedo, 2014, p.70), presenta cuatro vínculos mediante los cuales se promueven la socialización y la conformidad: Apego, compromiso, participación y normas personales. La teoría postula que cuando las personas se basan en tales vínculos, su deseo de entrar en comportamientos antisociales o anti-establecimiento se reduce (Ifinedo, 2014, p.70).

2.2.4. Theory of Reasoned Action (TRA)

La Teoría de la Acción Razonada ha sido encontrado ser muy útil en la predicción de comportamiento. Sugiere que cuanto más fuerte sea la intención de involucrarse en un comportamiento, mayor será la probabilidad de que se lleve a cabo el comportamiento. En el contexto del cumplimiento de las políticas de seguridad de la información, la actitud de

un empleado hacia el cumplimiento de estas políticas combinadas con las normas sociales llevará al empleado a la intención de cumplir con las políticas de seguridad; Llevando al cumplimiento real de las políticas (Siponen M. Mahmood A. & Pahnila S., 2014, p.219).

2.2.5. Social Engineering

Las técnicas de ingeniería social realizadas por hackers educados, explotan tres elementos principales, a saber: 1) factores humanos, 2) aspectos organizativos y 3) controles tecnológicos (Frauenstein & von Solms, 2009; citado en Vouren, Kritzinger & Mueller, 2015, p.127). Las dimensiones tecnológicas normalmente implican software anti-phishing, filtros de spam, cortafuegos, etc. La dimensión humana requiere conciencia y educación eficaces para ayudar a fortalecer el "firewall humano" e idealmente cultivar una cultura de comportamiento de seguridad de la información. Por otra parte, las medidas organizativas sólidas, por ejemplo, políticas y procedimientos, deben estar en su lugar para poner todo en perspectiva. De estas dimensiones, el factor humano es probablemente el más importante ya que este es el área que el phishing expone más (Frauenstein & von Solms, 2009, p.6).

2.2.6. Social Cognitive Theory (SCT)

La Teoría Social Cognitiva, (Bandura A, 2009; citado en Ifinedo, 2014, p.70), es una premisa relevante para explicar el comportamiento humano. SCT permite que se estudie la interacción simultánea y dinámica entre factores sociales y personales. SCT postula que los individuos están activamente comprometidos en su propio desarrollo y obtener los resultados deseados cuando creen que sus acciones están bajo su propio control, (Bandura A, 2009; citado en Ifinedo, 2014, p.70). En consecuencia, (Workman et al., 2008, citado en Ifinedo, 2014, p.70) descompone el SCT en dos elementos principales:

- Locus of control (Workman et al., 2008, citado en Ifinedo, 2014, p.70), el lugar de control, se refiere al grado en que un individuo cree que él o ella tiene la capacidad de controlar los eventos que directa o indirectamente los afectan. Rotter, sugirió que las personas que creen que controlan su propio destino aceptarán la responsabilidad de sus acciones. Esencialmente, las personas que sienten que los resultados están fuera de su control pueden desplazar la responsabilidad de sus acciones hacia los demás (1966, citado en Ifinedo, 2014, p.70).
- Self-efficacy (Bandura A, 2009; citado en Ifinedo, 2014, p.70), la auto-eficacia, simplemente se refiere a la creencia de los individuos en sus propias competencias y capacidades.

2.2.7. Cognitive Evaluation Theory (CET)

La Teoría de la Evaluación Cognitiva fue diseñada para predecir los efectos perjudiciales de las recompensas sobre la motivación intrínseca, especialmente cuando las recompensas eran tangibles (por ejemplo, premios o premios). Según el CET, las recompensas actúan negativamente cuando se las interpreta como una herramienta para controlar el comportamiento (porque los receptores se sienten controlados y sus sentimientos de autodeterminación y autonomía disminuirán). La CET también predice los efectos positivos de las recompensas, especialmente las recompensas verbales, en la motivación intrínseca (Siponen M. Mahmood A. & Pahnila S., 2014, p.219).

3. Metodología

La revisión sistemática desarrollada en el presente documento ha tomado como referencia la estructura propuesta de Barbara Kitchenham (Kitchenham , 2004) y como complemento o aclaración de la parte conceptual se utilizó el Manual Cochrane de revisiones sistemáticas de intervenciones (Centro Cochrane Iberoamericano, 2011). El protocolo de revisión sistemática empleada para la presente investigación es señalado gráficamente en la Figura 1, donde se indica la secuencia de ejecución y los procesos involucrados. Los resultados serán señalados en el desarrollo del presente documento.

La pregunta de investigación que se plantea es:

> *RQ1= ¿Cuáles son las teorías o conceptos que explican el cumplimiento de las políticas de seguridad de la información que implementan las organizaciones para proteger su información?*

La pregunta de investigación planteada fue desarrollada aplicando el método PICO (Participantes, Intervenciones, Comparaciones y Outcome (Desenlaces)) descrito por Centro Cochrane Iberoamericano (2011, p.106).

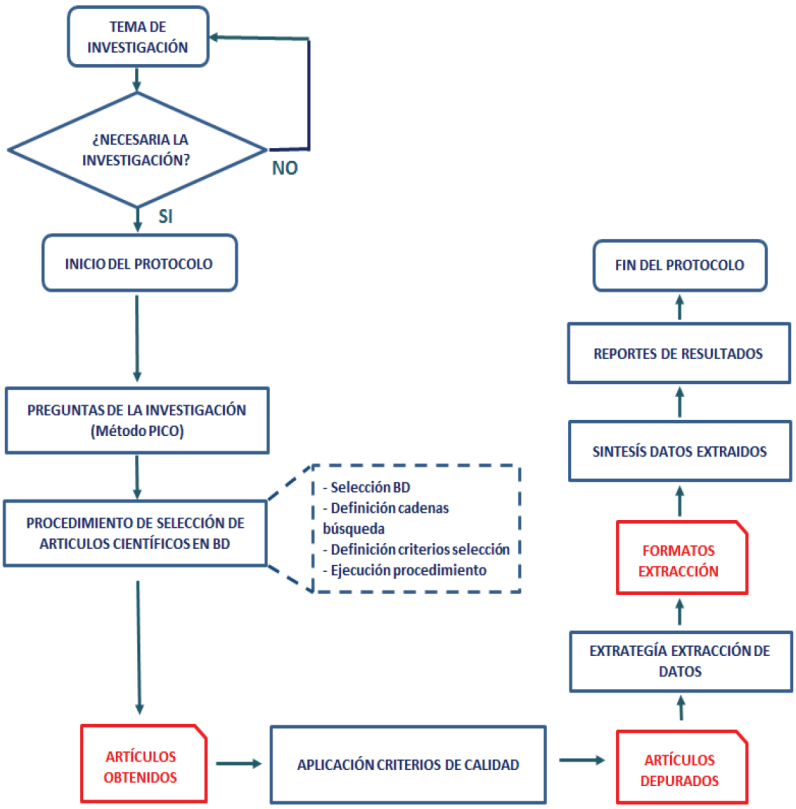

Figura 1 – Diagrama del protocolo de Revisión Sistemática

3.1. Proceso de bùsqueda

Las revisiones sistemáticas requieren de una búsqueda amplia, objetiva y reproducible de una gama de fuentes, para identificar tantos estudios relacionados como sea posible (dentro del límite de los recursos) (Centro Cochrane Iberoamericano, 2011, p.121). Sin embargo, es necesario hacer un balance entre esforzarse por la extensión y mantener la relevancia cuando se desarrolla una estrategia de búsqueda, pues aumentar la extensión (o sensibilidad) de una búsqueda se reducirá su precisión y se recuperarán más artículos que no son relevantes (Centro Cochrane Iberoamericano, p.147). Bajo estos considerandos se tomaron cuatro bases de datos, como fuentes potenciales de información según se describe en la Tabla 1. Para cada motor de búsqueda utilizado en las bases de datos seleccionadas, dada su particularidad forma de operación, se acondicionaron las cadenas de búsquedas, con el criterio de mantener inalterable las palabras claves definidas y que originan la cadena de búqueda. En todas las bases de datos se utilizó la opción de búsqueda avanzada.

Los criterios de inclusión son: - Publicaciones del año 2000 al 2017 , - Tipo documentos: journals, Magazines, Conference Publications o publicaciones academicas (arbitradas), Sources: Business, Management and Accounting,Computer Science, Engineering y estén publicados en Ingles. Los criterios de exclusion son: Documentos sin resultados experimentales y Documentos de literatura secundaria.

Base de datos	Palabras Claves	Cadena de búsqueda aplicado
IEEE Xplore: http://ieeexplore.ieee.org/Xplore/home.jsp	Kw01 = informat* Kw02 = securit* Kw03 = cultur* Kw04 = directive Kw05 = polit* Kw06 = factor Kw07 = accept Kw08 = reject* Kw09 = barrier Kw10 = people Kw11 = human	Document title: ((("Document Title":(informat* securit* cultur*)) OR "Document Title":"information security policies") OR "Document Title":"security culture") OR Abstract: (factor accept reject* barrier people human)
ScienceDirect: http://www.sciencedirect.com/		TITLE ((informat* AND securit*) OR (securit* AND cultur*) OR (informat* AND securit* AND cultur*)) AND ABSTRACT (factor OR accept OR reject* OR barrier OR people OR human)
Springer Link https://link.springer.com/		with the exact phrase: informat* securit* cultur* with at least one of the words: directive polit* factor accept reject* barrier people human
EBSCO: https://www.ebscohost.com/		Titulo: ((informat* AND securit*) OR (securit* AND cultur*) OR (informat* AND securit* AND cultur*)) AND Resumen: (factor OR accept OR reject* OR barrier OR people OR human)

Tabla 1 – Parámetros para el proceso de búsqueda

Respecto a las cadenas de búsqueda, estas fueron generadas mediante la combinación de palabras claves y la combinación de conectores lógicos "AND" y "OR", las palabras claves fueron obtenidas con base a la pregunta de investigación definida para el presente estudio, se consideraron los sinónimos. Todas las palabras claves y sus derivadas fueron

consideradas en el idioma inglés, dado que en dicho idioma existen la mayor cantidad de investigaciones publicadas. Los criterios de selección, cadenas de búsqueda adaptadas según particularidad de cada base de datos, empleados en la presente investigación están indicados también en la Tabla 1. Mediante la exploración en Google, dos (2) artículos fueron posteriormente adicionados (S1 y S2), a los cuales también les fueron aplicados los criterios de calidad establecidos. Estos dos artículos son también mostrados en la Tabla 2.

3.1.1. Procedimiento de selección realizado

El procedimiento que se ha seguido consta de los siguientes pasos:

Paso 1: Con base a los parámetros definidos en Tabla 1, se encontraron artículos que fueron guardados en un repositorio, programa Zotero.

Paso 2: Depuración de los artículos duplicados, encontrados en el Paso 1, a través del programa Zotero.

Paso 3: Depuración de artículos resultantes del paso anterior, cuyo título, palabras claves o resumen, no tengan una relación directa con nuestra pregunta de investigación.

Paso 4: Depuración de artículos resultantes del paso anterior, cuyo contenido no guarden relación directa con nuestra pregunta de investigación.

Paso 5: En la Tabla 2 se registraron los resultados obtenidos.

Base de datos	Fecha de extracciòn	Paso 1	Paso 2	Paso 3	Paso 4
IEEE Xplore	2017-05-05	70	70	23	2
ScienceDirect	2017-05-05	136	136	10	13
Springer Link	2017-05-05	67	67	7	1
EBSCO	2017-05-05	149	149	10	3
Google	2017-05-05				2
		Total de artículos seleccionados (*)			21

Tabla 2 – Documentos seleccionados Revisión Sistemàtica

3.1.2. Proceso de calidad de los estudios

La evaluación de la calidad de los estudios, se realizó mediante la aplicación de los criterios de calidad “Quality assessment” empleado por Kitchenham B., Brereton O., Budgen D., Turner M., Bailey J. & Linkman S (2009, p.9), según:

EQ1= ¿Se describen apropiadamente los criterios de inclusión y exclusión de la Investigación?

Evaluación: (Y= si, N=no, P = parcialmente)

EQ2= ¿Es probable que la investigación bibliográfica cubra todos los estudios pertinentes?

Evaluación: (Los autores han buscado artículos: Y= >=4 + adicional estrategias, N=3 o 4 sin extra, P = 2 o conjunto restringido de revistas)

EQ3= ¿Los evaluadores evaluaron la calidad/validez de los estudios incluidos?

Evaluación: (Y= Los autores definieron explícitamente los criterios calidad, N=no es explicita, P = la pregunta de investigación involucra cuestiones de calidad)

EQ4= ¿Fueron adecuadamente descritos los datos/estudios básicos?

Evaluación: (Y= información sobre cada estudio, N=no especifica resultados de estudios primarios individuales, P =información resumida de estudios primarios)

Los resultados de esta evaluación son mostrados en la Tabla 3 que es una adaptación de la Table 3 de Kitchenham B. et al (2009) quien consideró los siguientes puntajes: Y=1, P=0,5, N=0. En el Anexo 1 se muestra a detalle la lista de los 21 artículos primarios.

Doc	QA1	QA2	QA3	QA4	Puntaje
S1	Y	P	Y	P	3
S2	Y	Y	P	Y	3.5
S3	Y	Y	P	Y	3.5
S4	Y	Y	P	Y	3.5
S5	Y	Y	Y	Y	4
s6	Y	P	Y	Y	3.5
S7	Y	Y	Y	Y	4
S8	Y	Y	Y	Y	4
S9	Y	Y	Y	Y	4
S10	Y	P	Y	Y	3.5
S11	Y	Y	Y	Y	4
S12	Y	Y	Y	P	3.5
S13	Y	Y	Y	Y	4
S14	Y	Y	Y	Y	4
S15	Y	Y	Y	Y	4
S16	Y	Y	Y	Y	4
S17	Y	Y	Y	P	3.5
S18	Y	Y	Y	Y	4
S19	Y	Y	Y	Y	4
S20	Y	Y	Y	Y	4
S21	Y	Y	Y	Y	4

Tabla 3 – Resultados de aplicación de los criterios de calidad

3.1.3. Proceso de extracción de datos

Los artículos primarios fueron utilizados para el proceso de extracción de datos, obteniéndose información relevante, tales como: título, autor(es), año de publicación, país donde se realizó el estudio, muestra, tipo de investigación, teoría empleada. El registro de los datos extraídos fue realizado a través de la aplicación Microsoft Excel, lo cual permitió su uso posterior para la comparación de los artículos y análisis correspondiente, con lo cual se dio respuesta a la pregunta de investigación del presente documento Como información complementaria también se almacenaron los artículos completos en formato PDF.

4. Resultados

De los 21 artículos bajo estudio, desde el año 2014, se ha tenido un promedio de cuatro artículos publicados por año, salvo el 2016, pero que sin embargo, al cierre del año 2017 se podría tener mayor cantidad de artículos publicados, debido a que estamos a mitad de año, y es probable que el número de publicaciones se incremente.

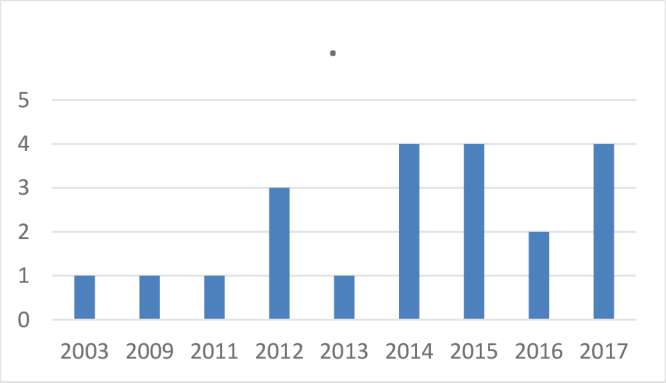

Figura 2 – Artículos primarios publicados por año

En lo que respecta a los lugares donde se llevó a cabo la investigación llama la atención que no se hayan encontrado estudios realizados para organizaciones de América del Sur o Centro.

Teorias empleadas en los artículos primarios

De los 21 artículos primarios bajo estudio, se han identificado 46 teorías o conceptos que son mostradas en la Tabla 4. Como se puede apreciar en la Tabla 4, la mayoría de las teorías más comunes se centran en la comprensión del comportamiento humano a través de teorías psicológicas o sociales que van más allá de la mera perspectiva tecnológica, debido a que el comportamiento humano es crucial en muchos fallos de seguridad y es considerado como el eslabón más débil de la cadena de seguridad (Ahmed M., et. al, 2012, p.82). Por lo que los atacantes, conocedores de esta situación, evaden los perímetros de seguridad de defensa casa vez mejor en estos días y dirigen sus ataques contra algo que ya esta en su red interna: los empleados (Arbor Networks, 2017, p. 10).

	Teoría Empleada	Ocurrencias	Artículos				Año	
1	Accountability theory	1	S13				2017	
2	Anticipated regret	1	S19				2015	
3	Cognitive evaluation theory (CET)	1	S6				2014	
4	Critical incidents technique	1	S2				2009	
5	Cultural factors	1	S10				2011	
6	Factor trust	1	S14				2015	
7	Framework cross-cultural dimensions	1	S5				2014	
8	Habit theory	1	S15				2012	
9	Human aspects of information security questionnaire (HAIS-Q)	1	S9				2014	
10	Information protection culture	1	S7				2015	
11	Information security policy	1	S21				2017	
12	Involvement theory	1	S11				2016	
13	Network effects	1	S13				2017	
14	Organizational climate (OC)	1	S20				2016	
15	Practice theory	1	S17				2017	
16	Privacy principies	1	S7				2015	
17	Psychological contract	1	S12				2017	
18	RegulatoIy focus theory	1	S1				2003	
19	Repertory grids technique	1	S2				2009	
20	Social cognitive theory (SCT)	1	S4				2014	
21	Social engineering	1	S14				2015	
22	Social pressure	1	S18				2013	
23	Sociology of translation	1	S17				2017	
24	Theory of knowledge sharing	1	S5				2014	
25	Theory of reasoned action (TRA) [Evolucionó a TPB]]	1	S6				2014	
26	Theory on dimensions of power (Hardy's, 1996)	1	S16				2012	
27	Twenty statements test (TST)	1	S2				2009	
28	General deterrence theory (GDT)	2	S18	S20			2013	2016
29	Information security culture	2	S7	S8			2015	2015
30	Management information systems	2	S17	S21			2017	2017
31	Rational choice theory (RCT)	2	S12	S20			2017	2016
32	Social bond theory (SBT)	3	S4	S11	S18		2014	2016
33	Protection motivation theory (PMT)	4	S3	S6	S15	S19	2012	2014
34	Theory of planned behavior (TPB)	4	S3	S4	S13	S19	2012	2014
	Total :	46		21				

Tabla 4 – Frecuencia de las teorías/técnicas empleadas

El detalle de la codificación de los artículos, tipo de publicación, tipo de investigación, entre otros, son mostrados en la Tabla 5. Dichas teorías o conceptos, han sido utilizados por los autores de los artículos primarios, para la generación de su modelo y la posterior validación de sus hipótesis a través de investigaciones en su mayoría cuantitativa mediante el uso de encuestas vía correo electrónico o página web.

De las teorías o conceptos, utilizadas por los autores, para explicar el cumplimiento de las políticas de seguridad de la información, se ha encontrado que "Theory of Planned Behavior (TPB)" junto con la "Protection Motivation Theory (PMT)" son las de mayor uso (utilizados en cuatro artículos), la "Social bond Theory (SBT)" fue utilizado en tres artículos, mientras que la "General deterrence theory (GDT)", "Information security culture", "Management information systems" y "Rational choice theory (RCT)", fueron utilizados en dos artículos. Sin embargo, considerando que la "Theory of reasoned action (TRA)" es un antecesor de "Theory of Planned Behavior (TPB)", se tendría que esta última es la más utilizada.

5. Discusión de Resultados

El análisis de los 21 estudios primarios, ha permitido identificar 46 teorías o conceptos que han utilizado los autores de los artículos primarios para explicar y proponer modelos que expliquen el cumplimiento de las políticas de seguridad de la información en las organizaciones. De todas estas teorías, la "Theory of Planned Behavior (TPB)" junto "Protection Motivation Theory (PMT)" son las que han tenido mayor uso, mientras que la "Social bond Theory (SBT)", "General deterrence theory (GDT)", "Information security culture", "Management information systems" y "Rational choice theory (RCT) fueron utilizados en al menos dos artículos. Sin embargo, algo en común que tienen estas teorías es que están enfocadas a estudiar, comprender y predecir el comportamiento del ser humano, debido a que el comportamiento humano es crucial en muchos fallos de seguridad y es considerado como el eslabón más débil de la cadena de seguridad (Ahmed M., et. al, 2012, p.82). El agente humano, de manera intencional o no intencional, se involucra en comportamientos mal prescritos que pueden poner en peligro los recursos de la organización IS (Harris & Furnell, 2012; Hu et al., 2011; Ifinedo, 2014; Pahnila et al., 2007; Siponen & Vance, 2010; Stanton et al., 2005; citado en Ifnedo, P., 2016, p.31).

Esta situación pone de manifiesto el enfoque interdisciplinario que indirectamente están evidenciando los autores de los artículos bajo análisis, haciéndose necesario una visión global, no solo desde la perspectiva tecnológica, sino también desde la perspectiva de otras disciplinas, como la social o psicológica, o tal vez otras más, que en su conjunto conlleve a un enfoque real del problema.

La transición hacia una verdadera visión interdisciplinar ocurre según Agazzi (2002) cuando, dentro de cada disciplina, se despierta una reflexión filosófica que lleva a percibir una exigencia de unidad, es decir a no considerar su propio discurso como cerrado y autónomo, sino como una voz específica dentro de un concierto. Hemos dicho que se trata de una reflexión filosófica, y esto se justifica considerando que es filosófico (y más precisamente epistemológico) el trabajo mediante el cual se aseguran las "condiciones preliminares" discutidas arriba, así como la toma de conciencia de la parcialidad de las diferentes ópticas disciplinares respecto al "punto de vista de la totalidad". Es también

Item	Año	Tipo publicación	Tipo investigación	Instrumento	Ubicación	Teoria / concepto empleada
S1	2003	Conference	Exploratorio ISP	ISP disponible en internet	USA - New York	RegulatoIy focus theory
S2	2009	Conference	Cualitativa	Entrevistas y focus group	No indica	Twenty statements test (TST)
						Repertory grids technique
						Critical incidents technique
S3	2012	Article	Cuantitativa	Cuestionarios por email	Canada	Protection motivation theory (PMT)
						Theory of planned behavior (TPB)
S4	2014	Article	Cuantitativa	Cuestionarios por email	Canada	Theory of planned behavior (TPB)
						Social cognitive theory (SCT)
						Social bond theory (SBT)
S5	2014	Article	Mixta	Entrevistas y encuestas	USA y Suecia	Theory of knowledge sharing
						Framework cross-cultural dimensions
S6	2014	Article	Cuantitativa	Cuestionario web	Finlandia	Protection motivation theory (PMT)
						Theory of reasoned action (TRA) [Evolucionó a TPB]
						Cognitive evaluation theory (CET)
S7	2015	Article	Cuantitativa	Cuestionarios por email	Países - 12	Information protection culture
						Information security culture
						Privacy principies
S8	2015	Article	Cuantitativa	Cuestionarios por email	Países - Varios	Information security culture
S9	2014	Article	Cuantitativa	Cuestionarios por email	Australia	Human aspects of information security questionnaire (HAIS-Q)
S10	2011	Conference	Cuantitativa	Cuestionarios web	Sudafrica	Cultural factors
S11	2016	Article	Cuantitativa	Cuestionario por email	Malasia	Social bond theory (SBT)
						Involvement theory

Item	Año	Tipo publicación	Tipo investigación	Instrumento	Ubicación	Teoria / concepto empleada
S12	2017	Article	Cuantitativa	Cuestionarios web	No indica	Rational choice theory (RCT)
						Psychological contract
S13	2017	Article	Cuantitativa	Encuesta web	Vietnam - Sudeste de Asia	Theory of planned behavior (TPB)
						Accountability theory, Network effects
S14	2015	Conference	Mixta	Mixto: Entrevistas y encuestas web	Sudafrica	Social engineering , Factor trust
S15	2012	Article	Cuantitativa	Cuestionarios web	Finlandia	Protection motivation theory (PMT)
						Habit theory
S16	2012	Article	Cualitativa	Caso de estudio	Suecia	Theory on dimensions of power (Hardy's, 1996)
S17	2017	Article	Cualitativa	Ethnographic approach	No indica	Management information systems
						Practice theory
						Sociology of translation
S18	2013	Article	Cuantitativa	Cuestionarios web y fisicos	China	General deterrence theory (GDT)
						Social bond theory (SBT)
						Social pressure
S19	2015	Article	Cuantitativa	cuestionarios via email	Suecia	Theory of planned behavior (TPB)
						Protection motivation theory (PMT)
						Anticipated regret
S20	2016	Article	Cuantitativa	Cuestionarios por email	Canada	General deterrence theory (GDT)
						Rational choice theory (RCT)
						Organizational climate (OC)
S21	2017	Article	Cuantitativa	Cuestionario	Palestina - Franja de Gaza	Information security policy
						Management information systems

Tabla 5 – Teorías empleadas en los artículos primarios

de índole filosófica la capacidad hermenéutica que se necesita para "interpretar" dentro del propio lenguaje, sin traicionar su sentido, los discursos de las otras disciplinas. El uso sabio de esta actitud hermenéutica permite un intercambio continuo de un discurso a otro que elimina poco a poco las "equivocaciones" (p.249).

Respecto a las otras teorías o conceptos restantes, señaladas en la Fig. N° 02, se aprecia nuevamente que en su mayoría, están orientadas a explicar o predecir el comportamiento humano para el cumplimiento de las políticas de seguridad de la información; sin embargo, aunque varios estudios han examinado factores sociales como antecedentes o moderadores del cumplimiento del ISP (Bulgurcu et al., 2009, Herath y Rao, 2009, Myyry et al., 2009), estos esfuerzos son insuficientes para construir una base teórica sustancial (Young J., et al, 2016, p4).

En lo que respecta a los resultados del presente trabajo, es importante indicar que el estudio ha sido limitado a conocer las teorías más relevantes que emplean los autores para proponer modelos que expliquen el cumplimiento de las políticas de seguridad de la información en las organizaciones. Un estudio posterior, podría realizarse integrando estas teorías para proponer un modelo que permita identificar los factores relevantes de dicha integración, bajo un enfoque social, psicológico, cultural, tecnológico, de gestión, entre otros.

6. Futuros trabajos:

En la Figura 3 se muestra un esquema de trabajo que integre varias disciplinas, en la que el factor "Personas" es la base del esquema, pero sin descuidar los otros aspectos tales como el de tecnología, gestión, infraestructura, entre otros, se propone como futuros trabajos. El esquema presentado se interpreta como:

- El aspecto humano, según el rol que desempeñe en la disciplina o actividad (usuario, tecnológico, ciudadano, empleado, etc.) tendrá una visión diferente en aspectos de seguridad y por tanto en el cumplimiento de las políticas de seguridad. Este es el enfoque de la "perspectiva interdisciplnaria" que se muestra en el esquema.
- El aspecto "infraestructura tecnológica", esta referida a los mecanismos de seguridad y control que se implementan a través de la tecnologia TI.
- El aspecto "políticas de seguridad" esta referida como el regulador en el comportamiento de las "personas" y en los requisitos que debe considerar la implementación de una "infraestructura tecnológica".
- La relación de estos tres aspectos, "políticas de seguridad", "infraestructura tecnológica" y "perspectiva interdisciplinaria", se consideraran necesarias para que exista un adecuado establecimiento de las políticas de seguridad, en la que considere todos estos aspectos.

La tarea para el investigador, sería la de encontrar los factores o mecanismos que conlleven a una unificación de estos aspectos, manteniendo una actualización contantes, debido a la creación de nuevas formas de ataques, surgimiento de nuevas tecnologías y por que no decirlo, por la rotación del personal.

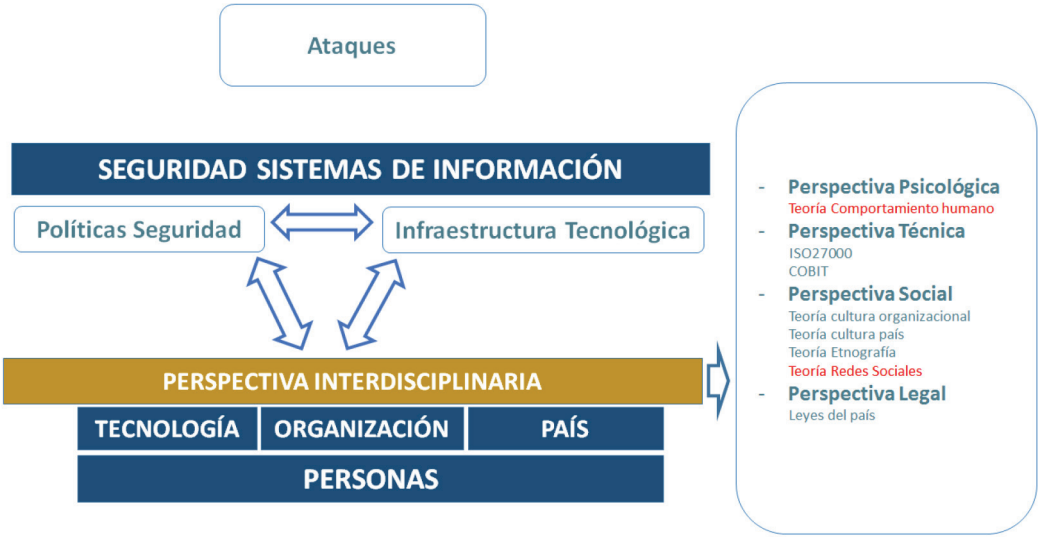

Figura 3 – Propuesta de estudios futuros

7. Conclusiones

Entender las teorías que permiten el cumplimiento de las políticas de seguridad de la información de la organización, desde una perspectiva interdisciplinaria, es clave para el resguardo de la información, lo cual podría evitar (Chang S.E., et al, 2015) que las organizaciones tiendan a implementar una gran cantidad de controles de seguridad para proteger sus activos de los empleados, mediante el seguimiento de cada una de sus acciones, lo cual conduce a sentimientos negativos de los empleados sobre la confianza y puede dañar / poner en peligro significativamente la relación de confianza entre las organizaciones y sus empleados (citado en Vuuren, et aI., 2015, p.126). Los resultados de la revisión sistemática, en donde las teorías están enfocadas al factor humano, guardan relación con el rol que desempeña el ser humano, pues según los diferentes roles que desempeña (como atacante o protector de la información, como usuario o como administrador de la información, como diseñador de nuevas políticas, normas, o procedimientos, como supervisor o supervisado de cumplimiento de las políticas de información, como diseñador de nuevos esquemas de protección, tecnología, como diseñador de nuevos ataques, etc.) tendrá un impacto en las organizaciones, que dependerá, valga la redundancia, del rol que desempeñe, como lo desempeñe, donde lo desempeñe y cuando lo desempeñe. Los profesionales en seguridad TI, deberían considerar que la seguridad de información no solo se garantiza mediante el empleo de perímetros de seguridad sofisticados, sino que deberían enfocar y considerar en sus estrategias de protección el factor humano, pues dado el comportamiento no deseado que tengan (voluntario o involuntario) provocará la anulación de los perímetros de seguridad implementados, generando brechas de seguridad importantes, con las consiguientes consecuencias y pérdidas económicas, como los señalados en el presente documento. Se

puede concluir como trabajos futuros, que establecer políticas de seguridad y esperar su cumplimiento, sin considerar otros aspectos, Figura 3, sin una interrelación unificada, tendría como consecuencia incrementar las brechas de seguridad, dado que según la función que desempeñe el factor humano, tendría una percepción diferente de lo que es seguridad de la información, y por tanto creer que las políticas de seguridad son exageradas y no útiles, no cumpliéndolas, exponiendo la seguridad de la información.

Referencias

SANS Institute, InfoSec Reading Room (2014). *Risk, Loss and Security Spending in the Financial Sector: A SANS Survey*. Recuperado a partir de https://www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690

Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study, *Computers & Security*, 49, (162–176). http://dx.doi.org/10.1016/j.cose.2014.12.006

Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument, *Computer Law & Security Review*, 31(2), 243–256. http://dx.doi.org/10.1016/j.clsr.2015.01.005

Agazzi, E. (2002). El desafio de la Interdisciplinariedad: Dificultades y Logros. *Revista Empresa y Humanismo de la Universidad de Navarra*, V(2/02), 241–252.

Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. (2012). Human errors in information security. *International Journal*, 1(3), 82–87. recuperado a partir de https://pdfs.semanticscholar.org/d5cb/1d63ee593b2815fe5c37c3f4a602ef9f269a.pdf

Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors (pp. 731-735). IEEE. https://doi.org/10.1109/ITNG.2015.124

Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2017). Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management* 15(1), 1–26.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3), 190–198. ISSN 0378-7206, http://dx.doi.org/10.1016/j.im.2012.04.002

Arbor Networks. (2017). Doppelgangers de la industria tecnologica: Innovación de campañas en el mundo del delito cibernético (No. 451 Research) (p. 14). Recuperado a partir de http://es.arbornetworks.com/reporte-451/

AT&T Cybersecurity Insights (2017). Protect your data through innovation, The CEO's Guide to Data Security, Volume 5, (pp. 1-20), recuperado a partir de https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf.

Castro, W., & Acuña, S. (2011). *Comparativa de Selección de Estudios Primarios en una Revisión Sistemática*. Madrid, España: Departamento de Ingeniería Informática, Universidad Autónoma de Madrid.

Centro Cochrane Iberoamericano. (2012). *Manual Cochrane de Revisiones Sistemáticas de Intervenciones, versión 5.1.0*. Barcelona: Centro Cochrane Iberoamericano. Disponible en http://www.cochrane.es/?q=es/node/269

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67(February), 196–206. https://doi.org/10.1016/j.chb.2016.10.025

Dyba, T., & Dingsoyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and software technology*, 50(9-10) 833–859.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33, 3–11. http://dx.doi.org/10.1016/j.cose.2012.07.001

Frauenstein, E., & von Solms, R. (2009). Phishing: how an organisation can protect itself. South Africa: Nelson Mandela Metropolitan University.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition, *Information & Management* 51(2014), 69–79.

Imperva. (2016). *Insiders: The Threat is Already Within, Hacker Intelligence initiative*. (pp. 1-13), recuperado a partir de https://www.imperva.com/docs/Imperva_HII_Insider_Threat.pdf

Han, J.Y., Kim, Y. J., & Kim, H. (2016). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 12, 1–35. http://dx.doi.org/doi: 10.1016/j.cose.2016.12.016

Kaspersky Lab (2017). *Damage control: the cost of security breaches it security risks special report series, IT security risks special report series*. (pp. 1-7). recuperado a partir de https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Kindervag, J., Shey, H., & Mak, K. (2016). The Future Of Data Security And Privacy: Growth And Competitive Differentiation. In *Vision: The Data Security And Privacy Playbook* (pp. 1-15). Forrester Research. recuperado a partir de https://www.forrester.com/report/The+Future+Of+Data+Security+And+Privacy+Growth+And+Competitive+Differentiation/-/E-RES61244

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews, Keele University Technical Report 2004. Keele, UK: Keele University.

Kitchenham, B., Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S., (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, 51(2009), 7–15.

Kruger, H., Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness, 2011 Information Security for South Africa, Johannesburg. (pp. 1-7). doi: 10.1109/ISSA.2011.6027505, recuperado a partir de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6027505&isnumber=6027504

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447–459. http://dx.doi.org/10.1016/j.cose.2013.09.009

Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture?. In *43rd Annual 2009 International Carnahan Conference on Security Technology*, Zurich , (pp. 361-366). doi: 10.1109/CCST.2009.5335511

Marcinkowski, S. & Stanton, J. (2003). Motivational aspects of information security policies. In *Systems, Man and Cybernetics. IEEE International Conference on, 2003, (vol.3 pp. 2527-2532)*. doi: 10.1109/ICSMC.2003.1244263

Marcinkowski, S. J., & Stanton, J. M. (2003). Motivational aspects of information security policies. *En Systems, Man and Cybernetics, 2003. IEEE International Conference on (Vol. 3, pp. 2527–2532)*. IEEE. Recuperado a partir de http://ieeexplore.ieee.org/abstract/document/1244263/

Mark Hardy, G., (2014). Risk, Loss and Security Spending in the Financial Sector

Niemimaa, E., & Niemimaa, M.(2017). Information systems security policy implementation in practice: from best practices to situated practices, *European Journal of Information Systems*, 26(1), 1–20. doi:10.1057/s41303-016-0025-y

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security,* 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Ponemon Institute, (2016). *2016 Cost of Data Breach Study:Global Analysis, Ponemon Institute© Research Report. (pp. 1-32)*. recuperado a partir de https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Ifinedo, P. (2016). Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?, *Information Systems Management*, 33(1), 30–41. DOI: 10.1080/10580530.2015.1117868

Siponen M. Mahmood A. & Pahnila S., (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management,* 51, 217–224.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security,* 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information & Computer Security, 23(2) 200 – 217. http://dx.doi.org/10.1108/ICS-04-2014-0025

University of Twente. (2017). *Protection Motivation Theory, Health Communication*. recuperado a partir de https://www.utwente.nl/en/bms/communication-theories/sorted-by-cluster/Health%20Communication/Protection_Motivation_Theory/

Van Niekerk, J.F., & Von, R. (2010). Information security culture: A management perspective, *Computer & Security,* 29(2010), 476–486.

Vuuren, I., Kritzinger, E., & Mueller, C., (2015). Identifying Gaps in IT Retail Information Security Policy Implementation Processes, Towards developing a secure IT enterprise built on trust. (pp. 126-133). IEEE.

Flores, W. R., 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. http://dx.doi.org/10.1016/j.cose.2014.03.004

Walls, A. (2014). *Best Practices for Managing 'Insider' Security Threats, 2014 Update*, (pp. 1-8). Gartner Reprint, recuperado a partir de https://www.gartner.com/doc/reprints?id=1-2YJTNEF&ct=160211&st=sb

Anexo 1 – Artículos primarios seleccionados

Item	Titulo	Autor(Es)	Año	Bd	Tipo
S1	Motivational Aspects of Information Security Policies	Slawomir J. Marcinkowski, Jeffrey M. Stanton	2003	Google (*)	Conference
S2	What is Security Culture? Does it differ in content from general Organisational Culture?	Jo Malcolmson	2009	Google (*)	Conference
S3	Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory	Princely Ifinedo	2012	Science Direct	Article
S4	Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition	Princely Ifinedo	2014	Science Direct	Article
S5	Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture	Waldo Rocha Flores, Egil Antonsen, Mathias Ekstedt	2014	Science Direct	Article
S6	Employees' adherence to information security policies: An exploratory field study	Mikko Siponena, M. Adam Mahmoodb, Seppo Pahnila	2014	Science Direct	Article
S7	Information security culture and information protection culture: A validated assessment instrument	Adéle Da Veigaa, Nico Martins	2015	Science Direct	Article
S8	Improving the information security culture through monitoring and implementation actions illustrated through a case study	Adéle da Veigaa, Nico Martinsb	2015	Science Direct	Article
S9	Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)	Kathryn Parsonsa, Agata McCormaca, Marcus Butaviciusa, Malcolm Pattinsonb, Cate Jerram	2014	Science Direct	Article
S10	An assessment of the role of cultural factors in information security awareness	H. A. Kruger; S. Flowerday; L. Drevin; T. Steyn	2011	IEEE Xplorer	Conference
S11	Information security policy compliance model in organizations	Nader Sohrabi Safa, Rossouw Von Solms, Steven Furnell	2016	Science Direct	Article

Item	Titulo	Autor(Es)	Año	Bd	Tipo
S12	An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective	JinYoung Han, Yoo Jung Kim, Hyungjin Kim	2017	Science Direct	Article
S13	Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace	Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno	2017	Science Direct	Article
S14	Identifying Gaps in IT Retail Information Security Policy Implementation Processes	Ileen E. van Vuuren; Elmarie Kritzinger; Conrad Mueller	2015	IEEE Xplorer	Conference
S15	Motivating IS security compliance: Insights from Habit and Protection Motivation Theory	Vance, A., Siponen, M., Pahnila, S	2012	Science Direct	Article
S16	Organizational power and information security rule compliance	Ella Kolkowska, Gurpreet Dhillon	2012	Science Direct	Article
S17	Information systems security policy implementation in practice: from best practices to situated practices	Elina Niemimaa , Marko Niemimaa	2017	Springer	Article
S18	Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory	Lijiao Chenga, Ying Lia, b, Wenli Lia, Eric Holmc, Qingguo Zhaic,	2013	Science Direct	Article
S19	The sufficiency of the theory of planned behavior for explaining information security policy compliance	Sommestad, Teodor1; Karlzén, Henrik1; Hallberg, Jonas1	2015	EBSCO	Article
S20	Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?	Ifinedo, Princely	2016	EBSCO	Article
S21	Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip	Abdelwahed, Ann S.; Mahmoud, Ahmed Y.; Bdair, Ramiz A	2017	EBSCO	Article