MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

FUTURAS INVESTIGACIONES PARA EL COMPORTAMIENTO DE SEGURIDAD DE LA INFORMACIÓN: UNA REVISIÓN SISTEMÁTICA

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

Magíster en Auditoría de Tecnologías de la Información

Por las estudiantes:
Alexandra Jacqueline ARCINIEGAS CORAL
Angélica del Rocío DEL PEZO SAONA

Bajo la dirección de:
Francisco Joseph BOLAÑOS BURGOS

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

Marzo del 2018

Futuras Investigaciones para el Comportamiento de Seguridad de la Información: Una revisión sistemática.

Futures Researches for Information Security Behavior: A Systematic Review.

Alexandra Jacqueline ARCINIEGAS CORAL[1]
Angélica del Rocío DEL PEZO SAONA[2]
Francisco Joseph BOLAÑOS BURGOS[3]

Resumen

El aumento en el uso de las tecnologías de la información conlleva también a las crecientes amenazas a la seguridad de la información, que en ocasiones son ignoradas o sus riesgos subestimados por parte de los usuarios internos de las organizaciones; de modo que, una de las principales preocupaciones de los administradores de la seguridad de la información es la amenaza interna. En el presente trabajo, se realiza una revisión sistemática de los estudios existentes en la literatura sobre el comportamiento de cumplimiento de Políticas de Seguridad de la Información [PSI] de los empleados en las organizaciones desde el año 2000 hasta el 2016; y, a través de cuatro taxonomías seleccionadas se examina el estado del arte del comportamiento de seguridad de la información, para identificar los enfoques que han recibido mayor atención por parte de los investigadores, tipos de comportamientos, tipos de usuarios internos, y las determinantes que influyen en el comportamiento conductual de los empleados. Se presenta información de las tendencias actuales en este campo de investigación; y, se proponen trabajos futuros que podrían ser considerados por la comunidad de investigación de la seguridad de la información.

Palabras clave: Cumplimiento de Políticas de Seguridad de la Información, Comportamiento, Tipos de usuarios, Estado del Arte, Revisión Sistemática.

Abstract

The increase in the use of information technologies also leads to the growing threats to information security, which are sometimes ignored or their risks underestimated by the internal users of the organizations; So, one of the main concerns of information security administrators is the internal threat. In the present work, a systematic review of the existing studies in the literature on the compliance behavior of Information Security Policies [ISP] of employees in organizations from 2000 to 2016 is carried out; and, through four selected taxonomies, the state of the art of information security behavior is examined, to identify the approaches that have received the most attention from researchers, types of behavior, types of internal users, and the determinants they influence the behavioral behavior of employees. Information on current trends in this field of research is presented; and, future works are proposed that could be considered by the information security research community.

Key words Information Security Policies Compliance, Behavior, User Types, State-of-the-Art, Systematic Review.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail aarciniegas@uees.edu.ec.

[2] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail adelpezo@uees.edu.ec.

[3] Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

Introducción

En la actualidad las organizaciones han alcanzado una fuerte dependencia hacia los Sistemas de Información [SI] (Cavusoglu, Mishra, y Raghunathan, 2004; Ifinedo, 2009, 2011; Lebek, Uffen, Neumann, Hohler, y Breitner, 2014; Stanton, Stam, Mastrangelo, y Jolton, 2005). De manera que el aumento en el uso de las Tecnologías de la Información [TI] conlleva un lado negativo, como son las crecientes amenazas a la seguridad de la información, que en ocasiones son ignoradas o sus riesgos subestimados por parte de los usuarios de TI (Kankanhalli, Teo, Tan, & Wei, 2003; Chen, Shaw, & Yang, 2006; Guo, Yuan, Archer, & Connelly, 2011; Hwang, Kim, Kim, & Kim, 2017).

De acuerdo con Loch, Carr, y Warkentin (1992) las amenazas a la seguridad de los SI pueden ser clasificadas a partir de cuatro dimensiones; según su fuente (internas o externas a la organización); según los perpetradores (humanos o no humanos); según la intención (intencionales o no intencionales - accidentales), y según las consecuencias (divulgación, modificación, destrucción o denegación de servicio). Del mismo modo, la taxonomía propuesta por Im y Baskerville (2005) presenta una clasificación de las amenazas a la seguridad de los SI como accidentales o deliberadas, en el que las accidentales son aquellas causadas por los seres humanos no intencionalmente y pueden desglosarse en errores humanos y catástrofes. Por otra parte, las amenazas deliberadas son las causadas por comportamientos intencionales de quienes interactúan con los SI, cuyas dimensiones son, el modo en el que se presenta la amenaza que puede ser agresión física, falsificación, código malicioso, agrietamiento y el motivo que puede ser fraude, espionaje y vandalismo.

Recientes investigaciones sugieren que una de las principales preocupaciones de los administradores de seguridad de los SI en las organizaciones, es la amenaza interna (Bonar y Rosenberg, 2011; Chen, Ramamurthy, y Wen, 2012; Willison y Warkentin, 2013). Empleados con acceso a los recursos de información, pueden provocar daños a la confidencialidad, integridad o disponibilidad de los SI por medio de acciones deliberadas como el descontento o espionaje; del mismo modo, pueden inducir riesgos por causa del incumplimiento pasivo de las Políticas de Seguridad de la Información [PSI], generado por la pereza, el descuido, insuficiente capacitación o la falta de motivación para proteger la integridad y la privacidad de la información confidencial de la organización (Warkentin y Willison, 2009).

Según la encuesta sobre las amenazas internas del Instituto de Auditoría Administración de Sistemas, Redes y Seguridad (Sans Intitute, 2017), señala que el 40% de los encuestados califica a los empleados internos maliciosos como el vector de amenazas más dañino al que se enfrentan, y el 36% cataloga a los empleados internos negligentes como la amenaza más perjudicial. De la misma manera, la Encuesta Global del Estado de Seguridad de la Información de la firma consultora PricewaterhouseCoopers (PwC, 2017), expresa que los empleados actuales de las organizaciones siguen siendo una de las principales fuentes de incidentes de seguridad.

Los resultados de la Encuesta Global de Seguridad de la Información de Ernst y Young (2017) indica que los empleados descuidados o desprevenidos son una de las causas de la exposición a riegos de seguridad; del mismo modo, el Estudio sobre Tendencias en Gestión de Ciber-Riesgos y Seguridad de la Información en Latinoamérica de Deloitte (2016) destaca que entre las amenazas con mayor probabilidad de ocurrencia se encuentran el abuso de los privilegios de acceso a información por parte de usuarios internos, los errores y omisiones de los usuarios en el uso de los sistemas de información que derivan en incidentes de seguridad y el robo de información por atacantes internos.

En consecuencia, los incidentes de seguridad provocan daños en la confianza del cliente y en la reputación de la organización, lo que perjudica en ocasiones el desempeño económico de las empresas afectadas (Campbell, Gordon, Loeb, y Zhou, 2003; Posey, Roberts, Lowry, y Hightower, 2014); por lo tanto, para mitigar las amenazas a la seguridad de la información, las organizaciones implementan medidas técnicas y procedimientos de seguridad (Aurigemma y Panko, 2012; Kraemer, Carayon, y Clem, 2009), siendo una de ellas la implementación de PSI, a través de las cuales se establecen, las consecuencias de su no cumplimiento, el uso aceptable de los recursos informáticos, y responsabilidades; así como los mecanismos de capacitación a sus empleados (Bulgurcu,

Cavusoglu, y Benbasat, 2010; Pahnila, Siponen, y Mahmood, 2007a; Pahnila, Siponen, y Mahmood, 2007b; Sommestad y Hallberg, 2013). Sin embargo, la efectividad de las implementaciones de PSI dentro de las organizaciones está relacionada con el cumplimiento de éstas por parte del empleado (Balozian y Leidner, 2017; Pahnila et al., 2007b). En este sentido, las investigaciones sugieren que no basta con que los empleados conozcan las PSI (Karjalainen y Siponen, 2011), sino que además éstos deben cumplirlas, de tal manera que las organizaciones tienen que emplear un mayor esfuerzo en no sólo impulsar la toma de conciencia de las PSI (Siponen, 2000), sino también en aprender cómo pueden alentar a los empleados a cumplirlas (Siponen y Vance, 2014).

En la gestión de la seguridad de la información actual, se proporciona importancia a los problemas del comportamiento de seguridad, lo que ha generado una creciente investigación en cuanto a los determinantes que se vinculan con la conducta y el cumplimiento de las PSI por parte del empleado, con base en una variedad de teorías como las de criminología, sociología y psicología, entre otras (D'Arcy, Herath, y Shoss, 2014; Goo, Yim, y Kim, 2014; Vance, Siponen, y Pahnila, 2012). En relación con lo expuesto, varios investigadores coinciden en que existe carencia de una visión general de los determinantes que predicen el comportamiento apropiado de seguridad y permita obtener el claro conocimiento sobre qué estrategias o procedimientos deben aplicar las organizaciones para lograr la eficacia en el cumplimiento de las políticas de seguridad por parte de los empleados (Balozian y Leidner, 2017; Guo, 2013; Padayachee, 2012; Stanton et al., 2005; Topa y Karyda, 2015).

Con la finalidad brindar un aporte útil en esta área de investigación, se realiza una revisión sistemática de los estudios existentes en la literatura sobre el comportamiento de cumplimiento de PSI de los empleados en las organizaciones desde el año 2000 hasta el 2016; y, a través de cuatro taxonomías seleccionadas (Stanton et al., 2005; Padayachee, 2012; Guo, 2013; Balozian y Leidner, 2017) se examina el estado del arte del comportamiento de seguridad de la información, para identificar los enfoques que han recibido mayor atención por parte de los investigadores, tipos de comportamientos, tipos de usuarios internos, y las determinantes que influyen en el comportamiento conductual de los empleados en las organizaciones. El presente documento muestra información de las tendencias actuales en este campo de investigación; y, se proponen trabajos futuros que pueden ser considerados por los investigadores.

Marco Teórico

Abuso del Computador.

D'Arcy, Hovav, y Galletta (2009); Harrington (1996); Kankanhalli, Teo, Tan, y Wei (2003); Kling (1980); D. W. Straub, 1990; D. W. J. Straub y Nance (1990), refieren al abuso del computador como el comportamiento del usuario final que hace uso indebido no autorizado y deliberado de los activos de información (hardware, software, datos y servicios informáticos) de una organización; análogamente es conocido como crímenes relacionados con la computadora que probablemente provoque daño directo a la organización (Guo, 2013; Workman y Gathegi Jhon, 2006).

La investigación de Parker (1976), fue la primera en estudiar y acuñar formalmente el término de Abuso del Computador, pero ésta no expresa claramente el uso de teorías. Estudios posteriores han aplicado teorías criminológicas como la teoría de la disuasión (Grasmick y Bryjak, 1980; Straub, 1990), código de ética (Harrington, 1996; Johnston, Warkentin, & Siponen, 2015), programas de sensibilización (Lee, Lee, y Yoo, 2004), conciencia y capacitación (D'Arcy et al., 2009), para fortalecer sus investigaciones.

Violación de Políticas de Seguridad de Información.

El comportamiento de violación o no cumplimiento de PSI, se refiere a las acciones de los usuarios finales que no están de acuerdo con las PSI de la organización (D'Arcy et al., 2014; Hu, Dinev, Hart, y Cooke, 2012) lo cual les induce a violar (Guo, 2013), incumplir (Balozian y Leidner, 2017) o romper las reglas (Tyler y Blader, 2005), normas o políticas establecidas y contractualmente vinculantes para el usuario final (Siponen y Vance, 2010), sin mostrar diferencia explícita de la intencionalidad maliciosa o no maliciosa (Guo, Yuan, Archer, y Connelly, 2011).

Por el contrario Vroom y Von Solms (2004), argumentan que este comportamiento se debe a negligencia o desconocimiento de las PSI de los usuarios finales incluso en organizaciones que tienen claramente establecidas sus políticas y con roles activos de los encargados de la seguridad de la información (Puhakainen, 2006).

Como complemento, la violación de las PSI, también es considerada como un comportamiento negativo (Guo, 2013), socialmente indeseable, difícil de medir usando medios convencionales ya que la tendencia de los usuarios finales es ocultar información o no participar en encuestas socialmente deseables (Trevino, 1992; Vance, 2012).

La literatura evidencia investigaciones destinadas a explicar los determinantes (Aytes y Conolly, 2003; D'Arcy et al., 2014; Hu, Xu, Dinev, y Ling, 2011; Siponen, 2005; Siponen y Vance, 2010; Vance, 2012) que influyen en los usuarios finales a cometer comportamientos de violación fundamentados en teorías de psicología social y de criminología (Pahnila et al., 2007a).

Obediencia de Seguridad Información.

Thomson y Von Solms (2005) definen al término Obediencia de Seguridad de Información como el comportamiento del usuario final de facto que debe cumplir con lo que exige la alta gerencia en la PSI de la organización. Con una adecuada aplicación y gestión de las PSI, los usuarios finales cambiarán de un nivel de conciencia a un nivel de obediencia (Furnell y Thomson, 2009); considerando que las PSI deben ser percibidas como obligatorias para aumentar su cumplimiento (Boss, Kirsch, Angermeier, Shingler, y Boss, 2009).

Otra tendencia, denomina Obediencia de Seguridad de Información a la amalgama entre la Cultura Corporativa, la Seguridad de Información y el Gobierno Corporativo (Thomson, Solms y Louw, 2006).

Taxonomía de dos Factores del Comportamiento de Seguridad del Usuario Final.

Stanton et al. (2005) desarrollaron una taxonomía que resume aquellos comportamientos individuales que pueden afectar la seguridad de información en el lugar de trabajo. Esta investigación se realizó en tres etapas. La primera etapa entrevistó a 110 profesionales con conocimientos sobre comportamientos relacionados con la seguridad del usuario final obteniendo una lista sin clasificar de los mismos; en la segunda etapa, con base en los resultados obtenidos de la etapa anterior, 10 expertos en seguridad de información categorizaron los comportamientos formando su propio diseño, encontrando similitudes entre las categorías, obtuvieron la taxonomía de seis elementos, para finalmente en la tercera etapa, ser probada con 49 expertos en TI, obteniendo los niveles de experiencia requerida y el supuesto intento asociado con cada uno de los comportamientos.

Stanton y sus colegas mostraron que los comportamientos se ajustan bien a un modelo bidimensional: intención y experiencia. La intencionalidad de la acción de un usuario es calificada como maliciosa (comportamiento inclinado al riesgo), neutral (comportamiento ingenuo o accidental) o beneficiosa (comportamiento adverso al riesgo); mientras que, la experiencia es el grado de conocimientos y habilidades informáticas o de tecnología de la información necesarios para realizar ciertas acciones, calificadas como altas o bajas (Ver Figura 1).

Figura 1. Taxonomía de dos Factores del Comportamiento de Seguridad del Usuario Final. Fuente: Adaptado de Stanton et al. (2005)

La Tabla 1 muestra los nombres de cada una de las seis categorías de la taxonomía, con sus respectivos niveles de intención y experiencia. Además, presenta ejemplos de acciones que pueden cometer los usuarios finales en cada uno de los comportamientos categorizados.

Tabla 1. *Categorías de comportamientos de los usuarios finales con respecto a la intención y experiencia*

Categoría	Experiencia	Intención	Acciones
Destrucción Intencional	Experto	Causar daño	• Robar secretos comerciales descifrando archivos protegidos • Implantar troyanos. • Clonar correos electrónicos. • Crear ataques de denegación de servicio.
Acción Indebida Perjudicial	Básico	Causar daño	• Enviar códigos maliciosos utilizando usuarios no autorizados. • Enviar spam o mensajes de acoso utilizando el correo electrónico institucional.
Reparaciones Peligrosas	Experto	Ninguna	• Configurar una aplicación de suplantación de paquetes para probar la capacidad de programación. • Configurar un escáner de monitoreo de red en su computador. • Configurar una puerta de enlace inalámbrica que permite el acceso de personas no autorizadas a la red de la organización.
Error Ingenuo	Básico	Ninguna	• Dejar una computadora sin supervisión. • Acceder a sitios web dudosos. • Elegir una contraseña incorrecta utilizando el número de identificación. • Escribir la contraseña en una nota adhesiva en el monitor. • Compartir información con otro usuario.
Aseguramiento Consciente	Experto	Hacer el bien	• Realizar programas de capacitación sobre la sensibilidad y criticidad de archivos. • Cerrar la computadora cuando se deja de usar. • Actualizar las contraseñas con regularidad.
Higiene Básica	Básico	Protección	• Resistir a un intento de ingeniería social al negarse a revelar su contraseña. • Informar de una vulnerabilidad de seguridad descubierta. • No divulgar datos o información de la empresa.

Fuente: Adaptado de Stanton et al. (2005).

Taxonomía de Comportamiento Compatible con la Seguridad de la Información.

Padayachee (2012) propone una taxonomía que decodifica el elemento conductual en los factores relevantes para el cumplimiento de las PSI. Su investigación se fundamenta en que la seguridad de información constituye un problema humano y que se deben considerar aspectos tales como la percepción, comportamiento y actitud (Crossler et al., 2012; Herath y Rao, 2009; Kraemer et al., 2009; Padayachee, 2012). Además de construir una cultura de seguridad al integrar la seguridad de información en una organización (Da Veiga y Martins, 2015).

La taxonomía está basada en la Teoría de la Autodeterminación (Deci y Ryan, 1985) por ser una de las teorías conductuales más influyentes en psicología (Padayachee, 2012) y fue realizada conforme a una revisión no sistemática ni exhaustiva sobre la base de la investigación empírica previa.

Padayachee (2012) categoriza la amenaza interna según los determinantes que la crean e identifican a aquellos que pueden estar relacionados con dos tipos de motivación (intrínseca y extrínseca) (Deci y Ryan, 1985) o desmotivación (Ver Tabla 2).

La motivación intrínseca, se refiere a realizar acciones propias de pertenencia, interesantes o deseables (Padayachee, 2012; Ryan y Deci,

2000; Tyler y Blader, 2005), siendo la más esperada aunque debe ser impulsada por factores externos. En cambio, la motivación extrínseca se refiere a realizar acciones que conlleva una recompensa en los factores externos (Herath y Rao, 2009; Padayachee, 2012; Ryan y Deci, 2000). Mientras que la desmotivación, la menos deseable para el comportamiento, se refiere a un estado de falta de intención de actuar, porque el usuario final no valora una actividad o siente ser incompetente para realizarla (Padayachee, 2012).

Además, Padayachee (2012) identifica aquellos factores que influyen de manera positiva hacia una respuesta de cumplimiento de seguridad de información; así como, aquellos factores que disminuyen o fomentan una respuesta inadaptada o de incumplimiento de seguridad de información.

Tabla 2. *Taxonomía de Comportamiento Compatible con la Seguridad de la Información*

Motivación Extrínseca			
Regulación Externa	**Introyección**	**Identificación**	**Integración**
Controles de Disuasión# Sanciones# Certeza de las Detecciones# Celeridad de las Detecciones# Gravedad del Castigo# Supervisión# Políticas# Controles Tecnológicos# Uso de Controles Disuasivos# Controles de Acceso# Recompensas+	Clima social Comportamiento de Pares+ Prácticas de la Administración+ Desaprobación social#	Conciencia+ Disponibilidad de Recursos+ Capacitación+ Visibilidad+ Calidad de la Información+ Compromiso Organizacional+	Evaluación de Amenazas+ Probabilidad de una Brecha de Seguridad+ Severidad Percibida de Brecha de Seguridad+ Evaluación de Afrontamiento Eficacia de Respuesta+ Costo de Respuesta# Locus de Control+ Autoeficacia+

Desmotivación	**Motivación Intrínseca**
Apatía*	Competencia+ (habilidades)
Resistencia*	Modo de Portarse+ (Buenos Hábitos)
Desobediencia*	Compromiso+
Bajo Autocontrol*	Obediencia+
Oportunista*	Ética+
Incompetencia*	Auto-desaprobación#
Comportamiento Desviado Pasado *	

Fuente: Adaptado de Padayachee (2012)

Marco de Conceptualización del Comportamiento relacionado con la Seguridad de Información.

Guo (2013), con base en una revisión de la literatura de la seguridad de información, realiza un análisis sobre los conceptos divergentes en relacion a la intención como el predictor del comportamiento de los empleados que pueden provocar incidentes de seguridad de información por negligencia, error o ataque malintencionado deliberado. Como resultado de su investigación presenta un marco que conceptualiza el comportamiento de seguridad de la variable dependiente (Ver Tabla 3).

Este marco de conceptualización, clasifica el comportamiento de los usuarios finales en cuatro categorías, el comportamiento de garantía de seguridad, el comportamiento conforme a la seguridad, el comportamiento de asumir riesgos de seguridad y el comportamiento perjudicial para la seguridad. Las dos últimas categorías podrían presumir un riesgo para la seguridad de la información (Guo, 2013). El comportamiento de asumir riesgos de seguridad, que puede terminar en un mal resultado (Hannah y

Robertson, 2015), no está alineado, por ejemplo, con las PSI y talvez ponga en riesgo la información de la organización, aunque no sea intencional. En cambio, el comportamiento perjudicial, dañino de seguridad es malicioso, intencional que puede provocar daño directo y terminar en un mal resultado para la organización (Hannah y Robertson, 2015).

No obstante, la investigación de Guo (2013) contribuye a la comprensión de los problemas de comportamiento de la seguridad de información, pero el autor señala que persistieron hallazgos inconsistentes conforme a otras investigaciones, debido a diversas razones; entre las cuales cita, el muestreo, análisis estadístico, errores de exclusión de los determinantes importantes y conceptualizaciones discordantes de los comportamientos relacionados a la seguridad (Chatterjee, Sarker y Valacich, 2015).

Tabla 3. *Conceptualización del Comportamiento relacionado con la Seguridad*

Comportamiento relacionado con la seguridad	**Comportamiento de garantía de seguridad**	**Comportamiento conforme a la seguridad**	**Comportamiento asumir riesgos de seguridad**	**Comportamiento perjudicial para la seguridad**
Definición	Comportamientos activos de un individuo que tiene un motivo claro para proteger los SI de la organización	Comportamientos acordes con las políticas de seguridad de la organización	Comportamiento que puede poner en riesgo los SI de la organización	Comportamientos que causarán daño directo a los SI de la organización
Ejemplo	Toma precauciones; informar incidentes	Abstenerse de comportamiento prohibido	Reducción de contraseña; copiar datos confidenciales a dispositivos móviles	Quiebre de contraseña; robo de datos
Intencionalidad	Intencional	Intencional o no intencional	Intencional	Intencional
Motivo (desde la perspectiva de seguridad)	Beneficioso	Neutral	Neutral	Malicioso
Experiencia	Alta	Baja a Alta	Baja a Alta	Alta
Rol	Usuarios finales y personas de SI	Usuarios finales y personas de SI	Usuarios finales y personas de SI	Más probablemente IS personas
Relación de trabajo	No	No	Si	No
Consecuencia	Mejorar la seguridad	(No aplicable)	Riesgo	Daño directo
Acción o inacción	Acción	Acción o inacción	Acción	Acción
Regla - Norma	(No aplicable)	Política organizacional	Política organizacional	Leyes y política organizacional
Otras Características	Hace lo que no se espera que haga	No hace lo que se espera que no haga	Hace lo que se espera que no haga	Hace lo que se prohíbe hacer

Fuente: Adaptado de Guo (2013)

Taxonomía de Usuarios Internos.

Balozian y Leidner (2017) presentan una taxonomía integral de usuarios internos que están autorizados a usar un sistema o instalación en particular (Neumann, 1999) en las organizaciones, para lo cual hacen una revisión de literatura de forma inductiva y un doble proceso de selección para ser más inclusivos. En el primer proceso, realizan una búsqueda de artículos de cumplimiento de PSI en las 24 revistas del ranking mundial y un diario incluido en la clasificación de eruditos senior utilizando bases de datos que incluyen revistas de seguridad de información previamente seleccionadas. Además, filtran la búsqueda en los años de publicación desde 1990 hasta 2015.

En el segundo proceso, revisan las referencias de los artículos seleccionados anteriormente para verificar la inclusión de artículos relevantes considerando sólo aquellos que realizan estudios empíricos. En total seleccionaron 67 artículos que investigaban amenazas internas de la seguridad de información y el cumplimiento o no cumplimiento de las PSI.

La Figura 2, muestra la taxonomía de Balozian y Leidner (2017) que divide a los usuarios de Seguridad de información en tres dimensiones: la intención (malintencionado o negligente), la capacidad (alta o baja) y la voluntad o no voluntad de cumplir, así también muestra los nombres de los tipos de usuarios internos (ingenuos negligentes, negligentes oportunistas y malintencionados).

Esta investigación, se diferencia de la taxonomía tradicional de Stanton et al. (2005) porque agrega la dimensión de la voluntad; mientras que, sin dejar de ser consistente con la taxonomía de Guo (2013), esta taxonomía es diferente en el enfoque, porque estudia los antecedentes de cumplimiento, es decir las variables independientes.

Intento	Intento No Malicioso		Intento Malicioso
Disposición / Capacidad	Dispuesto a Cumplir	No Dispuesto a Cumplir	No Dispuesto a Cumplir
Alta Experiencia	I) Obediente o Cumplidor	*III) Negligente (actos oportunistas)*	*V) Malicioso*
Baja Experiencia	*II) Negligente (actos ingenuos)*	IV) Negligente (actos oportunistas) potencial	VI) Malicioso – potencial

Figura 2. Taxonomía de Usuarios Internos. Fuente: Adaptado de Balozian y Leidner (2017)

De acuerdo con el análisis realizado sobre las taxonomías; se identifica que dos de ellas intentan explicar los tipos de comportamientos relacionados con la seguridad de la información de los usuarios finales, la taxonomía de Stanton et al. (2005) y la de Guo (2013), pueden ser equivalentes en la concepción que cada autor realiza de la intención y la motivación de los usuarios respectivamente, así como de los ejemplos de comportamientos que describen (Ver Tabla 4).

En la taxonomía de Balozian y Leidner (2017) es factible deducir los tipos de usuarios internos involucrados en las acciones conductuales de la seguridad de la información, de acuerdo con los criterios de los autores. Y, sobre la taxonomía de Padayachee (2012) es posible establecer los determinantes motivacionales extrínsecos, intrínsecos o de desmotivación que podrían aumentar o disminuir una respuesta aceptable de cumplimiento por parte de los usuarios en actividades de seguridad de la información.

Tabla 4. *Comparativo tipos de comportamiento relacionados con la seguridad de la Información (Stanton et al., 2005) - (Guo, 2013)*

Stanton(2005)	**Intención**	**Beneficiosa**	**Neutral**		**Maliciosa**
	Experiencia	**Alta - Baja**	**Alta - Baja**		**Alta - Baja**
	Ejemplo	- Hizo un programa de capacitación para aprender sobre la sensibilidad y la criticidad de los archivos especiales de la compañía para que pudiera aplicar las medidas de protección apropiadas al manejar la información. -Empleado informa una vulnerabilidad de seguridad descubierta a las autoridades apropiadas.	-El empleado configura una puerta de enlace inalámbrica que inadvertidamente permite el acceso inalámbrico a la red de la empresa por personas no autorizadas. -Elegir una contraseña incorrecta como "contraseña".		-El empleado se rompe en los archivos protegidos del empleador para robar un secreto comercial. -Utilizar el correo electrónico de la empresa para mensajes de SPAM promoviendo un negocio secundario
	Tipos de Comportamiento	Aseguramiento Consciente	Reparaciones Peligrosas		Destrucción Intencional
		Higiene Básica	Errores Ingenuos		Acción indebida perjudicial
Guo (2013)	**Tipos de Comportamiento**	Comportamiento de garantía de la seguridad	Comportamiento de asumir riesgos de seguridad	Comportamiento conforme a la seguridad	Comportamiento Perjudicial para la seguridad
	Ejemplo	-Toma precauciones; informar incidentes	-Reducción de contraseña; copiar datos confidenciales a dispositivos móviles	-Abstenerse de comportamiento prohibido	-Quiebre de contraseña; robo de datos
	Experiencia	**Alta**	**Alta - Baja**		**Alta**
	Motivación	**Beneficiosa**	**Neutral**		**Maliciosa**

Metodología

En esta investigación se realizó una revisión sistemática cualitativa de los estudios referentes al cumplimiento de PSI de los empleados en las organizaciones, comprendidos entre el año 2000 hasta el 2016, siguiendo la metodología descrita por Kitchenham (2004), que incluye:

- Establecer el objetivo de la investigación.
- Especificar las preguntas de investigación que se pretende responder.
- Presentar la estrategia para la búsqueda de documentos, en el que se establece, con base en las preguntas de investigación, los términos de búsqueda a considerar y los recursos a utilizar como revistas, bases de datos, referencias de los estudios primarios, etc.
- Determinar los criterios de inclusión y exclusión de los estudios.
- Evaluar la calidad de los estudios.
- Definir el procedimiento de recopilación de datos a través de formularios.
- Establecer el procedimiento de selección de estudios en el que se aplica los criterios de inclusión y exclusión generando una lista detallada de los documentos finalmente seleccionados como de los excluidos.

Luego, los tres autores analizaron cada una de las taxonomías identificadas; a través de la revisión de las referencias que las citaban, de manera que fueron escogidas considerando el número citaciones, a excepción del trabajo de

Balozian y Leidner (2017) que fue seleccionado debido a su pertinencia al tema de esta investigación (Ver Apéndice A). A partir de esta disección, se definieron los parámetros a seguir para el proceso de clasificación de los documentos relevantes obtenidos en la revisión sistemática; luego, de manera proporcional, los documentos fueron distribuidos a dos autores quienes realizaron la clasificación. En tres sesiones de trabajo con la participación de los tres autores se describían los casos particulares suscitados en el que no había un acuerdo en la clasificación de los documentos; de manera que, luego del análisis se llegó a un consenso logrando los resultados que se presentan en esta investigación.

Resultados

Revisión Sistemática.

Pregunta de Investigación.

¿Cuál es el estado del arte del comportamiento de seguridad de la información a través de las cuatro taxonomías seleccionadas?

Proceso de Búsqueda.

Desde octubre del 2016 a agosto del 2017 se realizó la búsqueda para identificar palabras claves, frases o conceptos relacionados con la pregunta de investigación. Luego, se procedió a utilizar las ecuaciones descritas en la Tabla 5 en la base de datos Scopus y Web of Science [WOS]. La ecuación de búsqueda 1 fue planteada por los autores; y, debido a la gran cantidad de artículos obtenidos, se limitó a las áreas de estudio Negocios, Ingeniería y Ciencias de la Computación. La ecuación de búsqueda 2, es una adaptación de la utilizada en el metanálisis de Sommestad, Hallberg, Lundholm, y Bengtsson (2014).

Criterios de Inclusión y Exclusión.

Con el fin de alcanzar el objetivo de esta investigación, se definieron los criterios de inclusión y exclusión para la selección de los estudios primarios y secundarios con base en la pregunta de investigación planteada.

Tabla 5. *Ecuaciones de Búsqueda en base de datos Scopus y WOS*

Búsqueda	Scopus	Fecha Consulta	Web of Science	Fecha Consulta
1	TITLE-ABS-KEY (security policy compliance behavior) AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"re")) AND (LIMIT-TO (SUBJAREA,"COMP") OR LIMIT-TO (SUBJAREA,"BUSI") OR LIMIT-TO (SUBJAREA,"ENGI")) AND (EXCLUDE (SUBJAREA,"ENGI"))	Julio 2017	TOPIC (security policy compliance behavior) Refined by: DOCUMENT TYPES:(ARTICLE OR PROCEEDINGS PAPER) AND WEB OF SCIENCE CATEGORIES: (COMPUTER SCIENCE INFORMATION SYSTEMS OR BUSINESS) Timespan: 2001-2016	Septiembre 2017
2	(TITLE-ABS-KEY("enforcing information security ") OR TITLE-ABS-KEY("compliance with information security") OR TITLE-ABS-KEY("compliant to information security") OR TITLE-ABS-KEY("adherence to information security") OR TITLE-ABS-KEY("adhere to information"))*	Agosto 2017	TITLE: (enforcing information security) OR TITLE: (compliance with information security) OR TITLE: (compliant to information security) Timespan: 2001-2016	Septiembre 2017

NOTA: * AND (LIMIT-TO (PUBYEAR,2016) OR LIMIT-TO (PUBYEAR,2015) OR LIMIT-TO (PUBYEAR,2014) OR LIMIT-TO (PUBYEAR,2013) OR LIMIT-TO (PUBYEAR,2012) OR LIMIT-TO (PUBYEAR,2011) OR LIMIT-TO (PUBYEAR,2010) OR LIMIT-TO (PUBYEAR,2009) OR LIMIT-TO (PUBYEAR,2008) OR LIMIT-TO (PUBYEAR,2007) OR LIMIT-TO (PUBYEAR,2006) OR LIMIT-TO (PUBYEAR,2001))

Criterios de Inclusión

- Estudios cuyo título, palabras claves, contengan uno o más términos relacionados a la pregunta de investigación, y el resumen incluya información explícita sobre comportamiento de cumplimiento, no cumplimiento o violación de las PSI de los usuarios finales en las organizaciones.
- Estudios cuyos modelos hayan sido probados de forma empírica en organizaciones con evidencias de los resultados obtenidos y que midieran cumplimiento o no cumplimiento de las PSI.
- Estudios que hayan utilizado PLS como técnica estadística (Lowry y Gaskin, 2014); en virtud de que, en esta área de investigación la mayoría de los estudios son predictivos.
- Estudios cuyas conclusiones hayan sido presentadas de manera coherente desde el punto de vista teórico o metodológico.

Criterios de Exclusión

- Estudios fuera del período establecido 2000 – 2016.
- Tesis doctorales, libros y capítulos de libro.
- Estudios no indizados en Scopus y WOS.

Proceso de Selección de Estudios.

Los pasos del proceso de búsqueda y selección de estudios con sus resultados se muestran en la figura 3. Para almacenar y organizar todos los documentos de esta investigación se utilizó Mendeley. Las búsquedas automatizadas de publicaciones generaron como resultado 168 documentos, de la inspección de las referencias de los artículos se obtuvo 11 estudios adicionales, además se identificaron cuatro taxonomías y dos estudios secundarios (Ver Tabla 6) de los cuales se consideraron 57 publicaciones más; de esta forma, se obtuvo un total de 236 documentos que pasaron al primer proceso de selección.

En el primer proceso de selección participaron los tres autores, y se excluyeron 56 estudios repetidos, además de 35 estudios de las búsquedas de Scopus, y 40 de las búsquedas de WOS, debido a que en los metadatos de las publicaciones (título, palabras claves y resumen) no se evidenció el aporte directo para responder a las preguntas planteadas en esta investigación.

Así mismo, del estudio secundario uno, se excluyeron dos que no correspondían a publicaciones en revistas y del estudio secundario dos, se excluyó un repetido. De igual forma, se descartaron dos estudios porque no correspondían al periodo 2000-2016, uno por ser libro, uno por ser un capítulo de libro, uno por ser tesis doctoral y tres por no estar indizados en Scopus o WOS.

Tabla 6. *Documentos adicionales encontrados en estudios secundarios*

Estudio Secundario	Referencia	Cantidad
1	(Boss, Galletta, Lowry, Moody, y Polak, 2015)	28
2	(Sommestad et al., 2014)	29

De esta manera, 94 documentos pasaron al proceso de lectura exhaustiva en el que, se registraron en formularios en Excel datos como: título completo, detalles de la publicación (revista, autores, año, volumen), fecha de consulta, resultados de la aplicación de los modelos, tamaño de la muestra, técnica estadística utilizada, e ítems de las encuestas.

Además, se solicitó a ciertos autores, información complementaria que no fue evidenciada en el artículo estudiado; algunos autores contestaron a nuestra solicitud de información, mientras que otros no contestaron o enviaron artículos actualizados o nuevos; de este último grupo, 3 fueron incluidos al conjunto de análisis.

En consecuencia, se registró 97 estudios primarios que pasaron al segundo proceso de selección en el que estuvieron involucrados los tres autores y con base en los criterios de inclusión y exclusión se descartaron los siguientes: doce porque el modelo no fue aplicado a empleados en organizaciones, uno por no estar indizado en Scopus o WOS, 23 por no realizar pruebas empíricas, once porque no medían cumplimiento, intención de cumplimiento o no cumplimiento de PSI, 14 por no usar PLS como técnica estadística, dos por no presentar los resultados de las pruebas empíricas, uno por el tamaño de la muestra, tres por tener información incompleta.

Como resultado del segundo proceso de selección se obtuvieron 30 estudios considerados relevantes y pertinentes para nuestro análisis; de los cuales, según las variables dependientes del comportamiento de seguridad de la información, se determina que: 16 miden intención de cumplimiento de las PSI, 6 estudios miden cumplimiento real de las PSI, 5 miden intención de violación o no cumplimiento de las PSI, entre otros (Ver Tabla 7).

Además, el 17% de los artículos analizados corresponden al año 2010, mientras que los estudios del 2011, 2012 y 2014 representan el 13% cada uno del total; así mismo, el 27% de los estudios se desarrollaron en Estados Unidos y el 24% en Finlandia; los modelos fueron aplicados a empleados de diversas compañías en un 28%, mientras que el 13% reflejan haber sido aplicados a empleados del área de tecnología de la información y sistemas de información.

Del mismo modo, el tipo de política de seguridad que más se ha empleado es el de uso de contraseñas con un 16% del total analizado; sin embargo, el 18% no describió el tipo de política utilizado. En el apéndice B se detallan los datos demográficos de los 30 estudios seleccionados.

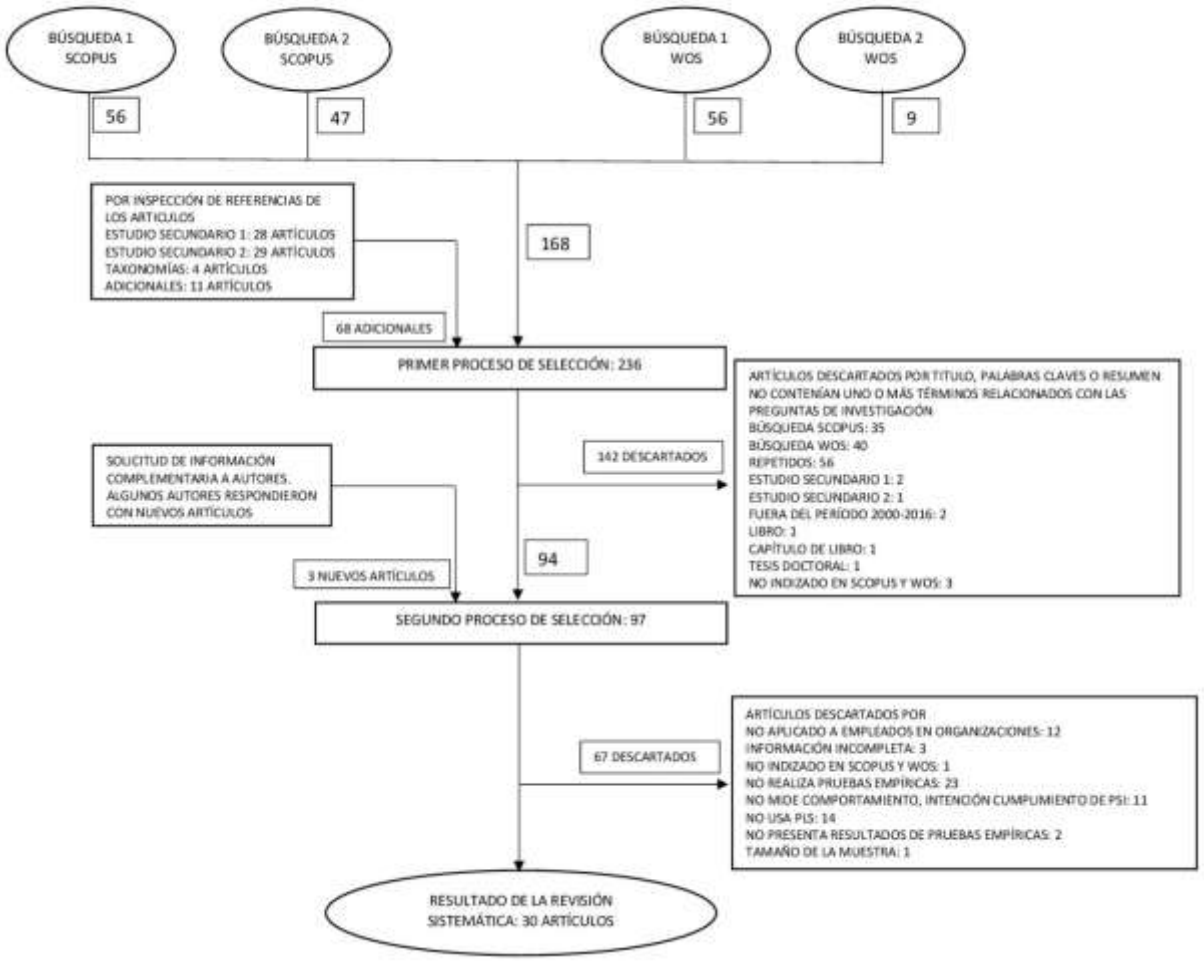

Figura 3. Proceso de búsqueda y selección de estudios

Tabla 7. *Clasificación de los estudios según las variables dependientes que analizan*

Intención de Cumplimiento	Intención de Violación o No Cumplimiento	Cumplimiento Real
Al-omari y El-gayar, 2012 Aurigemma y Mattson, 2014 Aurigemma y Mattson, 2015 Benbasat, 2010 Goo et al., 2014 Herath y Rao, 2009a Ifinedo, 2012 Johnston, Wech, Jack, y Beavers, 2010 Johnston et al., 2015 Li, Zhang, y Sarathy, 2010 Pahnila et al., 2007b Sohrabi Safa, Von Solms, y Furnell, 2016 Vance et al., 2012 Xue, Liang, y Wu, 2011 Zhang, Reithel, y Li, 2009 Herath & Rao, 2009b	D'Arcy et al., 2014 Hu et al., 2011 Siponen y Vance, 2010 Vance, 2012 Guo et al., 2011	Pahnila, Karjalainen, & Siponen, 2013 Huang, Parolia, y Cheng, 2016 Humaidi y Balakrishnan, 2015 Son, 2011 Yazdanmehr y Wang, 2016 Siponen, Adam Mahmood, & Pahnila, 2014
Intención y Cumplimiento Real	**Intención al Mal Uso**	**Comportamiento Omisivo**
Siponen, Pahnila, y Mahmood, 2010	D'Arcy et al., 2009	Workman, Bommer, y Straub, 2008

Clasificación de los estudios seleccionados con base en las taxonomías.

Para el proceso de clasificación de los estudios según la taxonomía de dos factores del comportamiento de seguridad del usuario final de Stanton et al. (2005); se analizó si en el contenido de cada artículo se describía la intención (maliciosa, beneficiosa o neutral) y el nivel de experiencia técnica (alta o baja) de los usuarios que intervinieron en las pruebas. En la mayoría de los casos no se especificaba tácitamente estas condiciones, por lo que fue necesario revisar los datos demográficos para identificar si eran usuarios de TI o no TI, además de los ítems del instrumento utilizado; o, los escenarios si éstos aplicaban, para contrastar los ejemplos de comportamientos usados en estos instrumentos con los descritos en la taxonomía de Stanton et al. (2005).

De esta forma, como se muestra en la figura 4, el 68% de los estudios fueron clasificados en la categoría de empleados sin ninguna intención cuyas acciones son accidentales o erróneas, con baja experiencia técnica, denominados en esta taxonomía como errores ingenuos. Un 16% se trató de empleados con intenciones beneficiosas cuyas acciones involucran proteger los activos de información contra las amenazas e informar sobre alguna vulnerabilidad de seguridad descubierta, en el que no se requiere un nivel de experiencia técnica alto, los cuales se categorizan como higiene básica. Tres estudios (Zhang et al., 2009; Johnston et al., 2010; Aurigemma y Mattson, 2015) que representan el 10% del total analizado, no se encuentran categorizados debido a la falta de evidencias (ítems del instrumento o escenarios), por lo que no fue posible contrastar los comportamientos de los usuarios con respecto a los descritos en esta taxonomía. Finalmente, ningún estudio cumplió con las descripciones de las categorías destrucción intencional y reparaciones peligrosas.

En la clasificación de los estudios según la taxonomía de comportamiento compatible con la seguridad de la información de Padayachee (2012), se consideraron sólo los constructos que resultaron significantes en los modelos aplicados, éstos fueron contrastados con los descritos en la taxonomía y el estudio fue clasificado como extrínseco, intrínseco o desmotivación según la cantidad de constructos usados en el modelo. En la figura 5 se demuestra que el 61% de los estudios utilizaron en mayor proporción determinantes de motivación extrínseca, mientras que 8 estudios (Zhang et al., 2009; Li et al., 2010; Johnston et al., 2010; Siponen & Vance, 2010; Xue et al., 2011; D'Arcy et al., 2014; Aurigemma y Mattson, 2015; Yazdanmehr y Wang, 2016) no fueron clasificados, debido a que la mayoría de los

constructos significantes no se encontraban descritos en esta taxonomía; por otro lado, un 13% de los estudios usaron en mayor grado determinantes de motivación intrínseca en sus modelos y por último ningún estudio fue clasificado como desmotivación.

Para realizar la clasificación de los estudios según el marco de conceptualización del comportamiento relacionado con la seguridad de información de Guo (2013), se procedió de manera similar que con la taxonomía de Stanton et al. (2005), identificando la intención y el comportamiento de los usuarios a través de los ítems del instrumento o escenarios, el mismo que fue contrastado con los conceptos que se describen en este marco.

De acuerdo con la figura 6, se muestra que el 50% de los estudios describen a usuarios con comportamientos intencionales o no intencionales que no violan las políticas de seguridad de la organización, los cuales se los denomina comportamiento conforme a la seguridad, el 20% especifica comportamientos intencionales que pueden poner en riesgo la seguridad (violan las políticas) pero sin la motivación de causar daño, estos son nombrados como comportamiento de asumir riesgos de seguridad; por otro lado, el 17% de los estudios detallan comportamientos intencionales cuyas acciones son las de proteger los sistemas de información, estos usuarios toman precauciones y reportan incidentes de seguridad los cuales se denominan comportamiento de garantía de seguridad, mientras que 3 estudios (Zhang et al., 2009; Johnston et al., 2010; Aurigemma y Mattson, 2015), que corresponden al 10% del total analizado, no fueron clasificados debido a la falta de evidencias (ítems del instrumento o escenarios).

En cuanto a la clasificación de los estudios según la taxonomía de usuarios internos de Balozian y Leidner (2017) se siguió la metodología descrita por los autores para la clasificación. La deducción del tipo de amenaza como se describe en esta taxonomía se realizó mediante la observación del modelo de estudio, los ítems de la encuesta y / o los escenarios, así como de los constructos utilizados en los modelos. Para clasificar los artículos en los que se trataban a usuarios como amenazas negligentes, Balozian y Leidner (2017) consideraron los siguientes constructos: autoeficacia, disponibilidad de recursos, seguridad – vulnerabilidad, educación en seguridad, capacitación, concientización o programas de capacitación, eficacia de respuesta, costo de respuesta, e impedimento de trabajo.

Así también, los autores identificaron casos en los ítems de las encuestas, como se describe: está bien compartir contraseñas con compañeros; o, está bien violar la política de seguridad de la información si no se le hace daño a la organización. Además, consideraron palabras claves como capacitación en seguridad, cumplimiento de políticas de seguridad, uso indebido de los sistemas de información, cumplimiento y conciencia de seguridad de la información. Por último, en la clasificación de los estudios que trataban a usuarios como amenazas maliciosas identificaron las palabras claves: delitos informáticos, abuso y crimen, palabras o expresiones relacionados con la venganza, empleados descontentos, actividades delictivas, comportamiento delictivo y antisocial.

Sobre la base de este análisis, se obtuvo que el 90% de los estudios describen a los usuarios como amenazas negligentes (Ver Figura 7). Con respecto al estudio de Zhang et al. (2009), no fue categorizado debido a la falta de ítems o escenarios; y, porque no fue posible identificar constructos o palabras claves tal y como describe el trabajo de Balozian y Leidner (2017).

En resumen, se puede evidenciar una asociación entre el comportamiento de violación de las políticas de seguridad con la intención de causar daño o para beneficios personales como el robo y venta de datos confidenciales a los competidores, denominado comportamiento de acciones indebidas perjudiciales (Stanton et al., 2005) con el comportamiento intencional de motivación maliciosa que puede causar daño directo a la seguridad de la organización, denominado comportamiento perjudicial para la seguridad (Guo, 2013), en el que se identifica a usuarios internos puramente maliciosos (Balozian y Leidner, 2017).

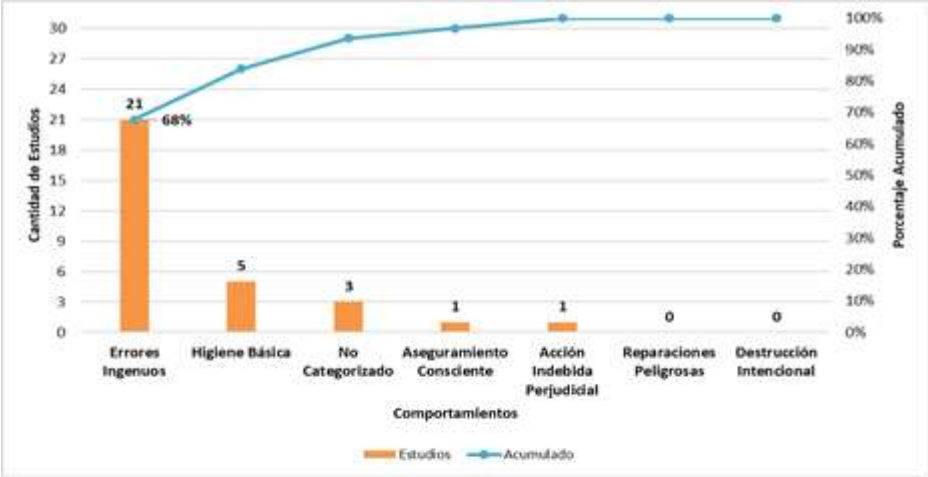

Figura 4. Porcentaje de estudios clasificados según la taxonomía de dos factores del comportamiento de seguridad del usuario final de Stanton et al. (2005)

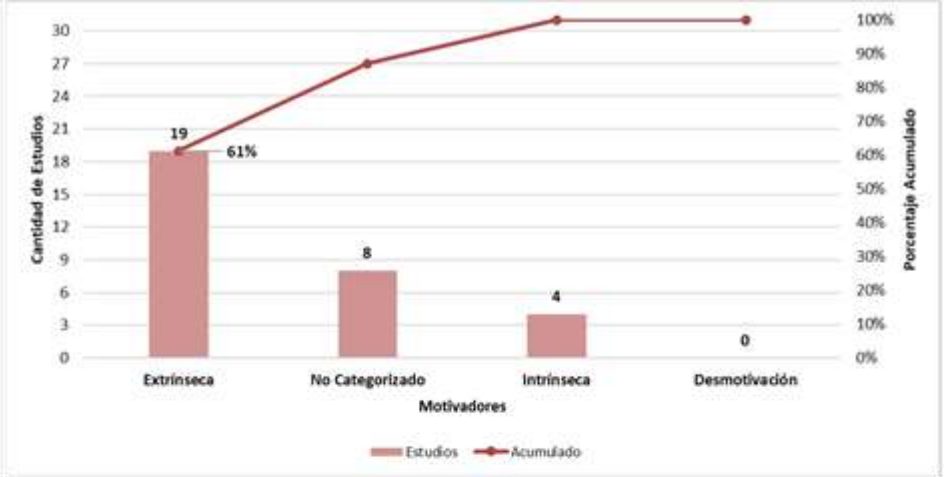

Figura 5. Porcentaje de estudios clasificados según la taxonomía de comportamiento compatible con la seguridad de la información de Padayachee (2012)

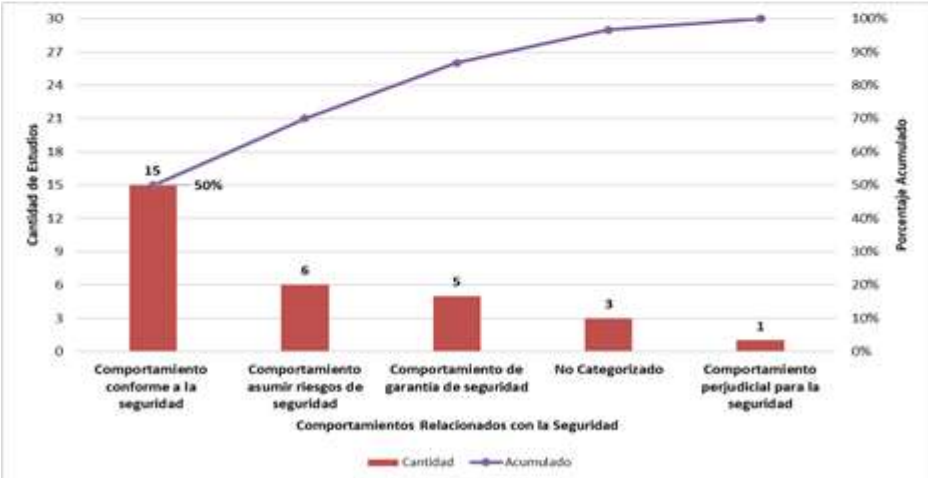

Figura 6. Porcentaje de estudios clasificados según el marco de conceptualización del comportamiento relacionado con la seguridad de información de Guo (2013)

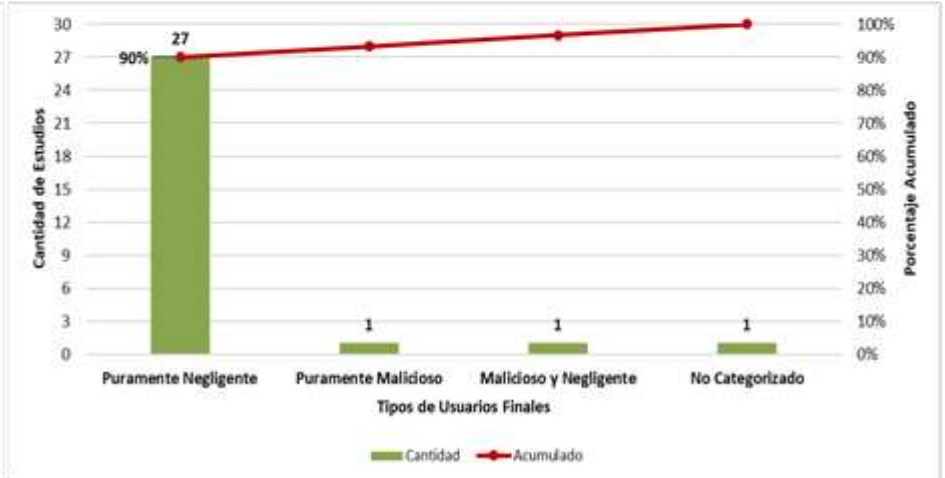

Figura 7. Porcentaje de estudios clasificados según la taxonomía de usuarios finales de Balozian y Leidner (2017)

De la misma manera ocurre con el comportamiento cuyas acciones son beneficiosas que involucran proteger los activos de información contra las amenazas e informar sobre alguna vulnerabilidad de seguridad descubierta denominado higiene básica (Stanton et al., 2005), que es comparable con el comportamiento de garantía de seguridad (Guo, 2013); sin embargo, siguiendo los parámetros de Balozian y Leidner (2017) a estos usuarios se los nombró como puramente negligentes.

En referencia a los usuarios interrnos puramente negligentes quienes no prentenden dañar a la organización, no cumplen con las políticas de seguridad por descuido, desconocimiento (negligente ingenuo); o, aún conociendo cómo proteger los activos de información de las amenazas de seguridad, eluden estas acciones en pro del rendimiento laboral u otras razones (negligente oportunista) (Balozian y Leidner, 2017), es posible apreciar una asociación cercana con el comportamiento intencional sin la motivación de causar daño que puede poner en riesgo los sistemas de información llamado comportamiento de asumir riesgos de seguridad (Guo, 2013), así como con el comportamiento llamado errores ingenuos de similares carácterísticas (Stanton et al., 2005).

Sobre los determinantentes de motivación extrínseca (Padayachee, 2012) es posible deducir que han sido utilizados para predecir el comportamiento errores ingenuos (Stanton et al., 2005) y el conforme a la seguridad (Guo, 2013), mientras que los de motivación intrínseca se han utilizado para predecir el comportamiento conforme a la seguridad (Guo, 2013).

Análisis de Resultados

Pregunta de Investigación ¿Cuál es el estado del arte del comportamiento de seguridad de la información a través de las cuatro taxonomías seleccionadas?

Para responder a esta interrogante es necesario desarrollar las siguientes preguntas:

Pregunta 1) ¿Qué tipos de comportamientos de los usuarios han sido estudiados en el comportamiento de seguridad de la información?

De las taxonomías de Stanton et al. (2005) y Guo (2013) que catalogan el comportamiento seguridad de la información de los usuarios, se puede evidenciar que aquellos que más han sido analizados, son los comportamientos de errores ingenuos en un 68% y los conformes a la seguridad en un 50% respectivamente.

Los resultados de nuestra investigación sugieren que el 70% de los estudios clasificados como comportamiento conforme a la seguridad y comportamiento de asumir riesgos de seguridad, según la taxonomía de Guo (2013) son comparables con los errores ingenuos de Stanton et al. (2005), al igual que el 17% clasificado como comportamiento de garantía de seguridad (Guo, 2013) es compatible con los comportamientos de higiene básica y aseguramiento consciente de Stanton et al. (2005) y el 3% que representa al comportamiento perjudicial a la seguridad según Guo (2013) se relaciona con los comportamientos de acción indebida perjudicial de Stanton et al. (2005) y se identifica como los menos explorados en la literatura (Ver figura 8).

Pregunta 2) ¿Qué tipos de usuarios han sido estudiados en el comportamiento de seguridad de la información?

De acuerdo con la taxonomía de Balozian y Leidner (2017), se obtuvo como resultado que los usuarios que no cumplen con las políticas de seguridad ya sea por desconocimiento, descuido o irresponsabilidad, denominados como puramente negligentes (ingenuos y oportunistas) se encuentran entre los más estudiados, mientras se evidencia poca investigación sobre los usuarios internos puramente maliciosos. Entre los 27 estudios realizados a usuarios puramente negligentes, se destaca el de Johnston et al., (2015) que fue clasificado por Balozian y su colega como malicioso y negligente, sin embargo en nuestro análisis se determinó que los ítems utilizados se refieren a comportamientos sin intención maliciosa, además los usuarios finales que intervinieron en la encuesta, se identificaron a sí mismos como directamente responsables de la protección de los datos sensibles (ver Figura 8).

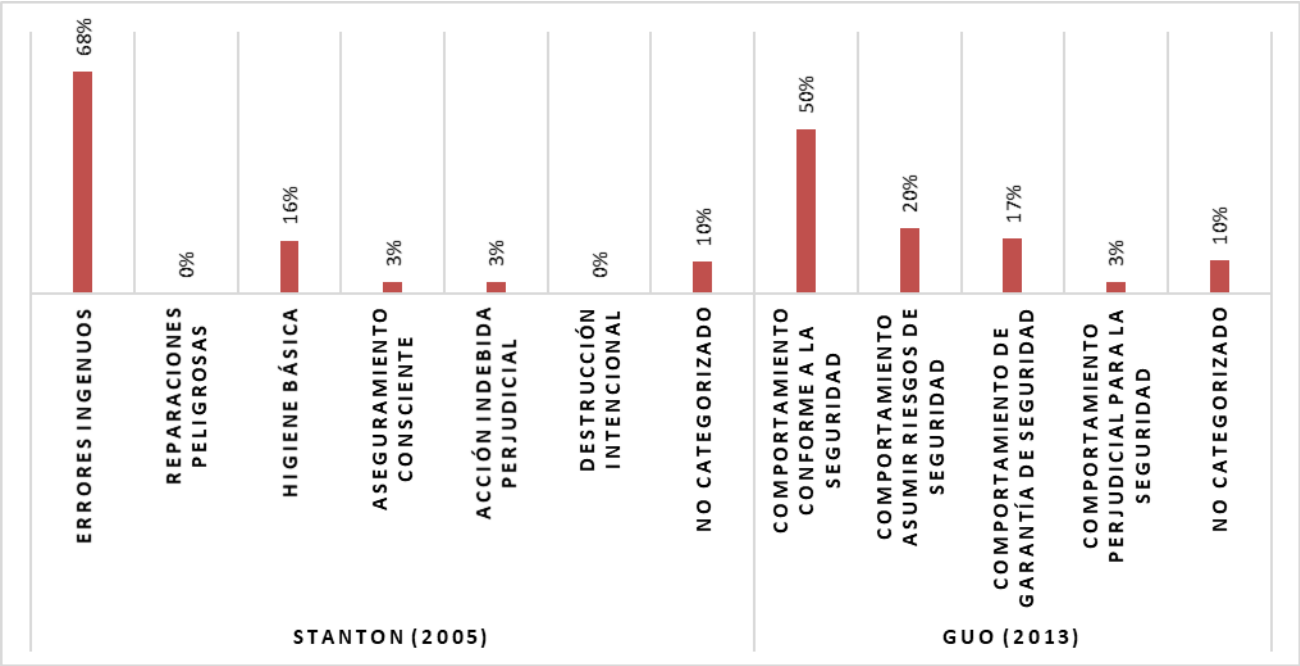

Figura 8. Clasificación de los 30 estudios según los tipos de comportamientos relacionados con la seguridad de la información

Pregunta 3) ¿Cuáles son los determinantes influyentes de los tipos de comportamiento del usuario en el comportamiento de la seguridad de la información?

Los hallazgos de la investigación revelaron que para el comportamiento de errores ingenuos (Stanton et al., 2005) y el conforme a la seguridad (Guo, 2013); resultó que, la autoeficacia de la Teoría de la Motivación de Protección (TMP) y las creencias normativas de la Teoría de la Acción Razonada (TAR) fueron las más utilizadas e influyeron en la intención de cumplimiento de las PSI de los empleados (Herath & Rao, 2009a; Siponen et al., 2010; Siponen et al., 2014; Pahnila et al., 2007b; Vance et al., 2012).

Así mismo; se encontró que, la percepción de la severidad de las amenazas y la percepción de la respuesta eficaz de TMP fueron determinantes significantes en la intención de cumplimiento de las PSI (Pahnila et al., 2013; Johnston et al., 2015), así como disminuye la probabilidad de omitir precauciones de seguridad de información (Workman et al., 2008) para los comportamientos de higiene básica (Stanton et al., 2005) y de garantía de seguridad (Guo, 2013).

Por otra parte, en el comportamiento de asumir riesgos de seguridad (Guo, 2013); se obtuvo que, la percepción de los beneficios de no cumplir que corresponde a la Teoría de la Elección Racional (TER) impacta negativamente en la intención de cumplimiento de PSI (Li et al., 2010), mientras que en la intención a violar las PSI, afecta positivamente (Vance, 2012).

Por último, en el comportamiento perjudicial a la seguridad (Guo, 2013) y en el de acción indebida perjudicial (Stanton et al., 2005), resultó que la percepción de los beneficios extrínsecos e intrínsecos de TER influyen en la intención de los empleados a violar las PSI (Hu et al., 2011) (Ver Figura 9).

Pregunta 4) ¿Cuáles son los determinantes influyentes en los tipos de usuarios que se han estudiado en el comportamiento de la seguridad de la información?

En los tipos de usuarios internos puramente negligentes, los determinantes que destacan son: la autoeficacia de TMP que influyó positivamente en la intención de cumplimiento de PSI (Pahnila et al., 2007b; Johnston et al., 2010; Siponen et al., 2010; Vance et al., 2012; Siponen et al., 2014; Johnston et al., 2015), la percepción de la severidad de la amenaza y la percepción de

la vulnerabilidad de TMP afectó en la intención de cumplimiento de PSI (Li et al., 2010; Vance et al., 2012; Pahnila et al., 2013; Siponen et al., 2014; Johnston et al., 2015) y disminuyó la probabilidad de omitir precauciones de seguridad de la información (Workman et al., 2008). Así mismo, la percepción de la certeza de las sanciones de la Teoría General de la Disuasión (TGD) tuvo un impacto significativo en la intención a cumplir con las PSI (Herath & Rao, 2009a; Herath & Rao, 2009b; Siponen et al., 2010); mientras que, en la intención al mal uso de las PSI impactó negativamente en usuarios con alto compromiso moral (D'Arcy et al., 2009).

Con base en los resultados obtenidos, se observa que en las investigaciones sobre el comportamiento de seguridad de la información se ha logrado categorizar los tipos de comportamiento de seguridad, tipos de usuarios internos, y los determinantes que influyen en la conducta de seguridad de los usuarios.

A través de las dos taxonomías (Stanton et al., 2005; Guo, 2013) que catalogan el comportamiento seguridad de la información, se evidencia un mayor énfasis de estudio de los comportamientos denominados: errores ingenuos, el de asumir riesgos de seguridad y el conforme a la seguridad; destacando que, el comportamiento perjudicial a la seguridad y el de acción indebida perjudicial son los menos analizados en la literatura.

Del mismo modo, a partir de la taxonomía de Balozian y Leidner (2017), se evidencia que los usuarios internos puramente negligentes (ingenuos y oportunistas) han sido mayormente estudiados, en contraposición a los puramente maliciosos.

Así también, es posible notar, que el determinante influyente en el cumplimiento de PSI que más se ha utilizado es la autoeficacia de la Teoría de la Motivación de Protección (TMP); y, de acuerdo con la taxonomía de Padayachee (2012), se lo cataloga como motivacional extrínseco. Además, los resultados revelan que los determinantes de desmotivación no han sido considerados en las investigaciones sobre el comportamiento de seguridad de la información.

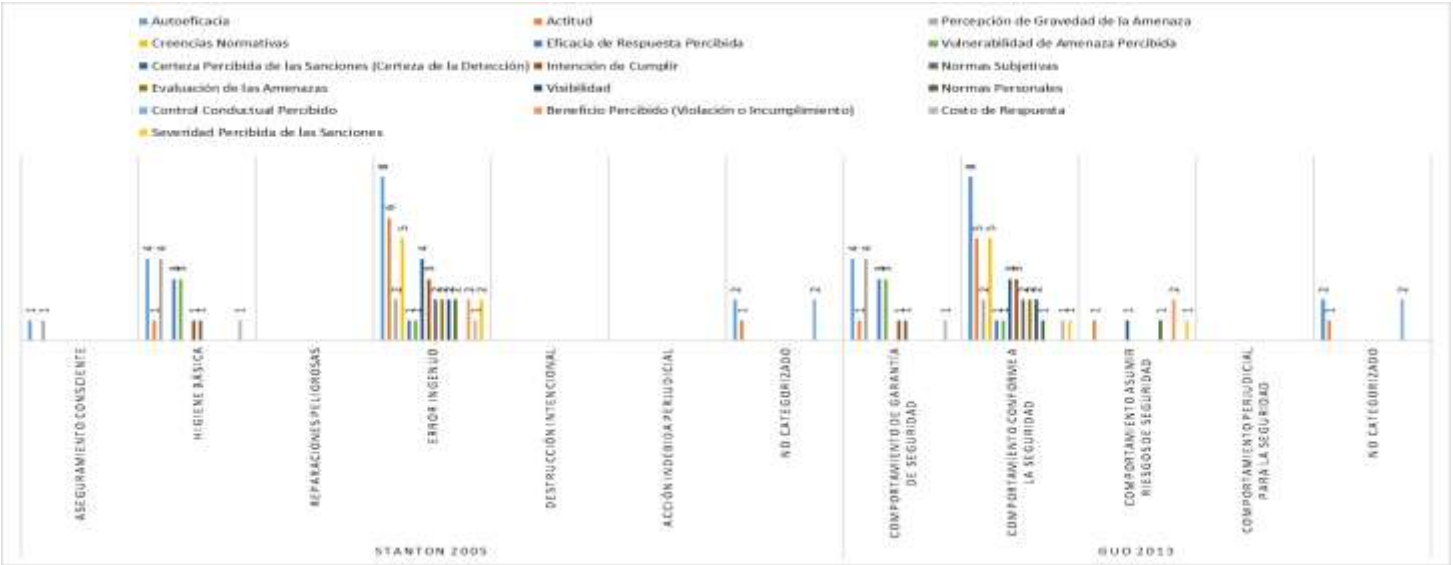

Figura 9. Determinantes influyentes en los tipos de comportamientos de seguridad de la información. Determinantes significantes en sólo un estudio: Compromiso Organizacional, Normas Descriptivas, Comportamiento de Pares, Eficacia Percibida, Probabilidad de Detección, Riesgo de Seguridad Percibido, Recompensas, Protección de Seguridad Percibida, Mecanismo, Satisfacción, Justicia de Castigo Percibida, Utilidad Percibida, Clima de Seguridad de Información, Compromiso Afectivo, Compromiso Normativo, Evitación de Seguridad, Certeza de Sanción Informal, Severidad de Sanción Informal, Conciencia, Percepción de la Celeridad de las Sanciones, Desaprobación Social, Legitimidad del Valor Percibido, Congruencia del Valor Percibido, Sanciones, Apoyo de la Gerencia, Beneficio Percibido, Barrera Percibida, Confianza Percibida, Susceptibilidad Percibida, Neutralización, Coincidencia de Identidad Percibida, Norma del Grupo de Trabajo, Sanciones Informales, Creencias Morales, Beneficios Extrínsecos Percibidos (Violación o Incumplimiento), Beneficios Intrínsecos Percibidos (Violación o Incumplimiento), Desconexión Moral, Locus de control.

CONCLUSIONES

Este trabajo muestra una revisión sistemática de los estudios existentes sobre comportamiento de cumplimiento de PSI de los empleados en las organizaciones; en el que, una contribución importante es la presentación del estado del arte del comportamiento de seguridad de la información; a través, de la clasificación de cada uno de los artículos obtenidos en la revisión, según los criterios presentados por las cuatro taxonomías seleccionadas.

A partir del análisis realizado, es posible determinar que en el área del comportamiento de seguridad de la información, se ha identificado los tipos de comportamiento del usuario final por las taxonomías de Stanton et al. (2005) y Guo (2013); en las que, los autores lograron parametrizar las acciones de los usuarios, como las de proteger los activos de TI, ayudar a otros a cumplir con las actividades de seguridad, autoeducarse en temas de seguridad de la información catalogándolas como comportamiento beneficioso inclinado a la intención o al cumplimiento de las PSI. En las acciones intencionales de no cumplimiento o evasión de las PSI, se hace una clara distinción entre las que se realizan sin la motivación de causar daño a la organización (desconocimiento, descuido, o por actividades laborales) de las que si pretenden causar perjuicio.

Con base en los resultados obtenidos, se observa que los esfuerzos de investigación para determinar los factores que influyen en el comportamiento de los empleados hacia el cumplimiento de las PSI dentro de las organizaciones se han realizado de manera generalizada, sin distinguir entre usuarios expertos o inexpertos en TI, además de los roles que ocupan dentro de la organización.

Es posible que exista una marcada diferencia entre los factores y determinantes que influyen en el comportamiento de los usuarios con pocos conocimientos en tecnología, que podrían tener la predisposición de cumplir con las PSI; pero, que no poseen la experiencia necesaria para hacerlo, que de aquellos usuarios con alto conocimiento de TI; quienes aún, conociendo cómo realizar las actividades de protección de seguridad, en ocasiones no lo hacen. Del mismo modo, la literatura revela la ausencia de estudios en los que se hayan diferenciado a los usuarios finales, de aquellos con privilegios de acceso a recursos de TI, y de los responsables de la seguridad.

Se sostiene que, para el logro de resultados eficaces que permitan establecer estrategias apropiadas en fomentar la conducta positiva de los empleados de acuerdo con su condición dentro de la organización, se deberían realizar estudios considerando el tipo de comportamiento específico a analizar, diferenciando entre muestras de usuarios según su experiencia en TI y rol que ocupa dentro de la organización, particularizando la aplicación de teorías, modelos y el empleo de encuestas u otros instrumentos de medición tomando en cuenta el enfoque conductual motivacional de cumplimiento o no cumplimiento de PSI (Crossler et al., 2012).

Las pocos estudios encontrados sobre comportamientos de intenciones maliciosas: acción indebida perjudicial, destrucción intencional (Stanton et al., 2005) y comportamiento perjudicial para la seguridad (Guo, 2013) confirma la carencia de investigación en este tema, que podría deberse a la falta de explicaciones teóricas para predecir o identificar con exactitud comportamientos maliciosos de los empleados y a la dificultad de recopilar este tipo de información, dada la no disposición de las organizaciones en revelar estos casos. (Willison y Warkentin, 2013; Balozian y Leidner, 2017). Una vía hacia futuras investigaciones en la comprensión de los factores que inducen a los empleados a inmiscuirse en comportamientos maliciosos es la aplicación de escenarios en las pruebas para medir la conducta (Pogarsky, 2004), que permiten presentar a los encuestados situaciones hipotéticas y obtener respuestas libres de sentimientos de incriminación (Crossler et al., 2012).

Otro avance significativo en la investigación del comportamiento de la seguridad de la información es la propuesta de Balozian y Leidner (2017) al tipificar a los usuarios internos de las organizaciones, describiendo a aquellos que están dispuestos a cumplir con las PSI como obedientes y cumplidores, distinguiendo de entre los negligentes a aquellos que son ingenuos (dispuestos a cumplir con las PSI pero son inexpertos, descuidados, sin conocimiento) y oportunistas (conocen cómo aplicar las PSI pero no están dispuestos a cumplir por factores no maliciosos), así como también define como maliciosos a los usuarios que no están

dispuestos a cumplir y su motivación es la de perjudicar a la organización.

Según los resultados de la clasificación realizada, se puede determinar que los usuarios negligentes son los más estudiados, considerando que se agrupó en esta categoría a todos aquellos usuarios que no tienen intención de causar daño, aunque no cumplen con las PSI, y a aquellos usuarios que intentan proteger los activos de información de la organización ya sea con alta o baja experiencia en TI; en virtud de que, Balozian y Leidner (2017) no considera de forma independiente en su investigación a los usuarios obedientes, que son aquellos que cumplen con las PSI.

Los autores sostienen que, la literatura tiende a investigar a los usuarios que no cumplen, más no busca comprender las características de los usuarios que cumplen, ni entender por qué cumplen; así mismo, determinan que los usuarios obedientes son el subproducto de implementar contramedidas que fuerzan y / o alientan a un usuario a cumplir y que estas contramedidas que pueden motivar a los posibles empleados incumplidores también motivarán a los empleados que cumplen (Balozian y Leidner, 2017). Por esta razón, a los usuarios obedientes los trata indirectamente en su investigación; y sustentan su aseveración afirmando que al tratar a los usuarios finales negligentes (ingenuos u oportunistas) indirectamente están tratando con los obedientes.

Sin embargo, Siponen y Vance (2014) recomiendan diseñar los instrumentos de una manera en la que, las suposiciones sobre generalizabilidad se consideren explícitamente; en otras palabras, los investigadores deben considerar cuál es el nivel de especificidad más apropiado en función de sus suposiciones teóricas o supuestas condiciones de frontera (cumplir o no cumplir).

En trabajos futuros sería importante aplicar modelos específicos según el tipo de usuario interno a analizar (Balozian y Leidner, 2017), separando para el caso de los negligentes a los ingenuos de los oportunistas. Una contribución para los administradores de seguridad consistiría en conocer y comprender qué tan efectivas son las estrategias organizacionales para cada tipo de usuario en particular, tanto en el incentivo al cumplimiento de PSI, así como en el desaliento al no cumplimiento de PSI (Crossler et al., 2012), como por ejemplo: ¿Los mecanismos para incrementar la conciencia de seguridad en usuarios negligentes oportunistas, contribuyen realmente a que éstos pasen a ser usuarios cumplidores de las PSI?

En referencia a los determinantes influyentes de los tipos de comportamiento en la seguridad de la información de los usuarios dentro de las organizaciones, se identifica la regularidad del uso de la autoeficacia de TMP y las creencias normativas de TAR que fueron constructos significantes en la intención de cumplimiento de PSI en empleados con comportamientos de errores ingenuos (Stanton et al., 2005), los conformes a la seguridad y el de asumir riegos de seguridad (Guo, 2013). En cuanto a los determinantes influyentes en usuarios puramente negligentes, también existe una recurrencia de uso de la autoeficacia de TMP en los estudios de intención de cumplimiento de PSI, mientras que la percepción de la severidad de la amenaza de TMP, además de influir en la intención de cumplir con las PSI, resultó ser un determinante que reduce la posibilidad de que los usuarios omitan realizar precauciones de seguridad de la información.

Por otro lado, en la investigación de los efectos disuasorios de TGD en el comportamiento de los usuarios, se ha analizado la posibilidad de una dependencia a la condición moral del individuo (Silberman, 1976; Bachman, Paternoster, y Ward, 1992; MacCoun, 1993; Strelan y Boeckmann, 2006, Strelan y Boeckmann, 2006). Un estudio previo sugiere que el nivel de moralidad de cada persona afecta en la influencia de la percepción de la severidad de las sanciones y la percepción de las certeza de las sanciones de los empleados en el uso indebido de las PSI (D'Arcy et al., 2009); por lo que, tomar en consideración el compromiso moral para futuras investigaciones en el ámbito de las transgresiones a las PSI, podría proporcionar explicaciones más precisas en la predicción de conductas delictivas (D'Arcy et al., 2009).

Así mismo, se observa en la literatura que en gran medida se han analizado los factores de predisposición personal en el estudio de cumplimiento de PSI (Goo et al., 2014), y en poco se han investigado los determinantes socio-organizacionales (Dhillon y Backhouse, 2001) como la justicia (Xue et al., 2011), compromiso organizacional (Herath y Rao, 2009b), y el clima de seguridad de la información (Goo et al., 2014),

que dentro de esta área de investigación, aportarían al conocimiento de cómo los diferentes fenómenos organizacionales afectan las conductas individuales de los empleados en el cumplimiento de PSI (Warkentin y Willison, 2009).

Otra brecha encontrada en la investigación del cumplimiento de PSI es la exploración de la influencia de las acciones inconscientes o automáticas, y rutinarias denominadas como hábitos. El hábito tiene la capacidad de explicar las conductas relacionadas con sistemas de información que no están vinculadas con el total control consciente del individuo (Limayem, Hirt, y Cheung, 2007). Los pocos estudios encontrados sobre este tema, revelan que el comportamiento pasado influye en los procesos de evaluación y afrontamiento de las amenazas (Vance et al., 2012), así como afecta positivamente de manera directa en la intención de cumplimiento de PSI (Pahnila et al., 2007a). Un mayor énfasis en esta subárea de investigación, ayudaría a comprender la naturaleza y beneficios asociados al hábito, otorgando a los oficiales de seguridad las bases para la toma de decisiones correctas en el fomento del hábito de ciertos comportamientos relacionados con la seguridad de la información (Limayem et al., 2007).

En concurrencia con investigaciones previas; los hallazgos del presente trabajo sugieren que, la metodología utilizada es robusta en cuanto a la selección de las bases de datos, la calidad de los estudios seleccionados y la aplicación minuciosa de los criterios de inclusión y exclusión; sin embargo, debe tomarse en cuenta ciertas limitaciones al interpretar los resultados. Primero por diseño; ya que, la mayoría de las investigaciones mencionadas en este documento se exploraron en diferentes contextos organizacionales y en un solo país, a excepción de Pahnila et al., (2013) que lo realizó en 4 países. Aunque los resultados de los modelos son consistentes en todas las organizaciones y países en los que fueron realizados, extrapolar los resultados para el estudio en diferentes tipos de organizaciones y culturas se lo debe realizar con cautela y no generalizar los hallazgos, porque las normas y dinámicas culturales pueden influir de manera única en las percepciones y relaciones individuales con la organización (Schneider, 1989), particularmente en el área de seguridad de la información.

En este sentido, se observa que el estudio sobre el cumplimiento de PSI se lo ha realizado en mayor medida en países del continente europeo seguido por los llevados a cabo en América del Norte, presentando una carente investigación de este tema en los países latinoamericanos; es así que, se debería inquirir si los resultados obtenidos en las culturas europeas y noroccidentales sobre los determinantes que influyen en el cumplimiento de PSI también producen el mismo efecto en empleados de las culturas latinoamericanas.

Es importante examinar además, que en mayor proporción se ha investigado sobre el cumplimiento de políticas de uso de contraseñas; ante esta realidad, los investigadores deberían preguntarse si es coherente analizar el cumplimiento de alguna política en particular indistintamente del tipo de organización en la que se aplica; por ejemplo, en una organización financiera donde se requiere el compromiso de confidencialidad de los empleados sobre la información personal de los clientes, podría ser de mayor utilidad realizar estudios de cumplimiento con respecto a políticas que regulen la copia de datos sensibles, el uso de unidades extraíbles o fuga de datos.

Segundo, en el análisis de la variable dependiente, se exhibe que los estudios sobre la intención de cumplimiento es mayormente recurrente que el cumplimiento real y aunque se sostiene que, la medida de intención de cumplimiento es una aproximación útil del comportamiento ya que proporciona información valiosa sobre los resultados de cumplimiento de PSI; es posible que las intenciones informadas de los encuestados difieran de sus comportamientos reales, porque siempre hay alguna discrepancia entre lo que las personas informan sobre sus comportamientos y lo que realmente hacen, en virtud de la deseabilidad social y la aquiescencia (Crossler et al., 2012). De modo que, utilizar medidas de observación objetiva, sería la alternativa para futuras investigaciones, no solo para abordar esta limitación, sino también para explorar dónde podrían existir discrepancias.

En conclusión, es posible determinar que la necesidad de investigación sobre el comportamiento de seguridad de la información, basada en la teoría académica y la evaluación empírica persiste (Balozian y Leidner, 2017). Se considera necesario abordar los retos planteados

en este trabajo; de manera que, los aportes de la investigación futura en entornos organizacionales contribuyan a la definición de tácticas específicas y adecuadas, de acuerdo con el tipo de organización y de usuarios que se analiza; y que, como resultado sea posible incitar al cumplimiento o desalentar el no cumplimiento de PSI a los empleados. Así también, se logre evaluar y auditar los comportamientos de los usuarios (Stanton et al., 2005), permitiendo a los responsables de la seguridad de la información prevenir, detectar y quizá contrarrestar las amenazas internas, al punto de establecer el nivel confiable de acceso de los empleados a los recursos de TI.

Referencias Bibliográficas

Al-omari, A., & El-gayar, O. (2012). Information Security Policy Compliance : The Role of Information Security Awareness. *18th Americas Conference on Information Systems 2012, AMCIS 2012*, 1–10.

Aurigemma, S., & Mattson, T. (2014). Do it OR ELSE ! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies. *Amcis 2014*, 1–12.

Aurigemma, S., & Mattson, T. (2015). The role of social status and controllability on employee intent to follow organizational information security requirements. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2015–March*, 3527–3536. https://doi.org/10.1109/HICSS.2015.424

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3248–3257. https://doi.org/10.1109/HICSS.2012.49

Aytes, K., & Conolly, T. (2003). A research model for investigating human behavior related to computer security. *In Proceedings of the 9th Americas Conference on Information Systems*, 1–6. Retrieved from http://aisel.aisnet.org/amcis2003%5Cnhttp://aisel.aisnet.org/amcis2003/260

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law and Society Review*, 343–372.

Balozian, P., & Leidner, D. (2017). Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *48*(3), 11–43. https://doi.org/10.1145/3130515.3130518

Benbasat, I. (2010). Information Security Policy Compliance an empirical study of rationality based beliefs and information security awarnesse. *MIS Quarterly: Management Information Systems*, *34*(3), 523–548.

Bonar, E. E., & Rosenberg, H. (2011). Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies. *Addictive Behaviors*, *36*(11), 1038–1044. https://doi.org/10.1016/j.addbeh.2011.06.010

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have To Fear? Using Fear Appeals To Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164. https://doi.org/10.1057/ejis.2009.8

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.1093/bja/aeq366

Campbell, K., Gordon, L. a, Loeb, M. P., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, *11*(May 2001), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87–92. https://doi.org/10.1145/1005817.1005828

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49–87. https://doi.org/10.1080/07421222.2014.1001257

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning & Performance Journal*, *24*(1), 1–14. Retrieved from http://search.proquest.com/openview/3321556a4203a04b8d265d449327c92a/1?pq-origsite=gscholar%0Ahttp://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=87d7976e-feb9-4d5f-b6f2-a7f931d20b63@sessionmgr14&vid=3&hid=9

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, *29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

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

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-dtermination in human behavior*. *Springer*. Retrieved from http://www.springer.com/gp/book/9780306420221

Deloitte. (2016). La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información. Encuesta 2016 sobre tendencias de ciber-riesgos y seguridad de la información en Latinoamerica. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte 2016 Cyber Risk Information Security Study - Latinoamérica - Resultados Generales vf (Perú).pdf

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Ernst & Young. (2017). EY's 19th Global Information Security Survey 2016-17.

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security*, *2009*(2), 5–10. https://doi.org/10.1016/S1361-3723(09)70019-3

Goo, J., Yim, Y.-S., & Kim, D. J. (2014). A Path to Successful Management of Employee Security Compliance : An Empirical Study of Information Security Climate. *IEEE Transactions on Professional Communication*, *57*(4), 286–308.

Grasmick, H. G. (Universit. of O., & Bryjak, G. J. (University of S. D. (1980). The deterrent effect of perceived severity of punishment. *Social Forces*. https://doi.org/10.1093/sf/59.2.471

Guo, K. H. (2013). Security-related behavior in

using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*(1), 242–251. https://doi.org/10.1016/j.cose.2012.10.003

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208

Hannah, D. R., & Robertson, K. (2015). Why and how do employees break and bend confidential information protection rules? *Journal of Management Studies*, *52*(3), 381–413. https://doi.org/10.1111/joms.12120

Harrington, S. J. S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *Misq*. https://doi.org/10.2307/249656

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–659.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54–60. https://doi.org/10.1145/1953122.1953142

Huang, H.-W., Parolia, N., & Cheng, K.-T. (2016). Willingness and Ability To Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective. *Pacis*. Retrieved from http://aisel.aisnet.org/pacis2016/57

Humaidi, N., & Balakrishnan, V. (2015). the Moderating Effect of Working Experience on Health Information System. *Malaysian Journal of Computer Science*, *28*(2), 70–92.

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18.

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions. *Information Management & Computer Security*, *17*(5), 372–387. https://doi.org/10.1108/09685220911006678

Ifinedo, P. (2011). An Exploratory Study of the Relationships between Selected Contextual Factors and Information Security Concerns in Global Financial Services Institutions. *Journal of Information Privacy and Security*, *7*(1), 25–49. https://doi.org/10.1080/15536548.2011.10855904

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

Im, G. P., & Baskerville, R. (2005). A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. *The DATA BASE for Advances in Information Systems*, *36*(4), 68–79. https://doi.org/http://doi.acm.org/10.1145/1104004.1104010

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113–134.

Johnston, A. C., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: Applying social learning theory

to explain information security policy compliance attitudes. *16th Americas Conference on Information Systems 2010, AMCIS 2010*, *3*, 2217–2230. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84870327508&partnerID=40&md5=b4729455201c6b2a685d3ace72756df6

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555.

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

Kling, R. (1980). Computer abuse and computer crime as organizational activities. *SIGCAS Computers and Society*, *11*(4), 12–24. https://doi.org/10.1145/957869.957871

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers and Security*, *28*(7), 509–520. https://doi.org/10.1016/j.cose.2009.04.006

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, *41*(6), 707–718. https://doi.org/10.1016/j.im.2003.08.008

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635–645. https://doi.org/10.1016/j.dss.2009.12.005

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, *31*(4), 705–737. https://doi.org/10.1002/fut.10029

Loch, K. D., Carr, H. H., & Warkentin, M. (1992). Threats to Information Systems: Today' s Reality, Yesterday' s Understanding. *MIS Quarterly*, *16*(2), 173–186. https://doi.org/10.2307/249574

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, *57*(2), 123–146. https://doi.org/10.1109/TPC.2014.2312452

MacCoun, R. J. (1993). Drugs and the law: a psychological analysis of drug prohibition. *Psychological Bulletin*, *113*(3), 497.

Neumann, P. G. (1999). Risks of insiders. *Communications of the ACM*, *42*(12), 160.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security*, *31*(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information Security Behavior: Towards mulit-stage models. *Pacis*, 102.

Pahnila, S., Siponen, M., & Mahmood, A. (2007a). Employees' behavior towards IS security policy compliance. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 1–10). https://doi.org/10.1109/HICSS.2007.206

Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. *Pacis 2007 Proceedings*, 438–439. https://doi.org/10.1007/978-0-387-72367-9_12

Parker, D. B. (1976). *Crime by computer*. New York: Scribner. Retrieved from https://books.google.com.ec/books?id=Hj85AAAAMAAJ

Pogarsky, G. (2004). Projected Offending and Implications for Heterotypic Continuity. *Criminology*, *42*(1), 111–135. https://doi.org/10.1111/j.1745-9125.2004.tb00515.x

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information and Management*, *51*(5), 551–567. https://doi.org/10.1016/j.im.2014.03.009

Puhakainen, P. (2006). *A design theory for information security awareness*. *Processing*. Retrieved from http://en.scientificcommons.org/13922630

PwC. (2017). The Global State of Information Security® Survey 2018. Retrieved from https://www.pwc.com/us/en/cybersecurity/information-security-survey.html#insight3

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology*, *25*(1), 54–67. https://doi.org/10.1006/ceps.1999.1020

Sans Intitute. (2017). Interested in learning SANS Institute InfoSec Reading Room Defending Against the Wrong Enemy : 2017 SANS Defending Against the Wrong Enemy : 2017 SANS Insider Threat Survey.

Schneider, S. C. (1989). Strategy Formulation: The Impact of National Culture. *Organization Studies*, *10*(2), 149–168. https://doi.org/10.1177/017084068901000202

Silberman, M. (1976). Toward a theory of criminal deterrence. *American Sociological Review*, 442–461.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M. (2005). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization*, *15*(4), 339–375. https://doi.org/10.1016/j.infoandorg.2004.11.001

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71. https://doi.org/10.1109/MC.2010.35

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly: Management Information Systems*, *34*(10).

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289–305. https://doi.org/10.1057/ejis.2012.59

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*(November), 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Sommestad, T., & Hallberg, J. (2013). A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance, 257–271. https://doi.org/10.1007/978-3-642-39218-4_20

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management*, *48*(7), 296–302. https://doi.org/10.1016/j.im.2011.07.002

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Straub, D. W. (1990). Effective IS Security: An Emprical Study. *Information Systems Research*, *1*(3), 255–276.

Straub, D. W. J., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *Misq*, *14*(March), 45–60. https://doi.org/10.2307/249307

Strelan, P., & Boeckmann, R. J. (2006). Why drug testing in elite sport does not work: perceptual deterrence theory and the role of personal moral beliefs. *Journal of Applied Social Psychology*, *36*(12), 2909–2934.

Thomson, K.-L., Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. https://doi.org/http://dx.doi.org/10.1016/S1361-3723(06)70430-4

Thomson, K. L., & Von Solms, R. (2005). Information security obedience: A definition. *Computers and Security*, *24*(1), 69–75. https://doi.org/10.1016/j.cose.2004.10.005

Topa, I., & Karyda, M. (2015). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 9264, pp. 169–179). https://doi.org/10.1007/978-3-319-22906-5

Trevino, L. (1992). Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations Author (s). *Business Ethics Quarterly*, *2*(2), 121–136.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143–1158. https://doi.org/10.5465/AMJ.2005.19573114

Vance, A. (2012). IS Security Policy Violations A Rational Choice Perspective. *Journal of Organizational and End User Computing*, *24*(1).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vroom, C., & Von Solms, rossouw. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198. https://doi.org/10.1016/j.cose.2004.01.012

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. https://doi.org/10.1057/ejis.2009.12

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: an Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Workman, M., & Gathegi Jhon. (2006). Punishment and Ethics Deterrents: A Study of Insider Security Contravention. *Journal of the American Society for Information Science and Technology*, *58*(2), 212–222. https://doi.org/10.1002/asi

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, *22*(2), 400–414. https://doi.org/10.1287/isre.1090.0266

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A

norm activation perspective. *Decision Support Systems*, *92*, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340. https://doi.org/10.1108/09685220910993980

APÉNDICE A. RESUMEN DEL ANÁLISIS DE LAS REFENCIAS QUE CITAN A LAS CUATRO TAXONOMÍAS SELECCIONADAS

		NÚMERO DE CITACIONES DE LOS ARTÍCULOS SELECCIONADOS DE LA REVISIÓN SISTEMÁTICA EN LAS REFERENCIAS																													
TAXONOMÍA	CITADO	R01	R02	R03	R04	R05	R06	R07	R08	R11	R12	R13	R15	R16	R17	R18	R19	R20	R21	R22	R23	R24	R25	R27	R28	R29	R30	R31	R32	R33	R34
Stanton et al. (2005)	297	1	0	11	55	42	12	47	21	20	2	27	0	55	21	45	13	11	15	3	4	2	1	4	1	1	0	2	0	0	2
Padayachee (2012)	46	1	6	8	21	9	9	19	9	15	1	8	0	21	22	13	7	14	11	5	4	3	0	1	1	0	0	1	0	0	3
Guo (2013)	39	2	0	2	2	11	4	15	13	3	1	3	0	12	11	19	6	4	6	0	1	0	0	3	1	0	0	0	0	0	10
Balozian y Leidner (2017)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL		4	6	21	78	62	25	81	43	38	4	38	0	88	54	77	26	29	32	8	9	5	1	8	3	1	0	3	0	0	15

		NÚMERO DE CITACIONES DE LAS TAXONOMÍAS Y LOS METANÁLISIS EN LAS REFERENCIAS					
		TAXONOMÍA				METANÁLISIS	
TAXONOMÍA	CITADO	Stanton et al. (2005)	Padayachee (2012)	Guo (2013)	Balozian y Leidner (2017)	(Boss, Galletta, Lowry, Moody, y Polak, 2015)	(Sommestad et al., 2014)
Stanton et al. (2005)	297		12	8		2	5
Padayachee (2012)	46	11		3		2	9
Guo (2013)	39	4	2			4	2
Balozian y Leidner (2017)	0			1			
TOTAL		15	14	12	0	8	16

APÉNDICE B. DATOS DEMOGRÁFICOS DE LOS 30 ESTUDIOS SELECCIONADOS

FUENTE	IDENT.	AÑO	REVISTA	MUESTRA	MUESTRA DIVIDIDA	TIPOS DE COMPANIAS	NRO. DE COMPANÍAS	PAÍS	TIPO DE POLÍTICA
Al-omari, A., & El-gayar, O. (2012)	R25	2012	18th Americas Conference on Information Systems 2012, AMCIS 2012	878		Banks	9	Jordania	Information Security
Aurigemma, S., & Mattson, T. (2014)	R29	2014	20th Americas Conference on Information Systems, AMCIS 2014	48 191	Population With Punishment Experiences Population Without Punishment Experiences	United States Department Of Defense (Dod)	1	United States	Protect Against Removable Flash Media Threats
Aurigemma, S., & Mattson, T. (2015)	R33	2015	Proceedings of the Annual Hawaii International Conference on System Sciences	182		United States Department Of Defense (Dod) Multiple Organizations	No Especific	United States	Not Information
Benbasat, I. (2010)	R04	2010	MIS Quarterly: Management Information Systems	464		Diverse Companies	No Especific	United States	Not Information
D'Arcy, J., Hovav, A., & Galletta, D. (2009)	R18	2009	Information Systems Research	269		Advertising/Marketing Aerospace Financial Services Information Technology Manufacturing Other	8	United States	e-mail Communications Unauthorized Access to Computer Systems Use of Unlicensed (pirated) Software Unauthorized Modification of Computerized Data
D'Arcy, J., Herath, T., & Shoss, M. K. (2014)	R34	2014	Journal of Management Information Systems	539		No Especific	No Especific	No Especific	Password Log Out Copying Sensitive Data Data Leakage

FUENTE	IDENT.	AÑO	REVISTA	MUESTRA	MUESTRA DIVIDIDA	TIPOS DE COMPANIAS	NRO. DE COMPANÍAS	PAÍS	TIPO DE POLÍTICA
Goo, J., Yim, Y.-S., & Kim, D. J. (2014)	R24	2014	IEEE Transactions on Professional Communication	581		Information Technology Service Management Forum (Itsmf)	1	South Korea	Information Systems Security
Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011)	R08	2011	Journal of Management Information Systems	306		No Especific	No Especific	No Especific	Password Copying Sensitive Data Use of the Internet and Network Resources
Herath, T., & Rao, H. R. (2009b)	R07	2010	European Journal of Information Systems	312		Diverse Companies	78	United States	Not Information
Herath, T., & Rao, H. R. (2009a)	R16	2009	Decision Support Systems	312		No Especific	77	United States	Information Systems Security
Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011)	R21	2011	Communications of the ACM	207		Large Organizations	5	China	Not Information
Huang, H.-W., Parolia, N., & Cheng, K.-T. (2016)	R15	2016	Pacis 2016 Proceedings	234		Manufacturing Service Diverse Companies	No Especific	No Especific	Not Information
Humaidi, N., & Balakrishnan, V. (2015)	R32	2015	Malaysian Journal of Computer Science	226 228	High Experience Low Experience	Government Hospitals	3	Malasia	Password Anti-virus Protection
Ifinedo, P. (2012)	R17	2012	Computers & Security	124		Organizations	No Especific	Canada	Information Systems Security
Johnston, A.C., Warkentin, y Siponen (2015)	R27	2015	MIS Quarterly: Management Information Systems	559		Government	No Especific	Finland	Password
Johnston, A. C., Wech, B., Jack, E., & Beavers, M. (2010)	R31	2010	16th Americas Conference on Information Systems 2010, AMCIS 2010	435		Various Industries	No Especific	No Especific	Not Information
Li, H., Zhang, J., & Sarathy, R. (2010)	R19	2010	Decision Support Systems	246		No Especific	No Especific	No Especific	Use of the Internet and Network Resources

FUENTE	IDENT.	AÑO	REVISTA	MUESTRA	MUESTRA DIVIDIDA	TIPOS DE COMPANIAS	NRO. DE COMPANÍAS	PAÍS	TIPO DE POLÍTICA
Pahnila, S., Karjalainen, M., & Siponen, M. (2013)	R01	2013	Pacific Asia Conference on Information Systems	340	Low Knowledge	Differents Areas Of Business	4	Finland Switzerland United Arab Emirate China	Password Handle the Documents
				173	High Knowledge				
Pahnila, S., Siponen, M., & Mahmood, A. (2007)	R28	2007	PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises	917		Diverse Companies	4	Finland	Information Security
Siponen, M., Pahnila, S., & Mahmood, M. A. (2010)	R03	2010	IEEE Computer Society	917		Information Technology And Communication Seguridad De La Información Logística Supermarket Chain	4	Finland	Password
Siponen, M., & Vance, A. (2010)	R05	2010	MIS Quarterly: Management Information Systems	395		Administration Office Of A University Major Electrical Company Corporate Office A Large Supermarket Chain	3	Finland	Password Log Out Copying Sensitive Data
Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014)	R11	2014	Information & Management	669		Finnish Corporations In Different Business Areas	4	Finland	Not Information
Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016)	R12	2016	Computers & Security	462		Retail/Wholesale Telcoms/Information Technology Education Government	4	Malasia	Not Information

FUENTE	IDENT.	AÑO	REVISTA	MUESTRA	MUESTRA DIVIDIDA	TIPOS DE COMPANIAS	NRO. DE COMPANÍAS	PAÍS	TIPO DE POLÍTICA
Son, J. Y. (2011)	R06	2011	Information & Management	602		Diverse Companies	Varias	United States	Access and Use of Information Assets e-mail Communications Use of the Internet and Network Resources Anti-virus Protection Unauthorized Access to Computer Systems
Vance, A. (2012)	R02	2012	Journal of Organizational and End User Computing	203		High Tech Services Banks	2	Finland	Password Log Out Copying Sensitive Data
Vance, A., Siponen, M., & Pahnila, S. (2012)	R20	2012	Information & Management	210		Municipal Organization	1	Finland	Information Systems Security
Workman, M., Bommer, W. H., & Straub, D. (2008)	R13	2008	Computers in Human Behavior	588		Large Technology-Oriented Services Corporation (Pseudonym: Ingenious Company)	No Especific	United States	Password Anti-virus Protection Systems Backup
Xue, Y., Liang, H., & Wu, L. (2011)	R23	2011	Information Systems Research	118		Organizations	No Especific	China	Mandatory IT Policies (settings)
Yazdanmehr, A., & Wang, J. (2016)	R30	2016	Decision Support Systems	201		Diverse Set Of Organizations	No Especific	United States	Information Security
Zhang, J., Reithel, B. J., & Li, H. (2009)	R22	2009	Information Management & Computer Security	176		Organizations	No Especific	No Especific	Not Information