MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Réplica de un modelo de cumplimiento de la política de seguridad de la información en las organizaciones

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

Magíster en Auditoría de Tecnologías de la Información

Por las estudiantes:

Gabriela Jazmín MONTESDEOCA VÁSQUEZ

Andrea Carolina GONZAGA ACUÑA

Bajo la dirección de:

Francisco Joseph BOLAÑOS BURGOS.

Universidad Espíritu Santo

Maestría en Auditoría de Tecnología de la Información

Samborondón - Ecuador

Enero del 2018

Réplica de un modelo de cumplimiento de la política de seguridad de la información en las organizaciones.

Replica of a model of information security policy compliance in organizations.

Gabriela Jazmín MONTESDEOCA VÁSQUEZ[1]
Andrea Carolina GONZAGA ACUÑA[2]
Francisco Joseph BOLAÑOS BURGOS[3]

Resumen

El presente estudio se basa en una adaptación del modelo propuesto por Herath & Rao (2009b), para identificar los determinantes que influyen en la intención de cumplimiento de las Políticas de Seguridad de la Información (PSI) en el contexto ecuatoriano. El modelo propuesto incluye 14 determinantes sugeridos en: General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Decomposed Theory of Planned Behavior (DTPB) y Organisational Commitment (OC). El mismo que, fue ejecutado en una Empresa Pública del Ecuador, de la cual se obtuvieron 592 respuestas válidas. La relación entre los determinantes fue metodológicamente verificada mediante el análisis de ruta. Como resultado, los hallazgos de la presente investigación contradicen a los de la propuesta original, en los siguientes determinantes: (a) probabilidad percibida de violación a la seguridad, (b) actitud frente a la política de seguridad, (c) severidad del castigo y (d) costo de respuesta. Dado que en nuestro estudio los tres primeros fueron significativos y la única ruta no significativa fue costo de respuesta. El hallazgo de este último, es contrario al esperado, en base al PMT (Rogers, 1975). Las contribuciones sugieren importantes implicaciones prácticas sobre la concientización eficiente a los empleados, dado que no se han evidenciado este tipo de estudios en el contexto ecuatoriano. Además, la adaptación de este modelo contribuye significativamente debido a que se ha evidenciado pocos estudios en la literatura sobre el comportamiento organizacional y su relación con el cumplimiento de las PSI.

Palabras clave: | adaptación, análisis de ruta, cumplimiento, determinante, política de seguridad.

Abstract

This study is an adaptation of the model proposed by Herath & Rao (2009b), to identify the determinants that influence in the Information Security Policies (PSI) compliance intention in the Ecuadorean context. The proposed model includes 14 determinants suggested in: General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Decomposed Theory of Planned Behavior (DTPB) and Organisational Commitment (OC). The sample was selected from a Public Company of Ecuador, based on 592 reliable responses. The relationship between the determinants was methodologically verified through the path analysis. As a result, the findings of the present investigation contradict the findings of the original study, in the following determinants: (a) perceived probability of security breach, (b) security policy attitude, (c) punishment severity and (d) response cost. In our study, the first three ones were significant and the only no significant path was response cost. This last finding is contrary to that expected, based on the PMT (Rogers, 1975). The contributions suggest important practical implications on employee awareness due to the fact that this type of studies has not been evidenced in the Ecuadorean context. In addition, the adaptation of this model contributes significantly due to the fact that few studies have been evidenced in the literature on organizational behavior and its relationship with PSI compliance.

Key words | adaptation, path analysis, compliance, determinant, security policy.

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

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

La Seguridad de la Información (SI) se ha convertido en una parte crítica para las organizaciones (Willison & Siponen, 2009), dado que los incidentes de SI se han incrementado significativamente (Siponen, Mahmood, & Pahnila, 2014).

En este sentido, en un estudio de las organizaciones de Estados Unidos y de Europa, revela que la pérdida o robo de datos ha aumentado en un 76% y que la principal causa es por negligencia de los empleados en un 59% (Ponemon Institute, 2016). En relación a esta situación, en un estudio de Deloitte (2016), que contó también con la participación de 13 países de Latinoamérica incluido Ecuador, destaca que mediante entrevistas con Directores de SI (CISO, por sus siglas en inglés) y otros ejecutivos a cargo de la gestión de ciber-riesgos y SI, 4 de cada 10 organizaciones sufrieron un incidente de seguridad en los últimos 24 meses, esta cifra se considera relevante y es un tema de preocupación para los CISOs.

Asimismo, en un estudio realizado por ESET (2017), en el que participaron 13 países de Latinoamérica incluido Ecuador, destaca que entre los incidentes de seguridad que comprometieron los criterios principales de la seguridad como la confidencialidad, integridad y disponibilidad de la información de las organizaciones, se encuentran los códigos maliciosos como la principal causa. En el mismo estudio, en relación a la gestión de la SI, sostiene que el control principalmente utilizado son las PSI en un 74%. Es importante destacar, que desde la percepción de las organizaciones participantes, el hecho de realizar programas de concientización en temas de seguridad influye en la probabilidad de evitar un incidente de seguridad.

Con respecto a Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario. Por otro lado, el 60% utiliza la misma contraseña en los dispositivos laborales y personales; el 59% almacena información laboral en la nube y el 35% ha hecho clic en correos recibidos por emisores desconocidos (Policía Nacional del Ecuador, 2016). Además, Gelbstein (2012) indica que este tipo de comportamientos cuando es adoptado en la organización, es difícil cambiar. Asimismo, este puede ser o no intencional, pero representa un riesgo para la organización y más aún ocasionar daños significativos en la reputación e incluso grandes pérdidas financieras (Cox, 2012; Son, 2011; Stanton, Stam, Mastrangelo, & Jolton, 2005).

Lo indicado hasta aquí sugiere que, los empleados representan la mayor amenaza en la seguridad de los sistemas de información (Pahnila, Siponen, & Mahmood, 2007b). Es por esto que, Chan, Woon, & Kankanhalli (2005), Dhillon (2001), Richardson (2008) y Steele & Wargo (2007), concuerdan que la mayor parte de estos incidentes ocurren por negligencia de los empleados.

Por otra parte, Bulgurcu, Cavusoglu, & Benbasat (2010a) apoyan el criterio de que las organizaciones que invierten tanto en la parte tecnológica como en estrategias socio-organizativas tienen mayores posibilidades de garantizar la SI. De acuerdo con Von Solms & Von Solms (2004), las PSI están entre los diez aspectos significativos para una gestión adecuada de la SI. Sin embargo, se ha identificado como principal problemática que la mayor parte de los empleados no cumplen con las mismas (Siponen, Pahnila, & Mahmood, 2010).

En relación a esta situación, las organizaciones enfrentan un gran desafío para garantizar el cumplimiento de las PSI por parte de los empleados. Considerando que estos últimos, son el eslabón más débil en la cadena de la SI (Al-Omari, Deokar, El-Gayar, Walters, & Aleassa, 2013; Bulgurcu et al., 2010a; Hu, Xu, Dinev, & Ling, 2011; Li, Zhang, & Sarathy, 2010; Son, 2011).

En este sentido, se han realizado varios estudios para comprender el cumplimiento de la política de seguridad por parte de los empleados (Puhakainen & Siponen, 2010; Siponen, Mahmood, & Pahnila, 2009; Siponen et al., 2010;

Warkentin & Willison, 2009). Teniendo en cuenta que, las decisiones del usuario final, con respecto a la seguridad, se pueden predecir (West, 2008).

En particular, Herath & Rao (2009b) sostienen que cuando la validación de los factores que intervienen en la intención de cumplimiento de las PSI, es independiente y no integral, sus resultados varían respectivamente.

En relación con los estudios realizados en Norteamérica, los autores Boss & Kirsch (2007), indican que, si entre las expectativas de la alta gerencia se encuentra el cumplimiento de las PSI, entonces aumenta la probabilidad de que los empleados adopten estas medidas de seguridad.

Por otra parte, Bulgurcu et al. (2010a) sugieren que se involucre a los empleados en la realización de las PSI, para que las mismas no representen un obstáculo en sus actividades laborales. Con respecto a otra investigación empírica de los mismos autores, concluyen que la claridad de las PSI influye positivamente en su cumplimiento (Bulgurcu, Cavusoglu, & Benbasat, 2010b).

Cox (2012), sostiene que las características narcisistas de los usuarios, no influyen significativamente en la actitud de comportamiento inseguro, en comparación con otros usuarios que no posean estas características.

Por lo que se refiere a los estudios realizados en Europa, los autores Pahnila, Siponen, & Mahmood (2007a), concuerdan que la calidad de las PSI tienen un impacto significativo en la intención de cumplimiento.

Myyry, Siponen, Pahnila, Vartiainen, & Vance (2009) resaltan que las personas que demuestran tener razonamiento moral preconvencional, esto es, aquellos que están convencidos que serán sancionados si no cumplen con las PSI, tienen una alta probabilidad de cumplir con las mismas.

Mientras tanto, Puhakainen & Siponen (2010) están convencidos que la capacitación, en relación con el cumplimiento de las PSI, debe utilizar métodos de entrenamiento que permitan el procesamiento cognitivo sistemático de la información y para lograrlo, la motivación es esencial.

Por otro lado, Siponen et al. (2010) señalan que la presión social de los compañeros de trabajo y superiores influye significativamente en la intención de cumplir con las políticas de seguridad.

A su vez, Pahnila, Karjalainen, & Siponen (2013) llevaron a cabo un análisis identificando dos grupos: (a) los que conocen las PSI y (b) los que no conocen las PSI. De donde resulta que, existen diferencias significativas entre los dos grupos. Por tanto, resaltan que los diferentes niveles de conocimiento representan diferentes niveles de cumplimiento.

Johnston, Warkentin, & Siponen (2015), sugieren que las sanciones tienen diversos hallazgos en la literatura. Por una parte, en su investigación, confirman un impacto significativo en la intención de cumplimiento de las PSI. Por otra, en el artículo de los autores Pahnila et al. (2007a) no se demuestra este impacto.

Prosiguiendo con el análisis, se evidencia poca literatura sobre esta temática en América Latina, sin embargo, se destacan dos estudios realizados en Brasil. En el primero, los autores Knorst, Vanti, Andrade, & Johann (2011) concuerdan que la mayor parte de los incidentes de seguridad, se debe al inadecuado comportamiento organizacional de los empleados. En relación al segundo, Klein & Luciano (2016) sugieren que la gravedad de la amenaza influye positivamente en el comportamiento de los empleados frente a los códigos maliciosos en correos electrónicos.

De manera puntual, en el primer estudio de Brasil, se propone un modelo para la alineación estratégica del comportamiento organizacional basada en la teoría de lógica difusa. Por otro lado, en el segundo, se evalúa un modelo basado en las teorías de comportamiento y la relación

entre sus determinantes es metodológicamente verificada mediante regresión lineal.

En los estudios tratados brevemente, se exponen varios factores relacionados al cumplimiento de las PSI basados en: (a) características propias de los empleados, (b) características de las PSI y programas de concientización y (c) características de la organización y cultura organizacional.

Con respecto a lo expuesto, en las revisiones sistemáticas sobre el cumplimiento o incumplimiento de las PSI, se evidencia que la mayoría de los autores se basan generalmente en: Teoría del Comportamiento Planificado (TPB, por sus siglas en inglés), para predecir el comportamiento de los empleados (Milicevic & Goeken, 2013; Njenga, 2016; Sommestad & Hallberg, 2013; Sommestad, Karlzén, & Hallberg, 2015). Por otro lado, en otra revisión sistemática se evidencian estudios en base a las siguientes teorías: (a) Teoría de la Disuasión (GDT, por sus siglas en inglés), (b) Teoría de la Motivación hacia la Protección (PMT, por sus siglas en inglés), (c) Modelo de Aceptación de Tecnología (TAM, por sus siglas en inglés), (d) Teoría de la Acción Razonada (TRA, por sus siglas en inglés), (e) Teoría del Comportamiento Planificado (TPB) y (f) Teoría de la moral (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014).

En definitiva, existen pocos trabajos que evidencien el análisis del compromiso organizacional, en particular, los relacionados a la intención de cumplimiento de las PSI. Los autores Njenga (2016) y Sommestad et al. (2014), concuerdan que la única publicación que analiza este determinante y esa relación, es el de los autores Herath & Rao (2009b).

Por ese motivo, el objetivo de la presente investigación es identificar los determinantes que contribuyen al cumplimiento de las políticas de seguridad con base en el comportamiento organizacional en el contexto ecuatoriano. Por lo cual, se adaptará el modelo propuesto por Herath & Rao (2009b), que permite evaluar desde una perspectiva integral los determinantes que influyen en el cumplimiento de las PSI, partiendo desde la premisa que los factores organizacionales, ambientales y de comportamiento influyen en su cumplimiento.

MARCO TEÓRICO

Para la presente investigación, se seleccionó un modelo que se basa en las teorías GDT, PMT, TPB, DTPB y OC, debido a que permite identificar de manera holística varios factores que la literatura sugiere que influyen en la intención de cumplimiento de la política de seguridad de la información (Herath & Rao, 2009b). En particular, en las instituciones públicas se enfatiza la importancia de que estos factores contribuyen a la gobernanza de la SI por la sensibilidad de la información, es decir, estas teorías y sus determinantes se ajustan más al tipo de empresa seleccionada en este estudio.

Políticas de seguridad

La política de seguridad es considerada una necesidad para las organizaciones y a la vez un recurso crítico (Amthor, Kühnhauser, & Pölck, 2014). Debido a que contribuye en la gestión de los sistemas de información (Baskerville & Siponen, 2002). En este sentido, estudios previos han realizado tópicos importantes sobre la política de seguridad (Baltatu, Lioy, & Mazzicchi, 2000; Schneider, 2000; Straub & Welke, 1998) y en establecer su definición (Flowerday & Tuyikeze, 2016). Cabe agregar que desde una perspectiva organizacional, uno de los roles de las PSI es prevenir el abuso informático (S. M. Lee, Lee, & Yoo, 2004).

Por otro lado, la norma ISO (2013) define la política de seguridad como un documento formal en que la alta gerencia de una organización establece las directrices a los empleados en relación a los objetivos y al contexto de la organización (Disterer, 2013). Por otra parte, Sandhu & Samarati (1994), agregan que una política es un control de acceso a los sistemas de información que está definida en relación al comportamiento de los empleados en determinados escenarios (Baltatu et al., 2000). A

su vez, este comportamiento definido como aceptable o inaceptable, comprende el uso e interacción con los activos de información (Alotaibi, Furnell, & Clarke, 2016).

Mientras tanto, Lee (2001) agrega que, una política de seguridad detalla los requisitos específicos o las reglas que deben cumplirse en el ámbito de la seguridad de red e información, las cuales deben cubrir un área única. También, en la política de seguridad se establecen las funciones y responsabilidades, así como las expectativas de comportamiento (De Lange, Von Solms, & Gerber, 2015). Por esto, es necesario que organizaciones posean políticas y procedimientos para la seguridad de su información, debido a que son tan importantes como las soluciones técnicas (Hina & Dominic, 2016).

GDT

Es una teoría jurídica la cual originalmente es aplicada en criminología u otros comportamientos antisociales (Fan & Zhang, 2011). Dado que es base para una extensa investigación en la justicia penal y ética debido a que la conducta humana es en cierto modo, racional y por lo tanto puede ser influenciada particularmente por incentivos negativos inherentes a su sanción (Sherman, 1993). Lo que indica que GDT, se basa en la imposición de un modelo normativo con énfasis en regulaciones que se adjudican a empleados a través de una amenaza de sanción, la cual ha sido aplicada exitosamente en los sistemas de información gubernamentales (Ugrin & Pearson, 2013).

Los autores Straub & Welke (1998), señalaron que la teoría de disuasión general, proporciona una base teórica para el uso de procedimientos determinados y medidas técnicas como un medio para limitar ciertas conductas de uso indebido de la información en organizaciones con la finalidad de convencer a posibles infractores que el riesgo de ser atrapado y severamente castigado es demasiado alto (L. Cheng, Li, Zhai, & Smyth, 2014).

Además hay que mencionar, que esta teoría GDT posee tres constructos, los cuales se los propone para influir sobre el comportamiento ilícito, estos son; (a) sanción formal e informal, (b) detección y (c) ejecución (D'Arcy & Herath, 2011). El primer constructo, la sanción se refiere a una persona quien cree que sus comportamientos serán severamente castigados, estas sanciones son efectivas en la medida en que son consideradas graves donde el castigo debe ser igual o mayor (Sodupe, 1991). En efecto las sanciones son importantes, por esta razón GDT menciona que el castigo debe ser inminente antes de que cause efecto; en el segundo constructo, se indica que la detección es la probabilidad de que sean capturados, aumentando la supervisión con ayuda del incremento de la detección (Williams & Hawkins, 1986).

Esto conlleva a que, los dos primeros constructos presten apoyo a la ejecución como un factor moderador en la teoría de disuasión, incluso con estos mecanismos de disuasión, aplicación activa y valores éticos, permiten que los empleados mantengan un rol importante en la efectividad y comportamiento, considerando que la SI es uno de los factores más importantes para toda organización (Lee et al., 2004).

PMT

Esta teoría fue introducida por primera vez por Rogers (1975). Desde entonces, varios estudios aplican este modelo para predecir y comprender particularmente el comportamiento relacionado con la salud (Chenoweth, Minch, & Gattiker, 2009). Cabe indicar que, el PMT se desarrolló en un intento por proporcionar claridad conceptual en el área del miedo de apelaciones y la investigación sobre el cambio de actitud (Milne, Sheeran, & Orbell, 2000). También, incorpora evaluaciones de amenazas, la efectividad percibida de una respuesta, la capacidad de un individuo para llevar a cabo esa respuesta y el análisis de costos en su diseño (Pechmann, Zhao, Goldberg, & Reibling, 2003).

Por esta razón, la presente teoría fue creada para determinar qué variables de estímulos aumentan el miedo en una persona y el proceso cognitivo

necesario para adoptar un comportamiento que lo protegerá del resultado (Rogers, 1975). En efecto esta teoría contiene cinco constructos principales: (a) la vulnerabilidad percibida; (b) la gravedad percibida; (c) la eficacia de respuesta; (d) autoeficacia y (e) el costo de respuesta, los cuales son los más significativos en el comportamiento de un individuo (Woon, Tan, & Low, 2005). También, en el modelo original, la influencia del miedo es un importante factor que influye en la iniciación de la selección del comportamiento individual por demás de ser una posible teoría para explicar las diferencias de comportamiento en materia de seguridad (Ifinedo, 2012).

TPB

La teoría fue propuesta por Ajzen (1985), siendo una extensión de la Teoría de la Acción Razonada (TAR) (Cheng, Tsai, Hung, & Chen, 2015). Asimismo, la teoría está respaldada por evidencia empírica, la que se basa en la intención y el control percibido del comportamiento para una predicción más acertada (Ajzen, 1991). De hecho, esta teoría indica que el comportamiento de una persona está determinado por su conducta (Ajzen, 2002).

Debido a la intención del empleado de cumplir con los requisitos, es utilizada adoptando los siguientes constructos principales: (a) actitud hacia el cumplimiento; es el grado en que se valora positivamente el rendimiento de comportamiento del cumplimiento; (b) creencias normativas; la presión social percibida de un empleado sobre el cumplimiento de los requisitos, causada por las expectativas de comportamiento de referentes tan importantes como ejecutivos, colegas y gerentes; (c) autoeficacia para el cumplimiento; es el juicio de un empleado sobre habilidades personales, conocimiento o competencia sobre el cumplimiento de los requisitos de la seguridad de la información y (d) intención de cumplir; es la intención de un empleado de proteger los recursos de información y tecnología de la organización contra posibles infracciones de seguridad (Bulgurcu et al., 2010a).

DTPB

En relación con la DTPB dirigida por Taylor & Todd (1995), se basa en la teoría de la conducta planificada (TPB) (Ramayah, Rouibah, Gopi, & Rangel, 2009). Hace un tiempo atrás, dicho modelo original mostraba limitaciones en relación a los comportamientos; lo que conlleva en las personas, a mantener un incompleto control voluntario lo cual significa que este modelo no demostraba claramente la relación entre el marco de creencias y la intención del comportamiento (Ndubisi, 2004). Esto se debe principalmente a que el marco de creencias se combinaba como conjuntos de creencias y podría no estar constantemente relacionados con la actitud (Bagozzi, 1981).

Así mismo, esta limitación contrarresta las influencias provocadas por creencias positivas y negativas, llevando a una relación insignificante entre los marcos y los antecedentes (Hung & Chang, 2005). De igual manera, Lin (2007) indica que para una mejor comprensión de las relaciones entre las estructuras de creencias y los antecedentes de la intención se requería una descomposición de las creencias actitudinales, argumentando que los componentes cognitivos de la creencia no podrían organizarse en una sola unidad conceptual o cognitiva (Ya-Yueh & Fang, 2004).

Por otro lado, DTPB para que se establezca una mejor perspectiva de la intención del comportamiento posee los principales constructos que se descomponen multidimensionalmente: (a) la actitud, (b) la norma subjetiva, (c) la ventaja relativa, (d) la complejidad, (e) la compatibilidad de la difusión de la teoría de la innovación y (f) el control de comportamiento (Taylor & Todd, 1995; Ya-Yueh & Fang, 2004). Estos determinan la intención del comportamiento y la realización de un comportamiento real (Hsieh, 2015). De manera que Taylor & Todd (1995) demostraron que el modelo descompuesto del DTPB tiene un mejor poder explicativo que los modelos originales TPB y TAR (Huang & Chuang, 2007).

OC

Es un concepto que tiene que ver con el grado de compromiso y lealtad que los empleados presentan hacia los empleadores (Wang, Keil, Oh, & Shen, 2017). Actualmente, OC es considerada cada vez más como una actitud vital que se relaciona con el trabajo de mejorar el vínculo psicológico del empleado con la organización, también involucra actitudes y comportamientos individuales en el lugar de trabajo (Xiang-Yang, Li-Ping, & Lau, 2008).

Por otra parte, el modelo OC identifica tres constructos: (a) compromiso afectivo, (b) compromiso continuo y (c) compromiso normativo (Allen & Meyer, 2000). En lo que concierne al compromiso afectivo, permite identificar el apego emocional positivo para la organización, el segundo es el compromiso continuo este hace referencia a la percepción de los altos costos asociados con el abandono de la organización, y finalmente el compromiso normativo es el sentido de obligación moral para con la organización (McMahon, 2007).

Por todo esto, en el ámbito del OC, existen varios niveles que pueden estar presentes en diversas combinaciones (Bartlett, 2001). Lo cual investiga el grado de apego emocional que siente un empleado de la compañía, a veces denominado compromiso afectivo, este componente del compromiso organizacional procura medir los sentimientos positivos que el empleado sienta para la organización y sus operaciones en general (Xiang-Yang et al., 2008). En efecto, esta teoría consiste en evaluar lo que motiva a los empleados a permanecer con los empleadores (Steers, 1977). Tomar el tiempo para entender la naturaleza de estos promotores y hasta qué grado se encuentran dentro de un determinado lugar, a menudo puede ayudar a reducir la cantidad de rotación de los empleados, proporcionando información sobre cómo realizar cambios en la cultura corporativa que permiten que los empleados se sientan involucrados en el negocio (Meyer, Stanley, Herscovitch, & Topolnytsky, 2002).

En el contexto de la Seguridad de la Información, el compromiso organizacional es el grado en que un empleado se identifica con la organización mediante un comportamiento seguro debido a que considera que su comportamiento influye en el logro de la seguridad de la información de toda la organización (Herath & Rao, 2009b).

Hipótesis de la investigación

La intención de la presente investigación es replicar completamente el modelo propuesto por los autores Herath & Rao (2009b), por lo que las hipótesis desarrolladas en la propuesta original incluyen las siguientes:

TPB, DTPB, PMT

H1: Las actitudes hacia las políticas de seguridad de la información influirán positivamente en las intenciones de cumplimiento de la política de seguridad.

GDT

H2: La severidad percibida sobre violación a la seguridad afectará positivamente el nivel de preocupación sobre violación a la seguridad.

PMT

H3: La probabilidad percibida de violación a la seguridad afectará positivamente el nivel de preocupación sobre violación a la seguridad.

H4: Los niveles más altos de preocupación por la violación a la seguridad darán como resultado actitudes más positivas hacia las políticas de seguridad.

H5: La efectividad percibida de las propias acciones afectará positivamente la actitud hacia las políticas de seguridad.

H6: El costo de respuesta percibido influirá negativamente en la actitud hacia las políticas de seguridad.

TPB; DTPB; PMT

H7: La auto-eficacia influirá positivamente en la actitud hacia las políticas de seguridad.

H8: La auto-eficacia afectará positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.

DTPB

H9: La disponibilidad de recursos afectará positivamente la autoeficacia.

GDT

H10: La severidad del castigo afectará positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.

H11: La certeza en la detección afectará positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.

TPB; DTPB

H12: Las normas subjetivas [expectativas de los demás] afectarán positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.

H13: Las normas descriptivas [comportamiento de otros similares] influirán positivamente en las intenciones de cumplir con las políticas de seguridad.

OC

H14: Los niveles más altos de compromiso organizacional llevarán a una mayor percepción de los empleados sobre la efectividad de sus acciones.

H15: El nivel de compromiso organizacional afectará positivamente las intenciones de seguir las políticas de seguridad.

METODOLOGÍA

En la presente investigación el enfoque metodológico es cuantitativo. Debido a que, se trata de determinar el nivel de asociación entre los determinantes estudiados mediante la técnica de análisis de ruta, lo cual permite realizar una inferencia causal de estas relaciones (Barchini, 2005). A continuación, se detalla la metodología utilizada en la presente investigación.

Participantes

Los participantes del presente estudio fueron seleccionados de una Institución pública del Ecuador, cuya muestra fue no probabilística. Como resultado, la tasa de respuesta fue del 78% y se tuvieron 592 respuestas válidas de 756 encuestas. Teniendo en consideración que la cantidad de empleados se encuentran en el rango de 1000 o más, que en comparación con la propuesta original se encuentra representado en un 25% de las organizaciones participantes.

En relación a los datos demográficos, el rango de edad de los participantes fue desde 20 hasta igual o mayores a 60 años, con mayor proporción entre 30 y 39 años, comprendido en un 47%. Por otra parte, el cargo de los participantes fue diverso incluyendo personal de TI y otros cargos, representado en un 92% este último. Acerca del género, el 51% de los participantes fueron mujeres y 49% fueron hombres. A su vez, el nivel de educación máximo alcanzado por los participantes, en mayor proporción fue “Educación universitaria completa”, mostrado en un 64%. Los detalles demográficos de la muestra se encuentran en la Tabla A1.

Instrumento

El instrumento consta de 43 ítems y se evalúan 14 constructos que se basan en 5 teorías como:

PMT, TPB, DTPB, GDT y OC. En este sentido, permite evaluar los determinantes organizacionales como compromiso organizacional, ambientales como efectos de disuasión, condiciones facilitadoras e influencia social; y de comportamiento como evaluación de la amenaza y eficacia de la respuesta para identificar la actitud frente a la política de seguridad que influyen en el cumplimiento de las PSI. En particular, los ítems fueron evaluados mediante una escala de Likert de 7 niveles (Totalmente en desacuerdo–Totalmente de acuerdo).

En relación al método usado para medir la consistencia interna y confiabilidad del instrumento, fue el alfa de Cronbach. De acuerdo con los autores Huh, DeLorme, & Reid (2006), para los estudios exploratorios como la presente investigación, la consistencia interna debe ser mayor o igual a 0.60. En este sentido, el coeficiente de alfa de Cronbach del instrumento es α = 0.89. A su vez, el de los constructos evaluados, se muestran en la Tabla 1.

Procedimiento

Se solicitó la autorización para la adaptación del modelo propuesto por los autores Herath & Rao (2009b) mediante correo electrónico. En este sentido, el investigador principal autorizó el uso de su modelo en el presente estudio.

Por otro lado, la adaptación del instrumento del paper original, se basa en lo expuesto por los autores Muñiz, Elosua, & Hambleton (2013). Asimismo, la validez de contenido de instrumento fue mediante el juicio de expertos, que se basa en lo sugerido por los autores Escobar-Pérez & Cuervo-Martínez (2008).

En general, los jueces expertos mostraron un nivel significativo de concordancia en las categorías evaluadas: (a) suficiencia (rGW = 0.8), (b) claridad (rGW = 0.8), (c) coherencia (rGW =0.9) y (d) relevancia (rWG = 0.7). De manera puntual, en esta última categoría, algunos de los ítems fueron evaluados como no relevantes. En este sentido, de acuerdo al criterio de los jueces expertos, se resaltan los constructos mayormente afectados como no relevantes: (a) probabilidad percibida de violación a la seguridad, (b) actitud frente a la política de seguridad y (c) norma descriptiva.

Asimismo, después de obtener los resultados del juicio de expertos, se procedió a realizar algunas mejoras al instrumento, conservando la claridad semántica del mismo y su relación con el constructo teórico. Por lo que, se realizó la revisión de cada ítem de la escala, discutiendo cada uno de los términos utilizados en su formulación inicial.

A continuación, se especifican los constructos que fueron parafraseados: (a) probabilidad percibida de violación a la seguridad, (b) severidad percibida de violación a la seguridad,

Tabla 1
Datos estadísticos de fiabilidad

Constructo	Número Ítems	Alfa de Cronbach
probabilidad percibida de violación a la seguridad	3	0.75
severidad percibida sobre violación a la seguridad	3	0.76
nivel de preocupación sobre violación a la seguridad	3	0.64
eficacia de la respuesta	3	0.66
costo de respuesta	1	n/a
disponibilidad del recurso	5	0.80
auto-eficacia	3	0.64
actitud frente a la política de seguridad	3	0.97
compromiso organizacional	3	0.66
severidad del castigo	3	0.78
certeza en la detección	2	0.74
norma subjetiva	5	0.92
norma descriptiva	3	0.89
intención de cumplimiento de la política de seguridad	3	0.80

(c) nivel de preocupación sobre violación a la seguridad, (d) costo de respuesta, (e) severidad del castigo y (f) certeza en la detección. Asimismo, se aclara que no se agregaron o eliminaron constructos al instrumento.

En relación con la ejecución del instrumento, se socializó el tema de investigación con directivos y jefes departamentales de la Institución, con la finalidad de motivar la participación de los empleados en este estudio. Debido al tipo de investigación y con el objetivo de garantizar la confidencialidad de la información, se solicitó el permiso a la alta gerencia de la institución, para llevar a cabo el levantamiento de información en la misma. En este sentido, previo a la ejecución del instrumento, se firmó un acuerdo de confidencialidad entre las partes involucradas.

Por lo tanto, los participantes fueron contactados por correo electrónico para que llenen la encuesta (a través de Formularios de Google), la misma que fue enviada a sus cuentas institucionales, a nivel nacional, considerando todos los cargos y dependencias. En definitiva, participaron los empleados que usan computadores y recursos de la Institución como el servicio de Internet y correo electrónico. De modo que se garantiza la diversidad en la recolección de los datos. Se debe agregar que la encuesta estuvo habilitada en el periodo de dos semanas.

En relación con la sensibilidad y la anonimidad en el levantamiento de la información, se tomaron en cuenta controles preventivos para que las respuestas dadas sean honestas, veraces y lo más cercano a la realidad institucional. Así, por ejemplo, la encuesta fue realizada mediante un formulario web y los datos no procesados recopilados estaban únicamente disponibles para uno de los investigadores. Además, no se solicitó información personal como nombres, apellidos o cédula de identidad y se informó a los participantes que la encuesta era anónima y que la recolección de los datos era con fines investigativos.

Asimismo, para garantizar la confiabilidad, se consideró una pregunta de atención, que fue usada para medir el nivel de atención de los participantes y que indicaba lo siguiente: “Soy una persona que no sabe lo que habla”, por lo que si el participante evaluaba este ítem en la escala del 2 al 7, este ítem se consideraba como no válido, es decir, fueron descartados 22% de los datos que no cumplieron con este criterio. También, se consideró agregar algunas definiciones para que se apliquen los términos de forma correcta y disminuir las malas interpretaciones que podrían darse al tener una diversidad de perfiles de los participantes.

ANÁLISIS DE RESULTADOS

Los datos fueron analizados usando el software estadístico SPSS versión 23.0, mediante el análisis de ruta. Para Klem (1998), el diagrama de ruta es una declaración resumida del conjunto de hipótesis que ocupan al investigador. A través de este diseño se pudo calcular las influencias directas e indirectas de los constructos investigados como la probabilidad percibida de violación a la seguridad, severidad percibida sobre violación a la seguridad, nivel de preocupación sobre violación a la seguridad, eficacia de la respuesta, costo de respuesta, disponibilidad del recurso, auto-eficacia, actitud frente a la política de seguridad, compromiso organizacional, severidad del castigo, certeza en la detección, norma subjetiva, norma descriptiva e intención de cumplimiento de la política de seguridad.

Resultados

Los resultados y su relación con otros determinantes se muestran en la Figura 1. En definitiva, las relaciones son estadísticamente significativas ($p<0.05$), a excepción de la relación entre los determinantes costo de respuesta con la actitud frente a la política de seguridad. En particular, los coeficientes de β son significativos para el determinante nivel de preocupación sobre violación a la seguridad ($\beta=0.524$; $\beta=0.370$; $p<0.05$). En relación al determinante actitud

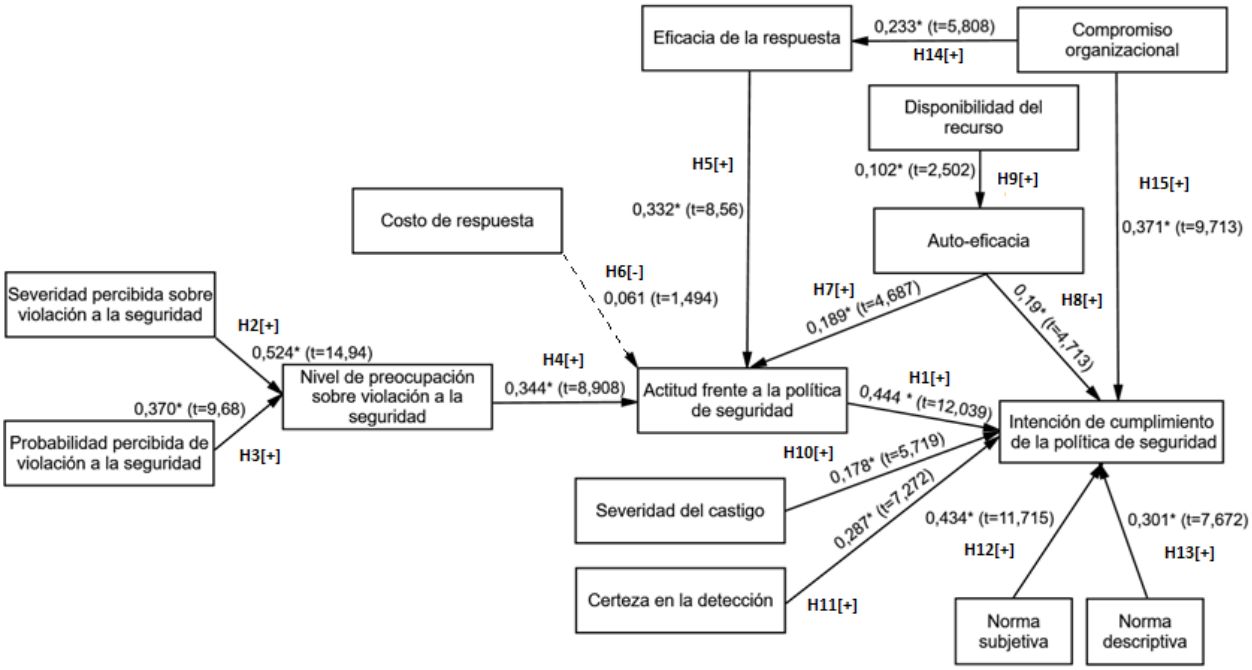

Figura 1 Resultados de la adaptación del modelo.
*Nota: * significativo en nivel p<0.05*

frente a la política de seguridad tiene un impacto significativo (β=0.344; β=0.332; β=0.189; p<0.05), a excepción del determinante costo de respuesta que no influye significativamente (β = 0.061). En este mismo sentido, la eficacia de respuesta es significativa (β=0.233; p<0.05) como la autoeficacia (β=0.102; p<0.05).

Por otra parte, el determinante intención de cumplimiento de la política de seguridad tiene un efecto significativo en el presente estudio (β=0.444; β=0.178; β=0.287; β=0.434; β=0.301; β = 0.371; β = 0.19; p<0.05).

En consecuencia, los resultados del modelo indican que se cumplen todas las hipótesis a excepción de la hipótesis 6 (Tabla A3). Asimismo, los estadísticos descriptivos de las variables del modelo se encuentran en la Tabla A2.

Los resultados del presente estudio muestran que comprender la severidad de la amenaza afecta significativamente el nivel de preocupación sobre violación a la seguridad. Este hallazgo, es similar al de la propuesta original. A su vez, es consistente con estudios previos. Dado que, otros autores encontraron que la severidad percibida influye significativamente en la intención de cumplimiento de las políticas de seguridad (Pahnila et al., 2013; Vance, Siponen, & Pahnila, 2012; Workman, Bommer, & Straub, 2008).

Asimismo, la probabilidad percibida de violación a la seguridad tiene un impacto significativo en el nivel de preocupación sobre violación a la seguridad. En contraste con la propuesta original, que no es significativo. Por otro lado, Vance et al. (2012) estudiaron este mismo determinante, en relación a la intención de cumplimiento de la política de seguridad, pero sus resultados indican que no tiene impacto significativo. Sin embargo, en otros estudios previos se confirma esta relación (Pahnila et al., 2013; Workman et al., 2008).

A su vez, nuestros resultados exponen que los empleados que tengan mayor nivel de preocupación sobre violaciones a la seguridad,

tendrán actitudes más positivas hacia las políticas de seguridad, coincidiendo con los resultados de la propuesta original. En relación a estudios previos, Pahnila et al. (2007a) también soporta la misma relación. Por otro lado, se ha evidenciado que la evaluación de la amenaza o nivel de preocupación sobre violaciones a la seguridad influye significativamente en la intención de cumplimiento de las PSI (Pahnila, Siponen, & Mahmood, 2007b; Siponen et al., 2014, 2010).

De forma sorpresiva, los resultados de este estudio sugieren que, aun cuando los empleados crean que cumplir con las políticas de seguridad represente un obstáculo en su rutina laboral, ellos tendrán perspectivas favorables hacia la política de seguridad. Es decir, el costo de respuesta no influye negativamente en la actitud frente a la política de seguridad. En relación a estudios previos, nuestros resultados concuerdan con el de los autores Pahnila et al. (2007a). Por el contrario, Bulgurcu et al. (2010a) soportan un impacto negativo del determinante como en la propuesta original. A su vez, Vance et al. (2012) sostienen que el costo de respuesta influye negativamente en la intención de cumplimiento de las PSI.

Con respecto al determinante eficacia de respuesta, Herath & Rao (2009b) destacan que los empleados que creen que su comportamiento impacta positivamente a la organización, es más probable que tengan actitudes más positivas hacia las políticas de seguridad. En consecuencia, en el presente estudio se evidencia que la eficacia de respuesta, tiene un impacto significativo en la actitud hacia la política de seguridad, al igual que en la propuesta original. Por otro lado, en relación a otros estudios, la eficacia de respuesta también influye significativamente en la intención de cumplimiento de la política de seguridad (Johnston et al., 2015; Pahnila et al., 2013; Siponen et al., 2014; Vance et al., 2012; Workman et al., 2008). Sin embargo, Pahnila et al. (2007b) y Siponen et al. (2010) muestran en sus estudios que esta misma relación no tuvo un impacto significativo.

En cuanto a la disponibilidad del recurso, en nuestro estudio como en la propuesta original, se encontró un impacto significativo en la auto-eficacia. De igual modo, este hallazgo coincide con el estudio de Pahnila et al. (2007a). Lo cual sugiere que si los empleados tienen acceso a recursos facilitadores desarrollan mayor su habilidad para desempeñar acciones seguras. Por otro lado, se ha evidenciado que este determinante ha sido ampliamente estudiado en relación a la actitud para cumplir con las PSI, efectividad de seguridad percibida, cultura de seguridad, intención de incumplimiento de la SI y en particular en la intención de cumplimiento de la política de seguridad del uso de internet (D'Arcy & Hovav, 2007; Li, Zhang, & Sarathy, 2009; Pahnila et al., 2007a). En relación con la intención de auto-defensa, no tiene impacto (Lee et al., 2004).

Asimismo, nuestros resultados como los de la propuesta original, demuestran que la auto-eficacia tiene un impacto significativo tanto en la actitud hacia la política de seguridad como en la intención de cumplimiento de las PSI. En particular, en un estudio previo se confirma que la autoeficacia no tiene un impacto significativo en la actitud frente a la política de seguridad (Al-Omari et al., 2013). Sin embargo, en la intención de cumplimiento de las PSI tiene impacto (Al-Omari et al., 2013; Al-Omari, El-Gayar, & Deokar, 2012; Bulgurcu et al., 2010a; Johnston et al., 2015; Pahnila et al., 2007b; Siponen et al., 2014, 2010; Vance et al., 2012). Aunque, Pahnila et al. (2013) no concuerdan con ese hallazgo.

Por lo tanto, la literatura propone la implementación de programas de concientización debido a que aportan significativamente a la auto-eficacia (D'Arcy & Hovav, 2007) y en consecuencia, en el cumplimiento de la política de seguridad (Li et al., 2010). En contraste con Lee et al. (2004), quienes sostienen que los programas de concientización no influyen en la auto-eficacia. Este resultado puede deberse, a que este recurso, por sí solo no aporta al cumplimiento de las políticas de seguridad, se deben de tener en cuenta otros recursos facilitadores para que los

empleados puedan tomar acciones seguras como en el presente análisis. Por otra parte, en un estudio de Latinoamérica mostró que la mayor parte de los empleados de un banco leerían las políticas de seguridad si perciben que la alta gerencia monitorea su comportamiento ante las mismas (Allassani, 2014). Esto plantea, que el involucramiento de la alta gerencia es importante para disuadir y desarrollar la auto-eficacia.

Por lo que se refiere a la actitud frente a la política de seguridad, nuestros resultados sostienen que la misma tiene un impacto significativo en la intención de cumplimiento. Asimismo, en comparación con estudios previos nuestros resultados coinciden con los autores Al-Omari et al. (2013), Al-Omari, El-Gayar, & Deokar (2012), Bulgurcu et al. (2010a), Li et al. (2010), Ng & Rahim (2005) y Pahnila et al. (2007a). Inclusive, en un estudio relacionado al cumplimiento de la política de seguridad del uso de internet, el impacto también fue significativo (Li et al., 2010). En contraste con la propuesta original, que no evidencia impacto.

Además, los hallazgos del presente estudio como los de la propuesta original, muestran que la influencia social tiene un impacto significativo en la intención de cumplimiento. Por esto, las normas subjetivas, que se basan en las expectativas de la alta dirección, jefes, colegas, departamento de Seguridad Informática y otros expertos en esta rama, influyen en el comportamiento de los empleados. Esto, también sugiere que los empleados conocen las expectativas de los mismos. Por otro lado, las normas descriptivas sostienen que el propio comportamiento se basa en el de los demás, también influyen en la intención de cumplimiento de las políticas de seguridad. Esto es un importante hallazgo y reafirma lo indicado en la literatura, que el respaldo de la alta dirección es vital para asegurar su cumplimiento (Puhakainen & Siponen, 2010).

Se debe agregar que, en un estudio de Latinoamérica se evidencia que la influencia social como las normas subjetivas, entre entidades públicas de investigación, influye también en la adopción de prácticas de seguridad de la información (de Albuquerque & dos Santos, 2015).

Acerca de las implicaciones de la teoría de la disuasión, hay dos características relevantes de la sanción que contribuyen a su efectividad como la certeza de la detección y la severidad del castigo (Blumstein, 1978), las mismas que en el presente estudio, influyen significativamente en la intención de cumplimiento de las políticas de seguridad. Esto sugiere, que si los empleados creen que hay una alta probabilidad de que sean descubiertos si violan las políticas de seguridad, ellos con certeza las cumplirían. En ese mismo sentido, si la severidad del castigo es percibida como alta, en consecuencia, aumenta el cumplimiento de la política de seguridad.

Por el contrario, en la propuesta original solamente la certeza de la detección tiene un impacto significativo en la intención de cumplimiento de la política de seguridad, debido a que la severidad del castigo no la tiene. En la literatura, se evidencian diversos resultados sobre las sanciones. Así, por ejemplo, algunos autores sostienen que la certeza en la detección influye positivamente en la intención de cumplimiento de las políticas de seguridad (Herath & Rao, 2009a; Li et al., 2009, 2010). Sin embargo, otros estudios no concuerdan (Hu et al., 2011; Son, 2011). Asimismo, con la severidad del castigo, que algunos autores coinciden en que no influye en la intención de cumplimiento de la política de seguridad (Herath & Rao, 2009a; Son, 2011). En particular, en estudios relacionados a la política de seguridad del uso de internet, la severidad percibida tampoco tuvo un impacto significativo (Li et al., 2010), pero en otro estudio, sobre la severidad percibida y la actitud hacia la política de seguridad, se sustenta un impacto significativo (Dugo, 2007). Además, en un estudio de Latinoamérica relacionado a códigos maliciosos en correos electrónicos, se evidencia una relación no significativa del determinante con el comportamiento seguro (Klein & Luciano, 2016).

Finalmente, nuestros hallazgos confirman que el compromiso organizacional influye significativamente en la eficacia de respuesta como en la intención de cumplimiento de la política de seguridad. Estos resultados concuerdan con los de la propuesta original. Por otro lado, Dugo (2007) y Stanton, Stam, Guzman, & Caldera, (2003), sostienen que mientras mayor sea el compromiso organizacional es menos probable que los empleados tengan comportamientos inseguros o contraproducentes.

En definitiva, los resultados de nuestro estudio ofrecen importantes implicaciones prácticas para el personal de Seguridad Informática. Por lo cual, se deben de considerar todos los determinantes evaluados debido a que de manera general influyen en el cumplimiento de las políticas de seguridad. Por mencionar, el determinante disponibilidad del recurso puede ser explotado garantizando la disponibilidad y facilidad del acceso a los recursos como la mesa de servicios, políticas de seguridad y programas de concientización. También, garantizar la calidad de las mismas, debido a que usualmente los empleados cumplirán con aquellas políticas de seguridad que sean claras (Ammann & Sowa, 2013). Asimismo, en relación a las sanciones por incumplimiento, estas deben ser transmitidas y conocidas por los empleados. Por ejemplo, a través de mensajes de correo electrónico, boletines internos, afiches, entre otros. En las Tablas A4 y A5 se muestra un resumen de los hallazgos encontrados, en comparación con la propuesta original y estudios previos respectivamente.

CONCLUSIONES

La técnica estadística utilizada fue análisis de ruta, debido a esto, los resultados deben ser tomados con precaución porque la técnica no permite confirmar la teoría. Sin embargo, la técnica es relevante porque permite un diagnóstico de asociación de constructos, es decir, la exploración de los constructos que están relacionados directamente. Considerando que, no se han realizado investigaciones en este contexto sobre esta temática, es importante primero realizar este tipo de diagnóstico.

En definitiva, se evidencian escasos estudios sobre esta temática en Latinoamérica y ninguno en el contexto ecuatoriano. En consecuencia, la ejecución de este estudio contribuye al contexto organizacional mediante la adaptación del modelo propuesto por los autores Herath & Rao (2009b), que de acuerdo a la revisión en la literatura proveen un modelo robusto e integral que permite identificar los determinantes que contribuyen al cumplimiento de las PSI.

En relación con los hallazgos encontrados, basados en 592 resultados de una muestra representativa, se evidencia que se contraponen con la propuesta original, los determinantes: (a) probabilidad percibida de violación a la seguridad, (b) actitud frente a la política de seguridad, (c) severidad del castigo y (d) costo de respuesta. Dado que, en la presente investigación, los tres primeros son significativos y como no significativo el costo de respuesta.

Con respecto al literal a, en el presente estudio, se demuestra que la evaluación de la amenaza es significativa, comprendida por la severidad y probabilidad percibida de violación a la seguridad, lo cual aumenta el nivel de preocupación sobre violación a la seguridad. El hallazgo es consistente con PMT (Rogers, 1975). Por el contrario, en la propuesta original, se evidencia que las percepciones de los empleados de que ocurra una amenaza son bajas. En este sentido, la literatura sugiere que esta situación aumenta el incumplimiento de las PSI (Pahnila et al., 2007a).

De donde se infiere que, los resultados de las muestras de ambos estudios se contraponen por diferencias entre el nivel de concientización sobre las amenazas de SI (Workman et al., 2008). También, puede deberse a que en el presente estudio, los empleados relacionan el cumplimiento de las PSI con evitar amenazas de seguridad (Vance et al., 2012). Esto requiere investigación adicional para determinar con mayor precisión este hallazgo, como la

incorporación de determinantes como el hábito, que Vance et al. (2012) han incorporado en su estudio y que contribuyen a la evaluación de la amenaza significativamente. Asimismo, para garantizar que el determinante continúe contribuyendo significativamente, el personal de seguridad informática debe concientizar a los empleados sobre esta temática mediante correos electrónicos, capacitaciones, afiches boletines internos (Li et al., 2009; Pahnila et al., 2007a). En este sentido, Workman et al., (2008) sugiere que la capacitación puede ser basada en la experiencia de usuarios que hayan presentado amenazas de seguridad, lo cual podría incrementar el nivel de percepción de evaluación de la amenaza. Asimismo, el involucramiento de la alta gerencia es clave para comunicar oportunamente sobre las amenazas que se encuentra expuesta la organización y las consecuencias que podría ocasionar su materialización (Siponen et al., 2009).

En cuanto a los literales b y c, se demuestra que las intenciones de cumplir con las PSI están influenciadas por la actitud frente a la política de seguridad y severidad del castigo, entre otros. En particular, nuestro resultado es consistente con las teorías TPB (Ajzen, 1991) y GDT respectivamente (Straub, 1990). Sin embargo, en la propuesta original no influyen los dos determinantes mencionados. En relación a la divergencia de los resultados sobre la actitud, es probable que esta situación se deba a diferencias en la cultura organizacional, dado que, tiene un alto impacto en la seguridad de la información (Vroom & Von Solms, 2004). Lo cual sugiere, que en el presente estudio, los empleados perciben una cultura de seguridad respaldada por la alta gerencia.

Como trabajos futuros, se sugiere incorporar al modelo, la Teoría de la ética, la cual puede contribuir a predecir el comportamiento organizacional, debido a que la decisión, entre cumplir o violar las PSI puede conllevar un conflicto ético (Al-Omari et al., 2013). Asimismo, se ha evidenciado que la concientización de la tecnología, que se define como la auto-concientización e interés por conocer problemas tecnológicos y sus soluciones por sí mismo mediante diferentes recursos como el Internet, influye positivamente en la actitud para cumplir con las PSI, por lo cual, se sugiere que puede contribuir al modelo y en efecto determinar con mayor precisión porque los resultados de ambos estudios se contraponen (Al-Omari et al., 2012). Ambas sugerencias están basadas en características del empleado que no son utilizadas en el modelo para predecir la actitud frente a la PSI.

En relación a trabajos futuros sobre el determinante severidad del castigo, puede ser incorporado al modelo, la celeridad de una sanción, que es la rapidez con la que un empleado será sancionado por no cumplir con las PSI (Hu et al., 2011). Asimismo, las normas personales basada en Rational Choice Theory (RCT), que se define como la moral del empleado. Debido a que, en estudios previos se evidencia una influencia moderadora sobre la intención de cumplir con políticas de seguridad de Internet (Li et al., 2010).

Por lo que se refiere al literal d, en la presente investigación, el costo de respuesta no influye negativamente en la actitud frente a la política de seguridad. En cambio, en la propuesta original influye. De manera puntual, el proceso de evaluación de afrontamiento de una amenaza, está dada por el costo de respuesta, eficacia de respuesta y autoeficacia (Rogers, 1983). En este sentido, el presente estudio evidencia que los determinantes mencionados contribuyen positivamente en la actitud frente a la política de seguridad. En particular, el hallazgo del costo de respuesta, puede deberse a que las medidas de seguridad implementadas son percibidas como transparentes para el usuario (Woon et al., 2005), por lo cual, no representan obstáculos en su rutina laboral. Precisamente, para que el determinante no influya negativamente, se sugiere que las organizaciones incluyan el tiempo que involucra aplicar las medidas de seguridad, a los tiempos asignados a las tareas laborales y capaciten a los empleados para que se reduzca la percepción negativa de aplicar las PSI (Bulgurcu et al., 2010a). De acuerdo al juicio

de expertos para validación de contenido del instrumento, se recomienda agregar más ítems para evaluar el determinante para concluir con mayor precisión su contribución como en otros estudios (Vance et al., 2012; Workman et al., 2008).

En lo que respecta a las limitaciones de este estudio y que establecen oportunidades para trabajos futuros, se menciona la normativa del contexto de la organización seleccionada, porque el acceso a la información de tipo confidencial es restringido. Dado que, el sector gubernamental prioriza la Seguridad de la Información. Por tanto, el tiempo relacionado con la firma del acuerdo de confidencialidad ocasionó demora en la ejecución del estudio.

Indiscutiblemente, en comparación con la propuesta original, se evidencia una diferencia por la diversidad de empresas incluidas. Sin embargo, la muestra obtenida en nuestro estudio es representativa, por lo que, se garantiza la diversidad de participantes y perfiles. Además, se enfatiza que el número de empleados de la organización de este estudio se encuentra en el rango de 1000 empleados o más. De modo que, en comparación con la propuesta original, este rango está solamente comprendido en un 25% de organizaciones participantes.

Los resultados del presente estudio también hacen una importante contribución a la auditoría de tecnologías de la información, que entre sus buenas prácticas, se sugiere verificar el cumplimiento de las PSI mediante la madurez de los controles implementados en una organización, debido a que si son débiles, aumentan la probabilidad de una violación a la seguridad. A su vez, confirmar que los mismos no representen obstáculos o por el contrario, que sean muy permisivos. Dado que, la literatura sugiere que ambos extremos no son eficientes. Por una parte, pueden provocar desmotivación. Por otra, aumentar la probabilidad de incumplimiento de las PSI (Gelbstein, 2017). Considerando que, entre los elementos que la auditoría no contempla eficazmente, es el comportamiento de los empleados, que es relevante en la SI (Vroom & Von Solms, 2004), se sugieren métodos alternativos como la presente investigación para auditar el comportamiento de los empleados.

Finalmente, como trabajos futuros se sugiere ejecutar el instrumento en otro tipo de organizaciones y países de Latinoamérica con el objetivo de evaluar nuestros resultados en el contexto y confirmar su similitud. Asimismo, en el análisis considerar las variables de control como edad, género, cargo, entre otros; para evidenciar su influencia en la intención de cumplimiento de las PSI.

Referencias Bibliográficas

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11–39). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I. (2002). Perceived behavioral control, self- efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683. https://doi.org/https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. In IEEE (Ed.), *2013 46th Hawaii International Conference on System Sciences* (pp. 3018–3027). Wailea, HI, USA. https://doi.org/10.1109/HICSS.2013.272

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information Security Policy Compliance: The Role of Information Security Awareness. In *Proceedings of the 18th Americas Conference on Information Systems (AMCIS '12)* (pp. 1–10).

Allassani, W. (2014). Determining factors

determinants of bank employees' reading habits of information security policies. *Journal of Information Systems and Technology Management*, *11*(3), 533–548. https://doi.org/10.4301/S1807-17752014000300002

Allen, N. J., & Meyer, J. P. (2000). Construct validation in organizational behavior research: The case of organizational commitment. In R. . Goffin & E. Helmes (Eds.), *Problems and Solutions in Human Assessment: Honoring Douglas N. Jackson at Seventy* (pp. 285–314). Kluwer, Norwell, MA: Springer.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 352–358). IEEE. https://doi.org/https://doi.org/10.1109/ICITST.2016.7856729

Ammann, F., & Sowa, A. (2013). Readability as Lever for Employees' Compliance With Information Security Policies. *ISACA Journal*, *4*, 1–4. Retrieved from http://www.isaca.org/Journal/archives/2013/Volume-4/Documents/13v4-Readability-as-Lever.pdf

Amthor, P., Kühnhauser, W. E., & Pölck, A. (2014). WorSE: a workbench for model-based security engineering. *Computers & Security*, *42*, 40–55.

Bagozzi, R. P. (1981). Attitudes, intentions, and behavior: A test of some key hypotheses. *Journal of Personality and Social Psychology*, *41*(4), 607–627. https://doi.org/https://doi.org/10.1037/0022-3514.41.4.607

Baltatu, M., Lioy, A., & Mazzicchi, D. (2000). Security policy system: status and perspective. In *Networks, 2000.(ICON 2000). Proceedings. IEEE International Conference on* (pp. 278–284). IEEE.

Barchini, G. E. (2005). Métodos "I + D" de la Informática. *Revista de Informática Educativa Y Medios Audiovisuales*, *2*(5), 16–24.

Bartlett, K. R. (2001). The relationship between training and organizational commitment: A study in the health care field. *Human Resource Development Quarterly*, *12*(4), 335. https://doi.org/10.1002/hrdq.1001

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337–346.

Blumstein, A. (1978). Introduction. In A. Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

Boss, S. R., & Kirsch, L. J. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. In *Proceedings of the 28th International Conference on Information Systems* (pp. 1–18). Montreal.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010a). 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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010b). Quality and Fairness of an Information Security Policy As Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1–7). Honolulu, HI, USA: IEEE. https://doi.org/10.1109/HICSS.2010.312

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, *1*(3), 18–41. https://doi.org/10.1080/15536548.2005.10855772

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human*

Behavior, *38*, 220–228.

Cheng, M.-J., Tsai, H.-H., Hung, S.-W., & Chen, P.-W. (2015). Exploring the adoption intentions through decomposed theory of planned behavior: An empirical study on mobile applications. In *2015 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 1461–1466). Portland: IEEE. https://doi.org/10.1109/PICMET.2015.7273216

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS* (pp. 1–10). IEEE. https://doi.org/https://doi.org/10.1109/HICSS.2009.74

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, *50*(10), 113–117. https://doi.org/10.1145/1290958.1290971

de Albuquerque Junior, A. E., & dos Santos, E. M. (2015). Adoption of Information Security Measures in Public Research Institutes. *Journal of Information Systems and Technology Management*, *12*(2), 289–315. https://doi.org/10.4301/S1807-17752015000200006

De Lange, J., Von Solms, R., & Gerber, M. (2015). Better information security management in municipalities. In *IST-Africa Conference, 2015* (pp. 1–10). IEEE.

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 Latinoamérica*. Perú. 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. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and Security*, *20*(2), 165–172. https://doi.org/10.1016/S0167-4048(01)00209-7

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 92–100. https://doi.org/https://doi.org/10.4236/jis.2013.42011

Dugo, T. M. (2007). *The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test*. *Methodology*. Retrieved from http://media.proquest.com.login.capitol-college.edu:2048/media/pq/classic/doc/1475173961/fmt/ai/rep/NPDF?hl=securities,security,cultures,culture&cit:auth=Dugo,+Todd+Michael&cit:title=The+insider+threat+to+organizational+information+security:+A+structural+

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez De Contenido Y Juicio De Expertos: Una Aproximación a Su Utilización. *Avances En Medición*, *6*, 27–36.

ESET. (2017). Eset Security Report Latinoamérica 2017. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Fan, J., & Zhang, P. (2011). Study on E-government information misuse based on General Deterrence Theory. In *8th International Conference on Service Systems and Service Management - Proceedings of ICSSSM'11*. https://doi.org/10.1109/ICSSSM.2011.5959454

Flowerday, S. V, & Tuyikeze, T. (2016).

Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183.

Gelbstein, E. (2012). Strengthening Information Security Governance. *ISACA Journal*, *2*, 1–6. Retrieved from https://www.isaca.org/Journal/archives/2012/Volume-2/Documents/12v2-Strengthening-Information.pdf

Gelbstein, E. (2017). Auditoría básica de SI: Los auditores, las políticas de SI/TI y el cumplimiento. *ISACA Journal*, *2*. Retrieved from https://www.isaca.org/Journal/archives/2017/Volume-2/Pages/the-auditors-is-it-policies-and-compliance-spanish.aspx

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

Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. In *Computer and Information Sciences (ICCOINS), 2016 3rd International Conference on* (pp. 564–569). IEEE.

Hsieh, P.-J. (2015). Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk. *International Journal of Medical Informatics*, *84*(1), 1–14. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2014.08.008

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. https://doi.org/10.1145/1953122.1953142

Huang, E., & Chuang, M. H. (2007). Extending the theory of planned behaviour as a model to explain post-merger employee behaviour of IS use. *Computers in Human Behavior*, *23*(1), 240–257. https://doi.org/https://doi.org/10.1016/j.chb.2004.10.010

Huh, J., DeLorme, D. E., & Reid, L. N. (2006). Perceived third-person effects and consumer attitudes on prevetting and banning DTC advertising. *Journal of Consumer Affairs*, *40*(1), 90–116. https://doi.org/10.1111/j.1745-6606.2006.00047.x

Hung, S.-Y., & Chang, C.-M. (2005). User acceptance of WAP services: test of competing theories. *Computer Standards & Interfaces*, *27*(4), 359–370.

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

ISO. (2013). Iso/Iec 27002:2013. Retrieved from https://www.iso.org/standard/54533.html

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. https://doi.org/10.25300/MISQ/2015/39.1.06

Klein, R. H., & Luciano, E. M. (2016). What Influences Information Security Behavior? A Study with Brazilian Users. *Journal of Information Systems and Technology Management*, *13*(3), 479–496. https://doi.org/10.4301/S1807-17752016000300007

Klem, L. (1998). Path Analysis. In L. G. Grimm & P. R. Yarnold (Eds.), *Reading and understanding multivariate statistics* (Eds.). Washington, DC: American Psychological Association.

Knorst, A. M., Vanti, A. A., Andrade, R. A. E., & Johann, S. L. (2011). Aligning information security with the image of the organization

and prioritization based on fuzzy logic for the industrial automation sector. *Journal of Information Systems & Technology Management*, *8*(3), 555. https://doi.org/https://doi.org/10.4301/S1807-17752011000300003

Lee, D. (2001). Developing Effective Information Systems Security Policies. *SANS Institute*.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707–718.

Li, H., Zhang, J., & Sarathy, R. (2009). Understanding the Compliance with the Internet Use Policy from a Criminology Perspective. In *Proceedings of the Fifteenth Americas Conference on Information Systems* (pp. 1–8). San Francisco, California.

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

Lin, H.-F. (2007). Predicting consumer intentions to shop online: An empirical test of competing theories. *Electronic Commerce Research and Applications*, *6*(4), 433–442. https://doi.org/https://doi.org/10.1016/j.elerap.2007.02.002

McMahon Brian. (2007). Organizational Commitment, Relationship Commitment and Their Association With Attachment Style and Locus of Control. *Vasa*. Retrieved from http://medcontent.metapress.com/index/A65RM03P4874243N.pdf

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. *Journal of Vocational Behavior*. https://doi.org/10.1006/jvbe.2001.1842

Milicevic, D., & Goeken, M. (2013). Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps towards Evidence-Based Structuring of the IS Security Domain. In *WI* (pp. 1067–1081). Retrieved from http://www.wi2013.de/proceedings/WI2013 - Track 7 - Milicevic.pdf

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta- analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Muñiz, J., Elosua, P., & Hambleton, R. K. (2013). Directrices para la traducción y adaptación de los tests: Segunda edición. *Psicothema*, *25*(2), 151–157. https://doi.org/10.7334/psicothema2013.24

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126–139. https://doi.org/10.1057/ejis.2009.10

Ndubisi, N. O. (2004). Factors influencing e-learning adoption intention: Examining the determinant structure of the decomposed theory of planned behaviour constructs. In *In Proceedings of the 27th Annual Conference of HERDSA* (pp. 252–262).

Ng, B., & Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users ' Intention to Practice Security. In *Proceedings of the Ninth Pacific Asia Conference on Information Systems* (Vol. 2003, pp. 234–247). Bangkok, Thailand.

Njenga, K. (2016). Information Systems Security Policy Violation : Systematic Literature Review on Behavior Threats by Internal Agents. In *Proceedings of the International Conference On Information Resources Management (Conf-IRM)* (pp. 1–13). Cape Town, South Africa.

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

Pahnila, S., Siponen, M., & Mahmood, A. (2007a). Employees' behavior towards IS

security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences* (p. 156). Waikoloa, HI, USA: IEEE. 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. In *Proceedings of the 11th Pacific Asia Conference on Information Systems* (pp. 438–439). Auckland, New Zealand. https://doi.org/10.1007/978-0-387-72367-9_12

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing*, *67*(2), 1–18.

Policía Nacional del Ecuador. (2016). Conozca amenazas y vulnerabilidades de capa 8 (usuario) cuando ingresa a redes sociales. Retrieved from http://www.policiaecuador.gob.ec/amenazas-y-vulnerabilidades-de-capa-8-usuario/

Ponemon Institute. (2016). *Closing security gaps to protect corporate data: a study of US and European organizations*. *Ponemon Institute*. Retrieved from https://info.varonis.com/hubfs/docs/research_reports/Varonis_Ponemon_2016_Report.pdf

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757–778. https://doi.org/Article

Ramayah, T., Rouibah, K., Gopi, M., & Rangel, G. J. (2009). A decomposed theory of reasoned action to explain intention to use Internet stock trading among Malaysian investors. *Computers in Human Behavior*, *25*(6), 1222–1230. https://doi.org/https://doi.org/10.1016/j.chb.2009.06.007

Richardson, R. (2008). *CSI computer crime and security survey*. *Computer Security Institute* (Vol. 1). https://doi.org/10.1007/978-3-319-04307-4

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change : A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology: A Source Book* (Vol. 19, pp. 469–573). New York: Guilford. https://doi.org/10.1093/deafed/ent031

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine*, *32*(9), 40–48. https://doi.org/https://doi.org/10.1109/35.312842

Schneider, F. B. (2000). Enforceable security policies. *ACM Transactions on Information and System Security (TISSEC)*, *3*(1), 30–50.

Sherman, L. W. (1993). Defiance, deterrence, and irrelevance: A theory of the criminal sanction. *Journal of Research in Crime and Delinquency*, *30*(4), 445–473. https://doi.org/https://doi.org/10.1177/0022427893030004006

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145–147. https://doi.org/10.1145/1610252.1610289

Siponen, M., 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

Sodupe, K. (1991). La teoría de la disuasión: un análisis de las debilidades del paradigma estatocéntrico. *Afers Internacionals*, (22), 53–79.

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *IFIP Advances in Information and Communication Technology* (Vol. 405, pp. 257–271). Berlin, Heidelberg: Springer Berlin Heidelberg. 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. *Information Management & Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

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

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., Guzman, I., & Caldera, C. (2003). Examining the Linkage between Organizational Commitment and Information Security. In *IEEE International Conference on Systems, Man and Cybernetics* (pp. 2501–2506). Washington DC, USA: IEEE. https://doi.org/10.1109/ICSMC.2003.1244259

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

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security*, *16*(1), 23–33.

Steers, R. M. (1977). Antecedents and Outcomes of Organizational Commitment. *Administrative Science Quarterly*, *22*(1), 46. https://doi.org/10.2307/2391745

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441–469.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144–176.

Ugrin, J. C., & Pearson, J. M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, *29*(3), 812–820. https://doi.org/https://doi.org/10.1016/j.chb.2012.11.005

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

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

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

Wang, J., Keil, M., Oh, L. bin, & Shen, Y. (2017). Impacts of organizational commitment, interpersonal closeness, and Confucian ethics on willingness to report bad news in software projects. *Journal of Systems and Software*, *125*, 220–233. https://doi.org/10.1016/j.jss.2016.12.004

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

West, R. (2008). The Psychology of Security. *Communications of the ACM*, *51*(4), 34–40.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review*, *20*, 545–572. https://doi.org/https://doi.org/10.2307/3053466

Willison, R., & Siponen, M. T. (2009). Overcoming the Insider: Reducing Employee Computer Crime Through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133–137. https://doi.org/10.1145/1562164.1562198

Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *Proceedings of the Twenty-Sixth International Conference on Information Systems* (pp. 367–380). Las Vegas. Retrieved from https://aisel.aisnet.org/icis2005/31

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

Xiang-Yang, L., Li-Ping, W., & Lau, A. (2008). An Empirical Study on New Generation Worker's Organizational Commitment, Motivation, Work Outcomes and HRM Strategic implications. In *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*. https://doi.org/10.1109/WiCom.2008.1711

Ya-Yueh, S., & Fang, K. (2004). The use of a decomposed theory of planned behavior to study Internet banking in Taiwan. *Internet Research*, *14*(3), 213–223. https://doi.org/https://doi.org/10.1108/10662240410542643

ANEXOS

Tabla A1
Datos descriptivos

592 empleados	Conteo	%
Participantes (información de los empleados)		
Género		
Mujer	301	51%
Hombre	291	49%
Edad		
Entre 20 y 29	138	23%
Entre 30 y 39	276	47%
Entre 40 y 49	120	20%
Entre 50 y 59	55	9%
Igual o mayor a 60	3	1%
Cargo		
Personal de Tecnologías de la Información (TI)	47	8%
Otro	545	92%
Educación		
Educación secundaria completa	11	2%
Educación universitaria no completa	64	11%
Educación universitaria completa	380	64%
Doctorado o maestría	137	23%
Distrito		
Gerencia General	171	29%
Guayaquil - Aéreo	45	8%
Guayaquil - Marítimo	74	13%
Manta	18	3%
Esmeraldas	17	3%
Quito	105	18%
Puerto Bolívar	24	4%
Tulcán	40	7%
Huaquillas	29	5%
Cuenca	17	3%
Loja - Macará	16	3%
Latacunga	15	3%
Subdirección de Apoyo Regional	21	4%

Tabla A2
Estadísticos descriptivos de las variables del modelo

	N	Mínimo	Máximo	Media	Desviación estándar	Asimetría		Curtosis	
	Estadístico	Estadístico	Estadístico	Estadístico	Estadístico	Estadístico	Error estándar	Estadístico	Error estándar
probabilidad percibida de violación a la seguridad	592	1,00	7,00	5,5360	1,25676	-,969	,100	1,024	,201
severidad percibida sobre violación a la seguridad	592	1,00	7,00	5,5023	1,19770	-,803	,100	,776	,201
nivel de preocupación sobre violación a la seguridad	592	1,00	7,00	5,1075	,80693	-,321	,100	2,279	,201
eficacia de la respuesta	592	2,33	7,00	4,9814	,70573	,104	,100	1,336	,201
disponibilidad del recurso	592	1,00	7,00	4,3307	1,25249	-,100	,100	-,333	,201
auto-eficacia	592	1,00	7,00	4,7720	1,29528	-,329	,100	-,096	,201
actitud frente a la política de seguridad	592	2,33	7,00	6,3384	,88041	-1,164	,100	,649	,201
compromiso organizacional	592	2,67	7,00	6,4082	,75887	-1,370	,100	1,488	,201
severidad del castigo	592	1,00	7,00	4,9420	1,30231	-,325	,100	-,058	,201
certeza en la detección	592	1,00	7,00	5,6115	1,25520	-,964	,100	1,098	,201
norma subjetiva	592	1,00	7,00	6,0084	1,10369	-1,450	,100	3,025	,201
norma descriptiva	592	1,00	7,00	5,1847	1,23953	-,619	,100	,678	,201
intención de cumplimiento de la política de seguridad	592	2,67	7,00	6,1807	1,01084	-1,317	,100	1,276	,201
N válido (por lista)	592								

Tabla A3
Resultados del modelo

Hipótesis	β estandarizado	Error estándar	t	p	Rcuadrado ajustado	Resultados
1: Las actitudes hacia las políticas de seguridad de la información influirán positivamente en las intenciones de cumplimiento de la política de seguridad.	0,444	0,042	12,039	0,000	0,196	Confirmado
2: La severidad percibida sobre violación a la seguridad afectará positivamente el nivel de preocupación sobre violación a la seguridad.	0,524	0,024	14,94	0,000	0,273	Confirmado
3: La probabilidad percibida de violación a la seguridad afectará positivamente el nivel de preocupación sobre violación a la seguridad.	0,370	0,025	9,68	0,000	0,136	Confirmado
4: Los niveles más altos de preocupación por la violación a la seguridad darán como resultado actitudes más positivas hacia las políticas de seguridad.	0,344	0,042	8,908	0,000	0,117	Confirmado
5: La efectividad percibida de las propias acciones afectará positivamente la actitud hacia las políticas de seguridad.	0,332	0,048	8,56	0,000	0,109	Confirmado
6: El costo de respuesta percibido influirá negativamente en la actitud hacia las políticas de seguridad.	0,061	0,104	1,494	0,136	0,002	No Confirmado
7: La auto-eficacia influirá positivamente en la actitud hacia las políticas de seguridad.	0,189	0,027	4,687	0,000	0,034	Confirmado
8: La auto-eficacia afectará positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.	0,19	0,032	4,713	0,000	0,035	Confirmado
9: La disponibilidad de recursos afectará positivamente la autoeficacia.	0,102	0,42	2,502	0,013	0,009	Confirmado
10: La severidad del castigo afectará positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.	0,178	0,031	5,719	0,000	0,051	Confirmado
11: La certeza en la detección afectará positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.	0,287	0,032	7,272	0,000	0,081	Confirmado
12: Las normas subjetivas [expectativas de los demás] afectarán positivamente la intención de cumplir con las políticas de seguridad de la información organizacional.	0,434	0,034	11,715	0,000	0,187	Confirmado
13: Las normas descriptivas [comportamiento de otros similares] influirán positivamente en las intenciones de cumplir con las políticas de seguridad.	0,301	0,032	7,672	0,000	0,089	Confirmado
14: Los niveles más altos de compromiso organizacional llevarán a una mayor percepción de los empleados sobre la efectividad de sus acciones.	0,233	0,037	5,808	0,000	0,052	Confirmado
15: El nivel de compromiso organizacional afectará positivamente las intenciones de seguir las políticas de seguridad.	0,371	0,051	9,713	0,000	0,136	Confirmado

Tabla A4
Análisis de resultados – Estudio original

No.	Determinantes	Relación	Hipótesis	
			Estudio original	Estudio Actual
1	Probabilidad percibida de violación a la seguridad	3	No significativo	Significativo
2	Severidad percibida sobre violación a la seguridad	3	Significativo	Significativo
3	Nivel de preocupación sobre violación a la seguridad	8	Significativo	Significativo
4	Costo de respuesta	8	Significativo	No Significativo
5	Eficacia de la respuesta	8	Significativo	Significativo
6	Disponibilidad del recurso	7	Significativo	Significativo
7	Auto-eficacia	8	Significativo	Significativo
8	Actitud frente a la política de seguridad	14	No Significativo	Significativo
9	Compromiso organizacional	14	Significativo	Significativo
10	Severidad del castigo	14	No Significativo	Significativo
11	Certeza en la detección	14	Significativo	Significativo
12	Norma subjetiva	14	Significativo	Significativo
13	Norma descriptiva	14	Significativo	Significativo
14	Intención de cumplimiento de la política de seguridad	-	Significativo	Significativo

Tabla A5
Análisis de Resultados - Estudios previos

No.	Determinantes	Relación	Estudios previos	Resultados	
				Estudios previos	Estudio actual
1	Probabilidad percibida de violación a la seguridad	3	(Herath & Rao, 2009b)	No significativo	Significativo
2	Severidad percibida sobre violación a la seguridad	3	(Herath & Rao, 2009b)	Significativo	Significativo
3	Nivel de preocupación sobre violación a la seguridad	8	(Pahnila et al., 2007a)	Significativo	Significativo
4	Costo de respuesta	8	(Bulgurcu et al., 2010a) (Pahnila et al., 2007a)	Significativo No significativo	No Significativo
5	Eficacia de la respuesta	8	(Herath & Rao, 2009b)	Significativo	Significativo
6	Disponibilidad del recurso	7	(Pahnila et al., 2007a)	Significativo	Significativo
7	Auto-eficacia	8	(Al-Omari et al., 2013)	No Significativo	Significativo
8	Actitud frente a la política de seguridad	14	(Al-Omari et al., 2013, 2012) (Bulgurcu et al., 2010) (Li et al., 2010) (Ng & Rahim, 2005) (Pahnila et al., 2007a)	Significativo Significativo Significativo Significativo Significativo	Significativo
9	Compromiso organizacional	14	(Herath & Rao, 2009b)	Significativo	Significativo
10	Severidad del castigo	14	(Li et al., 2010) (Son, 2011)	No Significativo No Significativo	Significativo
11	Certeza en la detección	14	(Herath & Rao, 2009a) (Hu et al., 2011) (Li et al., 2009, 2010) (Son, 2011)	Significativo No Significativo Significativo No Significativo	Significativo
12	Norma subjetiva	14	(Al-Omari et al., 2013) (Bulgurcu et al., 2010) (Herath & Rao, 2009a) (Li et al., 2009, 2010) (Pahnila et al., 2007a, 2007b) (Siponen et al., 2010)	Significativo Significativo Significativo No Significativo Significativo Significativo	Significativo
13	Norma descriptiva	14	(Herath & Rao, 2009a)	Significativo	Significativo
14	Intención de cumplimiento de la política de seguridad	-	-	-	-