



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ingeniería de Sistemas e Informática
Unidad de Posgrado

**Factores del Éxito que influyen en la adopción de las
Políticas de Seguridad de la Información**

TESIS

Para optar el Grado Académico de Magíster en Gobierno de
Tecnologías de Información

AUTOR

Norman Alexis FONG OCHOA

ASESOR

Dra. Luz Sussy BAYONA ORÉ

Lima, Perú

2023



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Fong, N. (2023). *Factores del Éxito que influyen en la adopción de las Políticas de Seguridad de la Información*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Norman Alexis Fong Ochoa
Tipo de documento de identidad	DNI
Número de documento de identidad	70614684
URL de ORCID	https://orcid.org/0000-0002-1704-6991
Datos de asesor	
Nombres y apellidos	Luz Sussy Bayona Oré
Tipo de documento de identidad	DNI
Número de documento de identidad	08602165
URL de ORCID	https://orcid.org/0000-0001-7133-9106
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Cayo Víctor León Fernández
Tipo de documento	DNI
Número de documento de identidad	07001405
Miembro del jurado 1	
Nombres y apellidos	Carlos Edmundo Navarro Depaz
Tipo de documento	DNI
Número de documento de identidad	08482690
Miembro del jurado 2	
Nombres y apellidos	Fany Yexenia Sobero Rodríguez
Tipo de documento	DNI
Número de documento de identidad	20120467
Miembro del jurado 3	
Nombres y apellidos	Luz Sussy Bayona Oré
Tipo de documento	DNI

Número de documento de identidad	08602165
Datos de investigación	
Línea de investigación	No aplica.
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	Perú, Lima, Cercado de Lima 12°03'22.5"S 77°05'04.7"W
Año o rango de años en que se realizó la investigación	2019 - 2021
URL de disciplinas OCDE	Ingeniería de Sistemas y Comunicaciones http://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

A los cuatro (04) días del mes de abril de 2023, siendo las 4:45 pm., se reunieron en la sala virtual <https://meet.google.com/nea-jmhm-dky> el Jurado de Tesis conformado por los siguientes docentes:

Dr. Cayo Víctor León Fernández (Presidente)
Dr. Carlos Edmundo Navarro Depaz (Miembro)
Mg. Fany Yexenia Sobero Rodríguez (Miembro)
Dra. Luz Sussy Bayona Oré (Miembro Asesor)

Se inició la Sustentación invitando al candidato a Magíster **NORMAN ALEXIS FONG OCHOA**, para que realice la exposición oral y virtual de la tesis para optar el Grado Académico de Magíster en Gobierno de Tecnologías de Información, siendo la Tesis intitulada:

“FACTORES DEL ÉXITO QUE INFLUYEN EN LA ADOPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN”

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

..... **DIECISIETE (17) - MUY BUENO**

Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Bachiller **NORMAN ALEXIS FONG OCHOA** el Grado Académico de Magíster en Gobierno de Tecnologías de Información.

Siendo las 18:15 horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.

Dr. Cayo Víctor León Fernández
(Presidente)

Dr. Carlos Edmundo Navarro Depaz
(Miembro)

Mg. Fany Yexenia Sobero Rodríguez
(Miembro)

Dra. Luz Sussy Bayona Oré
(Miembro Asesor)



Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

Lima, 25 de Enero del 2023

INFORME N° 000001-2023-UPG-VDIP-FISI/UNMSM

INFORME DE EVALUACIÓN DE ORIGINALIDAD

1. Autoridad Académica que emite el Informe de Originalidad:	Director de la Unidad de Posgrado
2. Apellidos y Nombres de la autoridad académica:	Dr. Cayo Víctor León Fernández
3. Operador del programa informático de similitudes:	Dr. Cayo Víctor León Fernández
4. Documento evaluado:	Tesis para Posgrado Título: "Factores del Éxito que influyen en la adopción de las Políticas de Seguridad de la Información"
5. Autor del documento:	Norman Alexis Fong Ochoa
6. Fecha de recepción de documento	23/01/2023
7. Fecha de aplicación del programa detector de similitudes:	23/01/2023
8. Software utilizado:	Turnitin
9. Configuración del programa detector de similitudes:	i. Excluye textos entrecomillados: SI ii. Excluye biografías: SI iii. Excluye cadenas menores a 40 palabras: SI iv. Otro criterio (especificar): NO
10. Porcentaje de similitudes según programa detector de similitudes	Cuatro por ciento (4%)
11. Fuentes originales de las similitudes encontradas	Se adjuntan en cuatro (04) fojas al presente informe
12. Observaciones:	Ninguna
13. Calificación de originalidad i. Documento cumple criterios de originalidad, sin observaciones. ii. Documento cumple criterio de originalidad, con observaciones. iii. Documento no cumple criterios de originalidad.	Documento cumple criterio de originalidad, sin observaciones.
14. Fecha del Informe:	23/01/2023

DR. CAYO VICTOR LEON FERNANDEZ
DIRECTOR DE LA UNIDAD DE POSGRADO(e)

CLF/rda



Dedicatoria a:

Mis padres, por ayudarme a salir adelante llevando a cabo esta Maestría.

A Dios, Señor de los Cielos, por darme la fuerza y sabiduría en estos años, a pesar de las circunstancias.

Agradecimientos a:

Mi profesora de tesis, la Dra. Luz Sussy Bayona Oré, por impartirme la sapiencia y conocimientos necesarios para concebir y desarrollar una tesis robusta.

INDICE GENERAL

RESUMEN	VII
ABSTRACT.....	VIII
CAPÍTULO 1: INTRODUCCIÓN.....	1
1.1 Situación Problemática.....	3
1.2 Formulación del Problema	7
1.2.1 Problema General	7
1.2.2 Problemas Específicos	7
1.3 Justificación Teórica	9
1.4 Justificación Práctica.....	9
1.5 Objetivos	10
1.5.1 Objetivo general	10
1.5.2 Objetivos específicos.....	10
CAPÍTULO 2: MARCO TEÓRICO	12
2.1 Marco Filosófico o Epistemológico de la Investigación	12
2.2 Antecedentes de Investigación	15
2.3 Bases Teóricas.....	17
2.3.1 Seguridad de Información. –.....	17
2.3.2 Políticas de Seguridad de Información. –	18
2.4 Definiciones	22
CAPÍTULO 3: ESTADO DEL ARTE	23
3.1. Revisión de Factores en la Adopción de Políticas de Seguridad.....	23
3.1.1 Selección de artículos	24
3.1.2. Factores Críticos encontrados en la literatura	24
3.1.3. Definición de los factores encontrados en la literatura	28
3.1.4. Discusión.....	29
CAPÍTULO 4: HIPÓTESIS	30
4.1 Hipótesis General	30
4.2 Hipótesis Específicas.....	30
4.2.1 Severidad de Sanciones	30
4.2.2 Certeza de Sanciones	32
4.2.3 Compromiso Organizacional	33
4.2.4 Actitud del Empleado	33
4.2.5 Autoeficacia de Seguridad.....	35
4.2.6 Severidad Percibida de Amenazas	36

4.2.7	Vulnerabilidad Percibida de Amenazas	37
4.2.8	Conciencia de las Políticas de Seguridad de Información.....	37
4.2.9	Programa SETA	38
4.2.10	Cultura de Seguridad Organizacional	40
4.2.11	Conocimiento de Políticas de Seguridad	41
4.2.12	Intención de Cumplimiento	41
4.3	Propuesta de Modelo	42
CAPÍTULO 5: METODOLOGÍA.....		44
5.1	Tipo de Investigación	44
5.2	Unidad de Análisis	44
5.3.	Población de Estudio	44
5.4.	Tamaño de Muestra	44
5.5.	Técnicas de Recolección de Datos	45
5.6.	Técnicas de Análisis de Datos	45
CAPÍTULO 6: RESULTADOS Y DISCUSIÓN		46
6.1	Análisis y Presentación de Resultados.....	46
6.1.1	Datos demográficos de la población	46
6.1.2	Factores críticos para la adopción de PSI	49
6.2	Modelo de Ecuaciones Estructurales	57
6.3	Comprobación de Hipótesis	63
6.4	Discusión.....	64
6.4.1	Severidad de Sanciones	64
6.4.2	Certeza de Sanciones	64
6.4.3	Compromiso Organizacional	65
6.4.4	Actitud del empleado.....	65
6.4.5	Autoeficacia de seguridad	66
6.4.6	Severidad Percibida de Amenazas	66
6.4.7	Vulnerabilidad Percibida de Amenazas	66
6.4.8	Conciencia de las PSI	67
6.4.9	Programa SETA	67
6.4.10	Cultura de Seguridad Organizacional	67
6.4.11	Conocimiento de Políticas de Seguridad	68
6.4.12	Intención de Cumplimiento	68
CONCLUSIONES		69
LIMITACIONES		71
RECOMENDACIONES		72
TRABAJOS FUTUROS		73

REFERENCIAS BIBLIOGRÁFICAS. –.....	74
ANEXOS. –	86
Anexo I.- Matriz de Consistencia.....	87
Anexo II.- Encuesta utilizada en la recolección de datos.....	90

ÍNDICE DE FIGURAS

Fig. 1.1 R�anking de Pa�ses de Latinoam�rica en niveles de implementaci�n de PSI. Sitio Web de Gesti�n.	5
Fig. 1.2 Frecuencia de art�culos cient�ficos publicados acerca de los factores que determinan el �xito de las PSI por pa�s	6
Fig. 4.1 Modelo propuesto de la investigaci�n.	43
Fig. 6.1 Resultados correspondientes al factor Severidad de Sanciones.	50
Fig. 6.2 Resultados correspondientes al factor Certeza de Sanciones.	50
Fig. 6.3 Resultados correspondientes al factor Compromiso Organizacional.	51
Fig. 6.4 Resultados correspondientes al factor Actitud hacia las PSI.	51
Fig. 6.5 Resultados correspondientes al factor Autoeficacia de Seguridad	52
Fig. 6.6 Resultados correspondientes al factor Severidad percibida de amenazas.	53
Fig. 6.7 Resultados correspondientes al factor Vulnerabilidad percibida de amenazas.	53
Fig. 6.8 Resultados correspondientes al factor Conciencia de las PSI.	54
Fig. 6.9 Resultados correspondientes al factor Programas SETA.	54
Fig. 6.10 Resultados correspondientes al factor Cultura de seguridad Organizacional.	55
Fig. 6.11 Resultados correspondientes al factor Conocimiento de Pol�ticas de Seguridad.	56
Fig. 6.12 Resultados correspondientes al factor Intenci�n de Cumplimiento.	56
Fig. 6.13 Resultados correspondientes a la Adopci�n de las Pol�ticas de Seguridad.	57
Fig. 6.14 Modelo de ecuaciones estructurales de los factores para la adopci�n de las PSI.	62

INDICE DE TABLAS

Tabla 3.1 Criterios para la revisión de artículos	23
Tabla 3.2 Cadena de búsqueda para la revisión de artículos.....	23
Tabla 3.3 Artículos seleccionados según base de datos.....	24
Tabla 3.4 Factores críticos encontrados en la literatura ordenados por frecuencia.	26
Tabla 3.5 Definiciones de los factores según autores	28
Tabla 6.1 Frecuencia de participantes en la encuesta con respecto al sexo.....	46
Tabla 6.2 Frecuencia de participantes en la encuesta por edades.	47
Tabla 6.3 Frecuencia de participantes en la encuesta por niveles de educación.	47
Tabla 6.4 Frecuencia de participantes en la encuesta con respecto a las líneas organizacionales.	48
Tabla 6.5 Frecuencia de participantes en la encuesta repartidos por experiencia laboral.	48
Tabla 6.6 Frecuencia de las razones de la ausencia de políticas de seguridad en las organizaciones	48
Tabla 6.7 Frecuencia de estándares de seguridad utilizados en las organizaciones.	49
Tabla 6.8 Modelo inicial	58
Tabla 6.9 Indicadores de bondad de ajuste del modelo inicial	59
Tabla 6.10 Modelo final	59
Tabla 6.11 Indicadores de bondad de ajuste del modelo final	61
Tabla 6.12 Confirmación de hipótesis de la investigación según resultados.	63
Tabla 7.1 Matriz de Consistencia	87

RESUMEN

La seguridad de la información es un aspecto importante en el panorama actual de incorporación de tecnologías de información en las empresas y organizaciones. Las políticas de seguridad de la información (PSI) establecen las directrices de seguridad de la información que los colaboradores de una organización deben de cumplir; sin embargo, pese a su importancia, el cumplimiento de las políticas no es efectivo en las organizaciones, lo que ha dado lugar a violaciones graves de la información de muchas organizaciones.

En la presente investigación se describe la situación actual de la adopción de las PSI, así como se hace mención de investigaciones previas que determinan diversos factores y su influencia en el éxito de la adopción de PSI. En base a esto, el objetivo de esta investigación es determinar la influencia de los factores de éxito en la adopción de las PSI en las organizaciones. Para apoyar la investigación, se toma en base la ISO 27001, que establece los estándares de aplicación de PSI.

Se utiliza un enfoque cuantitativo de tipo descriptivo-correlacional para abordar la investigación. La población estuvo constituida por los profesionales del área de seguridad de la información de las organizaciones. y una muestra de 108 profesionales de seguridad. Para realizar el análisis de los datos obtenidos se utilizó el modelo de ecuaciones estructurales (SEM).

Los resultados indican que existe una influencia de factores como certeza de sanciones, actitud del empleado, autoeficacia e intención de cumplimiento en la adopción de las PSI en el plano local, lo cual se encuentra en la línea de otras investigaciones realizadas en el plano internacional; la severidad de sanciones y el conocimiento de PSI influye en la intención de cumplimiento de las PSI; sin embargo, las influencias de otros factores, tales como vulnerabilidad percibida de amenazas y conciencia de las PSI, que fueron comprobadas en investigaciones previas realizadas en el extranjero, no han sido igualmente comprobadas en el entorno peruano, mientras que los programas de educación, entrenamiento y conciencia de seguridad muestran una influencia importante, mas no directa, en la adopción de las PSI.

En conclusión, se comprobó la influencia de los factores en la adopción de las políticas de seguridad.

Palabras clave: factores, adopción de políticas de seguridad de información, ISO 27000, COBIT.

ABSTRACT

Information security is one of the most important aspects to be addressed in today's information technology scenario, as companies and organizations which manage their information assets more efficiently are the ones which will most easily achieve financial and commercial success. Information security policies (ISP) establish the guidelines which all the personnel of an organization must follow regarding security aspects; however, despite its importance, policy compliance is ineffective in organizations, leading to serious breaches of the information of many organizations.

This research describes the current situation of adoption of ISP, as well as mention previous investigations which determine various factors and their influence on the success of the implementation of security policies. Based on this, the goal of this research is to determine the influence of success factors in the adoption of ISP in organizations. To support the research, ISO 27001 is based on the standards for the application of security policies.

A descriptive-correlational quantitative approach is used to carry out the research. The population was made up of professionals in the organizational information security areas, and a sample of 108 security professionals. For data analysis, the structural equations model (SEM) was used.

The results indicate that there is an influence of factors such as certainty of sanctions, employee attitude, self-efficacy and intention to comply in the adoption of ISP at the local level, which is in line with other research carried out at the international level; the severity of sanctions and the knowledge of ISP influence the intention to comply with the ISP; however, the influences of other factors, such as perceived vulnerability to threats and awareness of ISP, which were verified in previous research carried out abroad, have not been equally verified in the Peruvian environment, while education, training programs and security awareness show an important, but not direct, influence on the adoption of ISP.

In conclusion, the influence of the factors in the adoption of ISP was verified.

Keywords: factors, adoption of information security policies.

CAPÍTULO 1: INTRODUCCIÓN

La importancia de la seguridad de información (SI) se refiere a la necesidad de salvaguardar los activos de información de las organizaciones, asegurando su confidencialidad, integridad y disponibilidad, con el fin de mantener el bienestar económico y estructural de las propias organizaciones. Esto es sumamente importante dado que cada año se producen ataques de seguridad en las organizaciones, y para ello se deben delinear políticas de seguridad de la información (PSI) que todos los miembros de una organización, ya sea estatal o privada, deben seguir.

Diversos estándares y frameworks destacan la importancia de las PSI para proteger los activos de seguridad de las organizaciones. En particular, el estándar internacional ISO 27001 establece los protocolos necesarios para la implementación de las PSI en las empresas con el fin de establecer la seguridad de información en las organizaciones. Sin embargo, pese a que las políticas de seguridad son una medida importante para salvaguardar la confidencialidad, integridad y disponibilidad de la información y deben ser observadas por la totalidad del personal de las empresas, en muchos casos el cumplimiento de las mismas no es efectivo, lo que lleva a graves violaciones de seguridad de información, tales como robo y alteración de la misma, lo que a su vez ha llevado a repercusiones en el bienestar de las empresas, tales como el cese de actividad por la indisponibilidad de equipos de trabajo, y multas por incumplimiento legal de privacidad de los clientes, y en consecuencia, a pérdidas económicas y fracasos comerciales de las empresas y al impacto negativo en la imagen y reputación de las mismas, traducida en la pérdida de clientes leales y potenciales. El Perú no es ajeno a esta problemática, siendo incluso uno de los países más afectados, dado que estudios recientes determinan que sólo el 42% de empresas peruanas han implementado PSI (Rojas, 2019).

Dada esta situación, diversos autores realizaron una serie de estudios empíricos a nivel global desde la década pasada para determinar cómo influyen diversos factores en la adopción de las PSI aplicadas en las organizaciones, girando en torno a factores presentes en diversas teorías de comportamiento de los individuos como lo son la Teoría de Disuasión General (GDT), la Teoría

de Comportamiento Planeado (TPB), la Teoría de Decisión Racional (RCT), la Teoría de Acción Razonada (TRA), la Teoría de Lazos Sociales (SBT) y la Teoría de Motivación de Protección (PMT).

Estas teorías han sido adoptadas por los autores y aplicadas a la seguridad de información. Se plantean constructos que están orientados a analizar el comportamiento de los individuos en el proceso de adopción de las PSI. Entre estos factores podemos mencionar la severidad y certeza de sanciones aplicadas ante violaciones de seguridad de información (Chen et al., 2018a; Khan & Alshare, 2019), la actitud de los individuos con respecto a las PSI (Ifinedo, 2014; Siponen, Mahmood & Pahlila, 2014; Safa, Solms, & Furnell, 2016); las percepciones de severidad y vulnerabilidad de amenazas (Siponen et al., 2014; Bélanger et al., 2017; Rajab & Eydgahi, 2019), y la autoeficacia de los empleados para llevar a cabo tareas de seguridad de información, incluyendo las políticas (Siponen et al., 2014; Humaidi & Balakrishnan, 2018; Rajab & Eydgahi, 2019), entre otros.

Los modelos planteados en los estudios corresponden experiencias internacionales y no se han encontrado en la misma proporción estudios realizados en el Perú sobre factores que condicionan la adopción de PSI. En cuanto a estudios similares, éstos están enfocados en la implementación de los estándares de SI. Una de las prácticas del estándar ISO 27002 es que la información cuente con PSI. Por ello, las organizaciones hacen denodados esfuerzos para implementarlas, sin embargo, estas políticas no son adoptadas por todos los colaboradores. En respuesta a esto, este trabajo de investigación se enfoca en determinar qué factores condicionan la adopción de las políticas.

La presente investigación se encuentra motivada por la creciente problemática de violaciones de SI producto de la deficiente implementación y comunicación de las PSI al personal de las organizaciones, y la serie de crisis económicas y de reputación en las empresas generadas por las mismas. El estudio busca determinar cómo influyen los diversos factores que contribuyen a la adopción de políticas de seguridad con el fin de proporcionar un enfoque más efectivo para la adopción de políticas.

El objetivo de esta investigación es determinar la influencia de los factores de éxito en la adopción de las políticas de seguridad en las organizaciones. El presente documento se encuentra estructurado de la siguiente manera.

El Capítulo 1 es parte de esta introducción, y en él se detalla la situación problemática, se plantea el problema general y problemas específicos, y partiendo de estos últimos, se establecen el objetivo general y objetivos específicos de la investigación. Además, se explican las justificaciones teórica y práctica de la investigación.

En el Capítulo 2 se menciona el marco epistemológico del tema de investigación, la fundamentación teórica, y los antecedentes al tema investigado y se definen los términos y factores importantes para la investigación.

En el Capítulo 3 se detalla el estado del arte, basado en artículos científicos, realizado con el fin de encontrar y determinar los factores a estudiar en la tesis, así como los medios y países con mayor número de investigaciones.

En el Capítulo 4 se establecen la hipótesis general y las hipótesis específicas, se identifican y establecen las dimensiones de las variables y se establece el modelo propuesto en base a las variables encontradas en el estado de arte.

En el Capítulo 5 se define el tipo y diseño de investigación, la población y muestra y las técnicas para recolectar y analizar los datos.

En el Capítulo 6 se mencionan los resultados alcanzados y la discusión de los mismos tras finalizar el proceso de investigación.

Por último, se hace mención de las conclusiones y recomendaciones surgidas a raíz de la investigación.

1.1 Situación Problemática

Con la implementación de las tecnologías de información en las organizaciones, un aspecto importante a tratar es la seguridad de información (SI) (Chen et al., 2018a; Liu et al., 2020). Las organizaciones que gestionan de forma eficiente los activos de información alcanzan sus metas financieras y comerciales. Por esta razón, una de las acciones para asegurar la SI radica en el establecimiento de las PSI (Chen et al., 2018a; Kuo et al., 2020).

Las PSI son importantes para gestionar la seguridad en las organizaciones, dado que establecen las directrices que los colaboradores de la organización deben de cumplir (Doherty et al., 2009; como se citó en Weidman & Grossklags, 2020), lo cual, a su vez, implicará que la empresa mantenga y expanda su base de clientes, consolide su situación financiera y comercial en el escenario de negocios y optimizar su estructura organizacional y corporativa. Sin embargo, pese a que se espera que los colaboradores tengan conocimiento y cumplan con la PSI, en muchos casos se ha comprobado que el cumplimiento de las políticas no es efectivo, lo que ha dado lugar a violaciones graves de la información de muchas empresas, tales como robo y alteración de la misma (Merhi & Ahluwalia, 2019; Wiafe et al., 2020), el cese de actividad por la indisponibilidad de equipos de trabajo, y multas por incumplimiento legal de privacidad de los clientes, lo que a

su vez ha llevado a pérdidas económicas y fracasos comerciales de las empresas y al impacto negativo en la imagen y reputación de las mismas, traducida en la pérdida de clientes leales y potenciales (Kolkowska et al., 2017; Samonas et al., 2020).

Las organizaciones utilizan las buenas prácticas internacionales sobre Seguridad de la Información y diseñan las PSI. Sin embargo, a pesar de que “la implementación de Políticas de Seguridad es una de las prácticas más utilizadas en este campo, aún los niveles de adopción no son los óptimos” (Rojas, 2019, p. 19). Al respecto, un estudio reciente sostiene que las organizaciones todavía tienen la tendencia de ignorar las PSI (Setiawan y Maharani, 2022) y existen pocas investigaciones para evaluar el cumplimiento con la PSI (Angrani et al., 2022). Angrani et al. (2022) sostiene que asegurar el cumplimiento de la PSI requiere que el comportamiento de los colaboradores sea observado y monitoreado por la organización. En este contexto, se debe tener en cuenta la importancia de la conciencia de seguridad y los programas de capacitación y sensibilización sobre seguridad en la adopción de las PSI. Luego, evaluar la adopción de las PSI ayuda a conocer el nivel de cumplimiento de los usuarios de tecnología de la información.

En una revisión sistemática (Kuppusamy et al., 2022) sobre los factores que influyen en la adopción de las PSI se encontró que los factores normas subjetivas, actitudes, beneficios percibidos, vulnerabilidad percibida, severidad percibida y severidad de sanciones entre las más importantes.

Setiawan y Maharani (2022) encontraron que los factores de conciencia de seguridad y actitud del empleado tienen un impacto en la intención de seguir las PSI.

Los estudios anteriormente mencionados corresponden a experiencias internacionales. El aporte de esta investigación es conocer el comportamiento de estos factores en el contexto local.

La Figura 1.1. presenta un ranking según los niveles de implementación de prácticas de seguridad en el que Perú ocupa el último lugar en Latinoamérica en la implementación de políticas de seguridad, según el ESET Security Report Latinoamérica 2019 (Rojas, 2019), lo cual demuestra que en muchas empresas no existe una intención generalizada de aplicar políticas de seguridad. El Perú no es ajeno a esta problemática, siendo incluso uno de los países más afectados, dado que estudios recientes determinan que sólo el 42% de empresas peruanas han implementado PSI (Rojas, 2019).

Niveles de implementación de prácticas de gestión para la seguridad por país

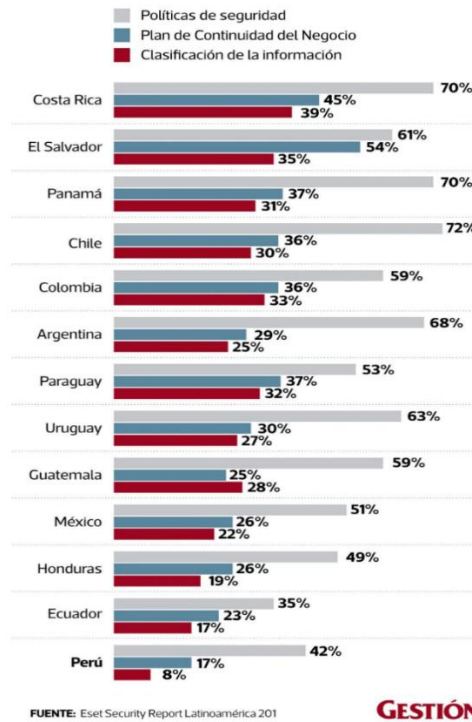


Fig. 1.1 Ránking de Países de Latinoamérica en niveles de implementación de PSI. Sitio Web de Gestión.

Existe una carencia de investigaciones para evaluar la adopción de la PSI (Angrani et al., 2022), en especial si se hace un análisis de la producción científica, utilizando la base de datos Scopus, sobre factores y PSI, se observa que Estados Unidos (58), Malasia (32), Reino Unido (23), Sudáfrica (16) y China (14) muestran presentan mayor cantidad de publicaciones. En el caso de los países de Latinoamérica figuran Brasil (3), Perú (2), Colombia (1) y Ecuador (1). En el caso de Perú presenta solo dos publicaciones, a mencionar: Celi & Díaz (2021) y Yupanqui, J., & Bayona, S. (2017), como se aprecia en la Figura 1.2.

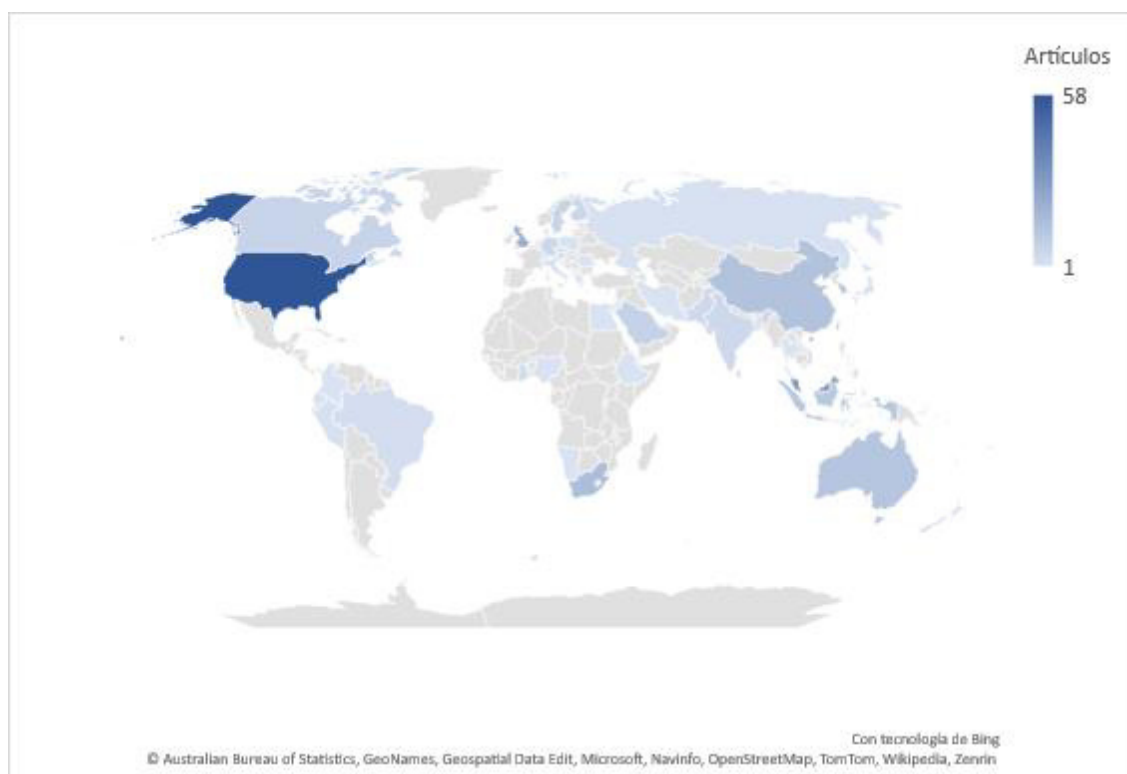


Fig. 1.2 Frecuencia de artículos científicos publicados acerca de los factores que determinan el éxito de las PSI por país

Diversas investigaciones llevadas a cabo en diferentes países han analizado y determinado progresivamente una serie de factores que determinan el cumplimiento o, en contramedida, el incumplimiento, de las PSI. Algunos factores a mencionar incluyen la capacidad disuasiva de las políticas de información en la probabilidad de violación de las mismas por parte del personal de la empresa, bajo amenaza de ser descubiertos y sancionados severamente (Khan & Alshare, 2019; Merhi & Ahluwalia, 2019; Rajab & Eydgahi, 2019; Safa et al., 2019; Trang & Brendel, 2019; Jaeger et al., 2020); el compromiso de los empleados con sus organizaciones, destacando el compromiso con la SI (Ifinedo, 2014; Safa et al., 2016; Chol & Song, 2018; Sharma & Warkentin, 2019); la actitud que los empleados adoptan en relación a las PSI (D'arcy & Lowry, 2019; Hina et al., 2019; Safa et al., 2019; Rajab & Eydgahi, 2019; Hong & Furnell, 2019; Nasir et al., 2019; Chang & Seow, 2019; Sommestad et al., 2019; Trang & Brendel, 2019; Koohang et al., 2020; Gwebu et al., 2020; Vance et al., 2020), lo cual determina su accionar diario a favor o en contra de las mismas; las percepciones de severidad y vulnerabilidad de amenazas (Rajab & Eydgahi, 2019; Hina et al., 2019; Addae et al., 2019), la autoeficacia de seguridad que los empleados deben poseer para tratar con todos los aspectos de la seguridad de información, incluyendo las políticas (D'arcy & Lowry, 2019; Pham, 2019; Rajab & Eydgahi, 2019; Nasir et al., 2019; Addae, Simpson & Ampong, 2019; Hina et al., 2019; Chang & Seow, 2019; Safa et al., 2019); la conciencia de PSI (Sommestad et al., 2019; Khan & Alshare, 2019; Pham, 2019; Jaeger et al., 2020; Koohang

et al., 2020), los programas SETA (Kim et al., 2019; Hina et al., 2019; Dhillon et al., 2020) y la cultura de seguridad organizacional (Khan & Alshare, 2019; Nasir et al., 2019; Sommestad et al., 2019).

En cuanto a los estudios que involucran a las PSI en el Perú, pese a que existen investigaciones que se enfocan en su mayoría en el desarrollo de sistemas de gestión de bases de datos, y aparte del trabajo de investigación consistente en un estado del arte con el fin de “identificar las amenazas no intencionales de ciberseguridad por parte de personal interno en instituciones públicas” (Castillo et al., 2021), no existen muchas investigaciones que se enfoquen exclusivamente en los factores que determinan la adopción de la PSI establecida por la organización. Según Rojas (2019), si “bien la implementación de Políticas de seguridad es una de las prácticas más utilizadas en este campo, aún los niveles de adopción no son los óptimos” (p. 19). Una investigación peruana que debe ser mencionada es la investigación basada en la actividad de los usuarios de tecnologías de información (TI) en una empresa microfinanciera en Lambayeque (Celi & Díaz, 2017; Celi & Diaz, 2021), basada en las teorías de comportamiento planeado, acción razonada y disuasión, en la que se determinó la influencia de factores como integración, compromiso, conciencia, motivación, entrenamiento, tecnologías de control, y medidas disuasivas, entre otros. Sin embargo, no se consideraron otros factores presentes en la literatura científica y que forman parte del aporte de esta investigación. Por estos motivos, es importante realizar más estudios que involucren factores de diversos modelos y teorías y su influencia en el escenario peruano.

1.2 Formulación del Problema

1.2.1 Problema General

¿En qué medida influyen los factores de éxito en la adopción de las PSI en las organizaciones?

1.2.2 Problemas Específicos

- ¿En qué medida influye la severidad de sanciones en la intención de cumplimiento de las PSI en las organizaciones?
- ¿En qué medida influye la certeza de sanciones en la intención de cumplimiento de las PSI en las organizaciones?

- ¿En qué medida influye la certeza de sanciones en la adopción de las PSI en las organizaciones?
- ¿En qué medida influye el compromiso organizacional en la actitud del empleado hacia las PSI en las organizaciones?
- ¿En qué medida influye la actitud del empleado en la cultura organizacional de seguridad?
- ¿En qué medida influye la actitud del empleado en la intención de cumplimiento de las PSI en las organizaciones?
- ¿En qué medida influye la actitud del empleado en la adopción de las PSI en las organizaciones?
- ¿En qué medida influye la autoeficacia de seguridad en la conciencia de PSI en las organizaciones?
- ¿En qué medida influye la autoeficacia de seguridad en la intención de cumplimiento de las PSI en las organizaciones?
- ¿En qué medida influye la autoeficacia de seguridad en la adopción de las PSI en las organizaciones?
- ¿En qué medida influye la severidad percibida de amenazas en la intención de cumplimiento de PSI en las organizaciones?
- ¿En qué medida influye la vulnerabilidad percibida de amenazas en la intención de cumplimiento de las PSI en las organizaciones?
- ¿En qué medida influye la conciencia de las PSI en la adopción de las PSI en las organizaciones?
- ¿En qué medida influyen los programas SETA en la cultura de seguridad organizacional?
- ¿En qué medida influyen los programas SETA en la intención de cumplimiento de las PSI en las organizaciones?
- ¿En qué medida influye la cultura de seguridad organizacional en la adopción de las PSI en las organizaciones?
- ¿En qué medida influye el conocimiento de las políticas de seguridad en la actitud del empleado hacia las PSI en las organizaciones?
- ¿En qué medida influye el conocimiento de las políticas de seguridad en la intención de cumplimiento de las PSI en las organizaciones?
- ¿En qué medida influye la intención de cumplimiento en la adopción de las PSI en las organizaciones?

1.3 Justificación Teórica

La presente investigación, que radica en un estudio empírico, es importante porque se enfoca en los procesos de diseño e implementación de políticas de seguridad de la información, un aspecto clave de la gestión de la seguridad de la información del cual existen varios antecedentes de inadecuada estructuración y comunicación, lo cual ha dado lugar a violaciones y brechas de seguridad de información, mismas que resultaron en pérdida de información valiosa para las organizaciones afectadas y el subsecuente impacto negativo económico, comercial y de reputación en las mismas (Kolkowska et al., 2017).

Aunado a lo anterior, el estudio toma como referencia los estándares de seguridad que dictan las pautas a seguir en seguridad de información, tales como ISO 27001 e ISO 27002 y el framework para la gobernanza de TI COBIT.

1.4 Justificación Práctica

La investigación tiene como objetivo determinar la influencia de factores como la severidad y certeza de sanciones, la autoeficacia, la actitud de los empleados, la percepción de amenazas, la conciencia de PSI, los programas de educación, entrenamiento y conciencia de seguridad y la cultura de seguridad organizacional, y con dichos resultados, otorgar a las organizaciones que hacen uso de las tecnologías de información una visión clara de la estructura apropiada y enfocada en el aspecto humano de las PSI.

Este último punto, el aspecto humano, representado por los empleados y el personal en general de las organizaciones, es de gran importancia, dado que actualmente muchas PSI diseñadas e implementadas en las empresas fracasan por no considerar de forma precisa al grupo objetivo que debe ejercer su cumplimiento (Ifinedo, 2014).

Dado que se ha demostrado en múltiples ocasiones que el aspecto más débil de la seguridad de información es, precisamente, el aspecto humano, las organizaciones deben evitar enfocarse excesivamente en el aspecto tecnológico y comenzar a tomar más en cuenta al personal que conforma gran parte de sus estructuras a la hora de diseñar, desarrollar e implementar sus PSI (Ifinedo, 2014).

1.5 Objetivos

1.5.1 Objetivo general

Determinar la influencia de los factores de éxito en la adopción de las PSI en las organizaciones.

1.5.2 Objetivos específicos

- Determinar la influencia de la severidad de sanciones en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la certeza de sanciones en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la certeza de sanciones en la adopción de las PSI en las organizaciones.
- Determinar la influencia del compromiso organizacional en la actitud del empleado hacia las PSI en las organizaciones.
- Determinar la influencia de la actitud del empleado en la cultura organizacional de seguridad.
- Determinar la influencia de la actitud del empleado en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la actitud del empleado en la adopción de las PSI en las organizaciones.
- Determinar la influencia de la autoeficacia de seguridad en la conciencia de PSI en las organizaciones.
- Determinar la influencia de la autoeficacia de seguridad en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la autoeficacia de seguridad en la adopción de las PSI en las organizaciones.
- Determinar la influencia de la severidad percibida de amenazas en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la vulnerabilidad percibida de amenazas en la intención de cumplimiento de las PSI en las organizaciones.

- Determinar la influencia de la conciencia de las PSI en la adopción de las PSI en las organizaciones.
- Determinar la influencia de los programas SETA en la cultura de seguridad organizacional.
- Determinar la influencia de los programas SETA en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la cultura de seguridad organizacional en la adopción de las PSI en las organizaciones.
- Determinar la influencia del conocimiento de las políticas de seguridad en la actitud del empleado hacia las PSI en las organizaciones.
- Determinar la influencia del conocimiento de las políticas de seguridad en la intención de cumplimiento de las PSI en las organizaciones.
- Determinar la influencia de la intención de cumplimiento en la adopción de las PSI en las organizaciones.

CAPÍTULO 2: MARCO TEÓRICO

2.1 Marco Filosófico o Epistemológico de la Investigación

Política. –

El término política proviene de la palabra griega *Politiká*, que es una romanización del griego antiguo Πολιτικά., refiriéndose a “asuntos de las ciudades”. Una definición alternativa de política, y aquella que atañe al tema de investigación, se refiere a un “sistema deliberado de principios para guiar decisiones y obtener resultados racionales.”

El científico político americano Theodore J. Lowi propuso tres tipos de política: distributiva, redistributiva, regulatoria y constituyente, y define la política regulatoria de la siguiente manera:

Aunque las leyes se expresan en términos generales ("Organizar artísticamente el sistema de transporte". "No mostrarás favoritismo en la fijación de precios"), el impacto de las decisiones regulatorias es claramente el de elevar directamente los costos y / o reducir o expandir las alternativas de individuos privados ("¡Fuera del césped!", "¡Produzca kosher si anuncia kosher!"). (Lowi, 1964, p.690)

Entonces, mientras que la implementación es firma por firma y caso por caso, las políticas no se pueden desagregar al nivel del individuo o de la firma individual (como en la distribución), porque las decisiones individuales deben tomarse por aplicación de una regla general y, por lo tanto, se interrelacionan dentro de los estándares más amplios de la ley. (Lowi, 1964, p.691)

Uno de estos tipos de política es, precisamente, las PSI.

James E. Anderson, en su obra *Public Policy-Making* (1977), estableció una versión del ciclo de política, que comprende los siguientes pasos: Establecimiento de agenda (Identificación del problema), formulación de política, toma de decisiones, implementación y evaluación. Todos

estos pasos deben ser seguidos por los oficiales de seguridad de información de las empresas al momento de crear las políticas de seguridad a aplicar en las mismas.

Seguridad de Información. -

La seguridad de información ha existido desde tiempos antiguos. dado que desde los inicios se comprendió que era necesario contar con mecanismos para proteger la correspondencia asegurando la confidencialidad de la información en el campo militar y la diplomacia. De igual forma, se establecieron mecanismos para determinar cualquier manipulación. Es el caso del político romano Julio César a quien se le acredita inventar el Cifrado César. El Cifrado César, que data de 50 A.C., evitaba la lectura de mensajes secretos cuando caían en manos de personas no autorizadas. Años después, la protección fue lograda en mayor parte utilizándose marcas en la información. De esta manera se protegía y transportaba por personas de confianza, y se mantenían en un entorno seguro (Suetonius, 2008).

Al expandirse los servicios postales, se cuentan con organizaciones especiales, creadas por los gobiernos, para interceptar, descifrar y leer mensajes (Johnson, 1997). Como ejemplo se menciona la creación en 1653 de la Oficina Secreta del Reino Unido.

En el siglo XIX aparecen sistemas más complejos para manejar la información dependiendo del grado de sensibilidad, como la codificación llevada a cabo por el gobierno británico con la publicación del Acta Oficial de Secretos en 1889 (Hastedt, 2011). Los sistemas de clasificación evolucionan a sistemas de múltiples capas para transmitir información entre varios frentes, precisamente en cuarteles generales diplomáticos y militares. En el período “entre guerras”, la codificación se volvió más sofisticada debido al uso de máquinas para ensamblar información, y en la Segunda Guerra Mundial, debido al volumen de información, se necesitó un alineamiento formal de sistemas de clasificación y controles de proceso. En este caso, se debe destacar el uso de la Máquina Enigma, utilizada en Alemania durante la guerra, descryptada exitosamente por Alan Turing (Sebag-Montefiore, 2011).

Hacia el final del siglo XX e inicios del siglo XXI, el auge de la tecnología, los sistemas de encriptación de datos, y finalmente, el uso de computadoras caseras baratas y el surgimiento de internet condujeron a la generación masiva de datos electrónicos. Sin embargo, los diferentes casos de ciberterrorismo propiciaron la búsqueda de nuevas y mejores formas de proteger la información, surgiendo así el concepto actual de seguridad de información (DeNardis, 2007).

Paradigma Positivista. –

Adler (1964, como se citó en Villamar, 2015) define al positivismo como “una epistemología híbrida que combina el racionalismo con el empirismo y la lógica deductiva con la lógica inductiva, también ha sido denominado hipotético deductivo, cuantitativo, empírico-analista y racionalista”.

El positivismo denota un enfoque filosófico, teoría o sistema basado en la opinión de que, en la vida social, así como el sentido de las ciencias naturales experiencias y su tratamiento lógico y matemático son la fuente exclusiva de toda la información que vale la pena. Es decir que, para el positivismo clásico, toda ciencia para ser considerada así, debe adaptarse a los paradigmas de las ciencias naturales, el cual se caracterizaba por el monismo metodológico, el método físico-matemático, la explicación causal y la predicción. (Villamar, 2015, p.2)

Hamati-Ataya (2012, como se citó en Villamar, 2015) define al positivismo de la siguiente manera:

El positivismo normalmente se adhiere a una visión evolutiva del cambio cognitivo por el cual el reconocimiento del actual progreso implica el reconocimiento del error del pasado y las teorías compiten sobre la base de su mayor “ajuste” con la evidencia experimental. (Villamar, 2015, p.2)

Según Duran (2002, como se citó en Villamar, 2015), “el paradigma positivista tiene como interés explicar, controlar y predecir la naturaleza de la realidad descrita como dada, singular, tangible, fragmentable y convergente, y en el cual la relación sujeta/objeto es manifestada como independiente, neutral y libre de valores”.

De acuerdo con este paradigma, se establece el objetivo fundamental, que consiste en la generalización mediante metodologías deductivas, cuantitativas, centrada sobre semejanzas y cuya última explicación está orientada a la causalidad, causas reales temporalmente precedentes y simultáneas. Finalmente, está libre de valores que pudieran contaminar los resultados. (Villamar, 2015, p.2)

La presente investigación se lleva a cabo usando el paradigma positivista, dado que se aplican varios aspectos de las definiciones de dicho paradigma durante su evolución.

2.2 Antecedentes de Investigación

2.2.1 Tesis Doctoral: *“Marco de mejora continua del gobierno TI en entidades financieras”*

La tesis traza como uno de sus objetivos (Objetivo Parcial 6), verificar la “validez de la Propuesta de Marco de Mejora Continua de Gobierno TI en base a la opinión de Expertos en Gobierno, Seguridad, Control Interno y Auditoría TI” (Prieto, 2016, p.3).

En un proceso de mejora continua del Gobierno de TI, implica la implementación de PSI, considerando factores como la Cultura de Seguridad, Conocimiento de Políticas de Seguridad, Compromiso Organizacional, Educación y Entrenamiento en Políticas de Seguridad y Sanciones a Violaciones de Políticas de seguridad.

El autor llega a las siguientes conclusiones:

La propuesta de un marco o metodología ágil de Gobierno de TI busca evaluar e implementar las iniciativas de Gobierno de TI de forma rápida y flexible, así como evolucionar su madurez dentro del proceso de mejora continua. (Prieto, 2016, p.176)

Gobierno y Seguridad de TI deben trabajar de forma coordinada para asegurar el normal funcionamiento de los sistemas de TI de forma segura y garantizar la continuidad de las entidades. (Prieto, 2016, p.176)

Relación con la tesis de investigación: El estudio, en el apartado de estado del arte, realiza una detallada y extensiva revisión literaria que coloca mucho énfasis en las PSI, siendo estas últimas uno de sus objetivos específicos. El autor, de esta forma, considera que Gobierno y Seguridad de TI no deben mantenerse aislados dado que los múltiples paradigmas de riesgos, los cuales están relacionados a Seguridad de TI, requieren necesariamente de una aplicación efectiva del Gobierno Corporativo.

Sin embargo, no se mencionan factores presentes en esta investigación como Actitud, Autoeficacia, Severidad Percibida de Amenazas, Vulnerabilidad Percibida de Amenazas ni Conciencia de Políticas de Seguridad.

2.2.2 Tesis de Doctorado: “*Friend or foe? Information security management of employees*”

Se realiza un estudio del rol y la función de los individuos en la SI considerando la importancia de conocer y entender lo que se gestiona: medidas dirigidas a mejorar el rendimiento individual de la SI y la práctica real de SI en las organizaciones (Albrechtsen, 2008).

El estudio utiliza factores como: tecnología, estructura formal, interacciones, relaciones sociales, conciencia, valores y normas, y factores contextuales. En contraste, el estudio no hace mención de factores como Severidad y Vulnerabilidad de Amenazas.

El autor llega a las siguientes conclusiones:

Los usuarios se ven como un recurso no explotado en el trabajo de SI, mientras que los gerentes de SI ven a los usuarios como una amenaza y un problema al nivel de SI. Sin embargo, cuando se trata de trabajo operativo, el rendimiento de la SI de los usuarios es pobre, dado que los usuarios llevan a cabo pocas acciones proactivas de seguridad de información y son indiferentes a la seguridad de información en su trabajo diario (Albrechtsen, 2008).

La mayoría de las medidas de seguridad de información no-tecnológicas dirigidas a los empleados son medidas formales tecno-administrativas, y la comunicación cara-a-cara y la participación de los empleados son utilizadas modestamente en la comunidad de seguridad de información. Entre más usuarios estén involucrados activamente en la medida, más efectiva la medida es evaluada en mejorar la conciencia y comportamiento; pero el efecto individual es bajo. Por lo tanto, existe una relación transversal entre el uso y el efecto subjetivo evaluado (Albrechtsen, 2008).

Las diferencias de acercamiento, experiencias y prioridades entre los gerentes de seguridad de información y los usuarios resultan en estrategias de gestión basadas en visiones prejuiciadas que ven a los usuarios como una amenaza de seguridad

y no como un recurso, y los profesionales de seguridad de información dan las premisas para el trabajo de seguridad de información en una organización sin involucrar a los usuarios en ningún grado. Consecuentemente, los acercamientos de la gerencia pueden ser insuficientes para tratar con los usuarios como un recurso dado que las actividades de seguridad de información están basadas en entendimientos irreales del trabajo real en el extremo (Albrechtsen, 2008).

La participación de los empleados puede mejorar la calidad de las soluciones de seguridad administrativas, mejorar la usabilidad de la tecnología de seguridad, mejorar el conocimiento de los profesionales de seguridad en las actividades de seguridad de información en el extremo y cerrar la brecha de entendimiento y comunicación entre los gerentes de seguridad y los usuarios, entre otros beneficios (Albrechtsen, 2008).

Relación con la tesis de Investigación: Los resultados de esta tesis indican que los empleados constituyen el elemento más vulnerable de la seguridad de información, dado que en muchas ocasiones ellos llevan a cabo poco trabajo y poseen poca conciencia de las medidas de la seguridad de información, comprendiéndose entre estas las políticas de seguridad. El estudio indica, además, que se debe cubrir la brecha entre los empleados y los gerentes y profesionales de seguridad de información promoviendo la participación y comunicación.

2.3 Bases Teóricas

2.3.1 Seguridad de Información. –

La Seguridad de información (SI) se entiende la protección de la “información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la misma” (Nieles et al., 2017, p. 7). La SI, por lo tanto, es definida como un “aspecto natural de las actividades diarias de todos los miembros de una organización” (Alshare et al., 2018, p. 3). Así, la implementación cuidadosa de los controles de SI es vital para la protección de los activos de información de una organización, así como su reputación, posición legal, personal y otros activos tangibles o intangibles (Nieles et al., 2017, p. 7).

Es probable que la incapacidad de una organización para seleccionar e implementar reglas y procedimientos de seguridad adecuados tenga un impacto negativo en la misión de la organización. Sin embargo, las reglas y procedimientos de seguridad bien elegidos que se implementan para proteger activos importantes respaldan la misión organizacional general (Nieles et al., 2017). En el entorno actual de códigos maliciosos, violaciones del sistema y amenazas internas, los problemas de seguridad que se publicitan pueden tener consecuencias nefastas, especialmente para la rentabilidad y la reputación de la organización. Las organizaciones del sector público y privado mejoran tanto sus ganancias como el servicio a sus clientes cuando existen protecciones de seguridad adecuadas (Nieles et al., 2017). La SI, por lo tanto, “es un medio para un fin y no un fin en sí mismo” (Nieles et al., 2017, p. 7).

La seguridad de información es una de las preocupaciones críticas para las organizaciones modernas. Así, los datos e información organizacionales deben ser protegidos de ataques tanto pasivos como activos, y todas las organizaciones deben asegurar sus datos de acceso ilegal, interrupción no deseada, alteración no autorizada y aniquilación de datos; por lo tanto, la seguridad de información enfatiza la confidencialidad, la integridad y la disponibilidad de la información (Alqathani, 2017). La confidencialidad se refiere a la privacidad, la integridad de mantener la constancia, corrección y dependencia de los datos, y la disponibilidad al acceso a los datos 24/7. Una seguridad de información apropiadamente implementada no solo juega un rol vital en asegurar los datos organizacionales, sino que también provee de métodos para el almacenamiento de los datos (Alqathani, 2017).

2.3.2 Políticas de Seguridad de Información. –

Diversos autores sostienen que la PSI es un documento importante para salvaguardar proactivamente la disponibilidad, confidencialidad e integridad de los activos relacionados con la información corporativa (Doherty et al., 2009; como se citó en Niemimaa, 2017). Más específicamente, se ha discutido que este documento debe “establecer el enfoque de la organización en la gerencia de SI”. Para este fin, una buena PSI debe contener los roles, las responsabilidades, las autorizaciones de uso, y las sanciones y penalidades por incumplimiento (Doherty et al., 2009; como se citó en Fong & Bayona-Oré, 2022).

Consecuentemente, la política debe actuar como el punto de partida para los colaboradores con respecto a todos los problemas de SI, y al hacer eso, se convierte en “el corazón y líder” de la gestión de seguridad exitosa (Doherty et al., 2009; como se citó en Fong & Bayona-Oré, 2022). Por esta razón, y dado que las políticas de seguridad proveen lineamientos formales y recursos

que especifican las responsabilidades de los usuarios al momento de tratar con la información organizacional, los usuarios necesitan acceder al documento de políticas de seguridad para obtener información relevante acerca de sus necesidades de cumplimiento (Pham, 2019).

Definición según la ISO 27001.-

Para el estándar ISO 27001:

El primer propósito que cumple una política de seguridad de información es transmitir los objetivos que la alta dirección se propone alcanzar con la implementación del sistema, mientras que el segundo objetivo del documento es construirlo de manera que resulte fácil de entender para las partes interesadas. (ISOTools Excellence, 09 de abril de 2017, p.1)

Algunas de las observaciones relacionadas a las PSI contenidas en la norma, comprenden:

Adaptabilidad. –

Las políticas deben adecuarse a los requerimientos de la organización, y no al revés. Por lo tanto, se debe descartar la opción de copiar el documento de políticas de otra organización, en especial si los requerimientos de dos entidades de rubros distintos son diferentes. (ISOTools Excellence, 09 de abril de 2017, p.1)

Definición de los Objetivos. – “El documento debe definir los objetivos de seguridad de información, así como su forma de aprobación y la manera en que han de ser revisados” (ISOTools Excellence, 09 de abril de 2017, p.1).

Compromiso. -

Siendo la parte introductoria del documento, la alta dirección debe comprometerse totalmente con el sistema y con su propósito final: cumplir con los requerimientos en materia de seguridad de información de los stakeholders. (ISOTools Excellence, 09 de abril de 2017, p.1)

Comunicación. – “El documento debe establecer quienes son los encargados de comunicar a las partes interesadas los alcances y la evolución del sistema, tanto durante la implementación del mismo como en la medida en que se presenten revisiones, actualizaciones o mejoras” (ISOTools Excellence, 09 de abril de 2017, p.1).

Revisiones. –

La PSI debe ser revisada de forma periódica, y estas revisiones, así como el tiempo en que se realizan, deben ser documentadas. (ISOTools Excellence, 09 de abril de 2017, p.1).

De esta manera, el documento de PSI no necesita detallar los procesos, las verificaciones o las auditorías del sistema, y por ello, mayor brevedad en varios casos puede traducirse en mayor precisión y calidad. (ISOTools Excellence, 09 de abril de 2017, p.1)

Definición según la ISO 27002.-

La norma **ISO 27002** define la PSI como “aquel documento que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa. El contenido de estas políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa, además de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas” (pmg-ssi.com, 03 de agosto de 2017, p.1).

ISO 27002 establece una estructura general de los documentos de PSI:

El resumen debe establecer una visión general de forma breve, que puede incluso combinarse con la introducción (pmg-ssi.com, 03 de agosto de 2017, p.1).

En la introducción se debe explicar el asunto general de la política (pmg-ssi.com, 03 de agosto de 2017, p.1).

En el ámbito de aplicación se describen departamentos, áreas o actividades de una empresa cubiertas por la política, y dependiendo de la relevancia, se pueden mencionan otras políticas relevantes. (pmg-ssi.com, 03 de agosto de 2017, p.1).

En el Objetivo se describe la intención de la PSI (pmg-ssi.com, 03 de agosto de 2017, p.1).

En los Principios:

Se describe las reglas sobre las acciones o decisiones para conseguir los objetivos. Puede ser de utilidad identificar de forma previa los procesos clave que influyen en un aspecto clave de la política para después identificar las reglas de operación de los procesos. (pmg-ssi.com, 03 de agosto de 2017, p.1)

En las Responsabilidades:

Se especifica el responsable de acciones relacionadas a los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, además de las responsabilidades de las personas en los roles asignados. (pmg-ssi.com, 03 de agosto de 2017, p.1)

En Resultados clave se describen “todos los resultados relevantes para las actividades de la empresa” producto del cumplimiento de los objetivos (pmg-ssi.com, 03 de agosto de 2017, p.1).

En las Políticas relacionadas se describirán políticas que son relevantes para alcanzar los objetivos y otros detalles relacionados a temas específicos (pmg-ssi.com, 03 de agosto de 2017, p.1).

La ISO 27002 indica que la gerencia debe establecer de forma clara las líneas de las políticas de actuación e indicar su apoyo y compromiso a la seguridad de información mediante la publicación y mantenimiento de las políticas en toda la organización. (pmg-ssi.com, 03 de agosto de 2017, p.1)

Además, en relación con las PSI, la norma establece dos acciones de control de riesgos:

Definir un conjunto de PSI, mismas que deben ser aprobadas por la alta dirección, publicadas y comunicadas a todos los individuos de la organización y terceros relevantes. (pmg-ssi.com, 03 de agosto de 2017, p.1)

Las PSI deben ser planificadas y revisadas con regularidad, o de ocurrir cambios significativos para garantizar su idoneidad, adecuación y efectividad (pmg-ssi.com, 03 de agosto de 2017, p.1).

Como métricas asociadas a las PSI, ISO 27002 establece dos aspectos fundamentales: Cobertura de la política y Grado de despliegue y adopción.

Definición según COBIT 5:

COBIT 5, en el Capítulo 2, afirma la importancia de un marco GEIT en las organizaciones.

El Consejo de Administración debe ordenar la adopción y adaptación de un marco GEIT, tal como COBIT 5, como una parte integral del desarrollo del gobierno corporativo. Dicho marco establece el enfoque general y, a partir de ahí, se puede usar la orientación proporcionada por normas específicas y buenas prácticas para diseñar políticas, procesos, prácticas y procedimientos específicos,

siendo las políticas, junto con los principios y marcos, uno de los siete catalizadores. (ISACA, 2012, p.15)

Entre dichas políticas se encuentran comprendidas, precisamente, las PSI.

Uno de los procesos que ayudan a guiar la creación y mantenimiento del gobierno y la gestión de los catalizadores es el **EDM01**, que consiste en Asegurar el establecimiento y mantenimiento del marco de gobierno (cultura, ética y comportamiento; principios, políticas y marcos; estructuras organizativas; y procesos). (ISACA, 2012, p.16)

En el Capítulo 5, COBIT indica, sobre el GEIT:

En términos de una implementación típica de GEIT, el objetivo de la habilitación del cambio es que las partes interesadas del negocio y de TI lideren con el ejemplo y animen al personal en todos los niveles a trabajar de acuerdo con la nueva forma deseada, y entre los comportamientos comprendidos en esta nueva forma deseada, figura la aplicación de los principios rectores, las políticas, normas, procesos o prácticas definidos, como una política de seguridad. (ISACA, 2012, p.35)

2.4 Definiciones

En base a los conceptos anteriores, se establecen las siguientes definiciones:

Política regulatoria. - Política también conocida como mandato, que limita la discreción de los individuos y agencias y promueve ciertos tipos de comportamiento (Lowi, 1964, p. 690).

Seguridad de Información. – “Protección de la información y activos de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de salvaguardar su confidencialidad, integridad y disponibilidad” (Nieles et al., 2017, p. 2).

Política de seguridad de información. – “Documento para la SI, cuyo objetivo es proporcionar dirección de gestión y apoyo para la seguridad de la información de acuerdo con los requisitos comerciales y las leyes y regulaciones relevantes” (Niemimaa, 2017, p. 12).

CAPÍTULO 3: ESTADO DEL ARTE

3.1. Revisión de Factores en la Adopción de Políticas de Seguridad

Con el propósito de alcanzar el objetivo de este estudio se realizó una revisión sistemática de literatura, para identificar los artículos referentes a investigaciones realizadas en el periodo 2012 – 2020.

Para realizar la búsqueda de los artículos necesarios para la revisión, se planteó la siguiente pregunta: “¿Qué factores influyen en la adopción de las políticas de seguridad de información?”

En la Tabla 3.1 se presentan los criterios para realizar la revisión.

Tabla 3.1 Criterios para la revisión de artículos

Atributos	Descripción
Población	“Seguridad de Información”
Intervención	Políticas de seguridad de información aplicadas en las organizaciones
Resultados	Modelos elaborados para identificar los factores influyentes en la adopción de las Políticas de Seguridad de Información.
Contexto	Casos de estudio sobre los factores que influyen en la adopción de las Políticas de Seguridad de Información.

Se utilizaron las palabras clave “*factors*” AND “*information security policies*”, como se aprecia en la Tabla 3.2.

Tabla 3.2 Cadena de búsqueda para la revisión de artículos.

Atributos	Descripción
Población	Seguridad de Información

Intervención	‘Information Security Policies’ AND ‘Factors’
Resultados	(Elementos encontrados)
Contexto	Organizaciones privadas y públicas

Los estudios fueron identificados utilizando las palabras claves en las diferentes bases de datos especializados tales como SCOPUS, WILEY, Science Direct, Emerald Insight y Taylor and Francis Online.

3.1.1 Selección de artículos

Finalmente, para excluir los artículos poco útiles para la investigación, se necesitó, mediante su lectura, determinar si los temas de investigación involucraban específicamente a las PSI.

En el proceso de revisión de literatura, que comprendió un total de 53 artículos pertenecientes a investigaciones realizadas entre los años 2012 y 2020, se encontraron diversos modelos y constructos provenientes de teorías y conceptos utilizados por los autores para tratar de determinar los factores clave que influyen en la adopción de las PSI en las organizaciones.

En la Tabla 3.3 se presenta la distribución de la lista de artículos seleccionados por bases de datos.

Tabla 3.3 Artículos seleccionados según base de datos.

Base de datos	Cadena de Búsqueda	Artículos Seleccionados
Emerald Insight		5
Science direct		24
Scopus	‘Information Security Policies’ AND ‘Factors’	16
Wiley		7
Taylor & Francis Online		1

3.1.2. Factores Críticos encontrados en la literatura

La frecuencia de los factores más comunes encontrados en la literatura se presenta en la Tabla 3.4. Los factores mencionados son Actitud del empleado, Autoeficacia, y Normas Personales y

Subjetivas del empleado hacia el cumplimiento de las PSI, Severidad Percibida y Vulnerabilidad Percibida de las Amenazas de Seguridad, Conciencia de las Políticas de Seguridad de Información, Severidad y Certeza de disuasivos / sanciones, Programas de educación, entrenamiento y conciencia de seguridad (SETA) y Conciencia de las Amenazas de Seguridad de Información, entre los más frecuentes.

Tabla 3.4 Factores críticos encontrados en la literatura ordenados por frecuencia.

Factor	Frecuencia	Artículos
Actitud	18	Al-Omari et al. (2013); Ifinedo (2014); Kim (2014); Lee et al. (2016); Safa et al. (2016); Bélanger et al. (2017); D'arcy & Lowry (2019); Hong & Furnell (2019); Nasir et al. (2019); Hina et al. (2019); Amankwa et al. (2018); Dang-Pham et al. (2017); Ifinedo (2018); Kajtazi et al. (2018); Parsons et al. (2014); Sommestad et al. (2015); Hanus et al. (2018); Moody et al. (2018).
Severidad percibida	10	Siponen et al. (2014); Bélanger et al. (2017); Rajab & Eydgahi (2019); Vance et al. (2012); Hina et al. (2019); Addae et al. (2019); Ifinedo (2018); Sommestad et al. (2015); Hanus et al. (2018); Moody et al. (2018).
Autoeficacia	9	Al-Omari et al. (2013); Ifinedo (2014); Vance et al. (2012); Chang & Seow (2019); Nasir et al. (2019); Aurigemma & Mattson (2017); Chen et al. (2018b); Humaidi & Balakrishnan (2018); Hanus et al. (2018).
Normas subjetivas	9	Guo & Yuan (2012); Ifinedo (2014); Bélanger et al. (2017); D'arcy & Lowry (2019); Khan & Alshare (2019); Safa et al. (2019); Yazdanmehr & Wang (2016); Jaeger et al. (2020); Sommestad et al. (2015).
Conciencia de las PSI	8	Chen et al. (2018a); Yazdanmehr & Wang (2016); Sommestad et al. (2019); Koohang et al. (2020); Jaeger et al. (2020); Parsons et al. (2014); van Vuuren et al. (2015); Hanus et al. (2018).
Severidad de disuasivos / sanciones	8	Chen et al. (2018a); Merhi & Ahluwalia (2019); Khan & Alshare (2019); Safa et al. (2019); Trang & Brendell (2019); Jaeger et al. (2020); Alshare et al. (2018); Ifinedo (2016).
Vulnerabilidad percibida	8	Siponen et al. (2014); Bélanger et al. (2017); Hina et al. (2019); Addae et al. (2019); Ifinedo (2018); Sommestad et al. (2015); Hanus et al. (2018); Moody et al. (2018).
Programa SETA	8	Han et al. (2017); Lowry et al. (2015); Kim et al. (2019); Hina et al. (2019); Abdelwahed et al. (2016); Da Veiga & Martins (2015a); Da Veiga & Martins (2015b); van Vuuren et al. (2015).
Certeza de disuasivos / sanciones	5	Merhi & Ahluwalia (2019); Safa et al. (2019); Hong & Furnell (2019); Trang & Brendell (2019); Willison et al. (2018).

Normas Personales	5	Guo & Yuan (2012); Ifinedo (2014); Yazdanmehr & Wang (2016); Jaeger et al. (2020); Ifinedo (2018).
Apoyo de la gerencia	4	Khan & Alshare (2019); Abdelwahed et al. (2016); Humaidi & Balakrishnan (2018); Ifinedo (2016).
Compromiso Organizacional	3	Ifinedo (2014); Safa et al. (2016); Chol & Song (2018).
Cultura Organizacional de Seguridad	3	Khan & Alshare (2019); Nasir et al. (2019); Alshare et al. (2018).
Conciencia de las Amenazas de SI	2	Chen et al. (2018a); Hanus et al. (2018).

3.1.3. Definición de los factores encontrados en la literatura

En la Tabla 3.5 se presentan las definiciones de los factores.

Tabla 3.5 Definiciones de los factores según autores

Factor	Definición	Autor
Severidad de sanciones	Creencia del individuo que será castigado por su comportamiento delincuencia.	Safa et al. (2019)
Certeza de sanciones	Creencia del individuo que un acto delincuencia será detectado por la autoridad pertinente.	Safa et al. (2019)
Compromiso organizacional	Fuerte creencia y aceptación de los valores y objetivos de la organización, una voluntad de dedicar esfuerzo en nombre de la misma, y un fuerte deseo de mantenerse como uno de sus miembros.	Ifinedo (2014)
Actitud del empleado	Sentimientos positivos o negativos experimentados por el empleado cuando cumple con las PSI.	Lee et al. (2016)
Autoeficacia de Seguridad	Capacidades y competencias del individuo para seguir las políticas de PSI y llevar a cabo las tareas, influenciadas por la habilidad del empleado de trabajar con sistemas de computador en general y el apoyo de la gerencia.	Chen et al. (2018a)
Severidad percibida de amenazas	Percepción del grado de daños físicos y psicológicos que puede causar un problema de seguridad de información.	Siponen et al. (2014)
Vulnerabilidad percibida de amenazas	Percepción de un individuo de cómo una amenaza de seguridad tomará lugar si no se toman medidas para contrarrestarla.	Siponen et al. (2014)
Conciencia de políticas de seguridad de información	Conocimiento y entendimiento del empleado de los requerimientos prescritos en las PSI de la organización y los objetivos de dichos requerimientos.	Chen et al. (2018a)
Programa SETA	Proceso educativo por el cual los empleados cumplen las condiciones necesarias para la seguridad de información en la organización y ayuda a los empleados a trabajar en un ambiente ético y seguro y a reconocer las amenazas y vulnerabilidades de los sistemas de información en sus organizaciones.	Han et al. (2017)
Cultura de seguridad organizacional	Establecimiento de políticas, estándares, entrenamiento y programas educativos de seguridad de información en la organización por parte de la alta gerencia.	Khan & Alshare (2019)

3.1.4. Discusión

Al finalizar la revisión sistemática, se han encontrado varios aspectos interesantes. La mayoría de investigaciones poseen un enfoque cuantitativo, lo que se refleja en la cantidad de artículos que realizaron sus correspondientes revisiones de literatura y utilizaron métodos estadísticos para probar sus hipótesis. Asimismo, la mayoría de estos estudios tienen alcances correlacional y explicativo, lo que indica la necesidad de conocer cómo influyen los factores en la adopción de las PSI, y responder por las causas de la pobre adopción de estas políticas, respectivamente. Finalmente, la mayoría de investigaciones provienen de Estados Unidos (siendo este país el que presenta la mayor cantidad), Corea del Sur, Malasia, Canadá y Finlandia, lo que implica que estos países han presentado la mayor frecuencia de brechas de seguridad y, por consiguiente, la necesidad de llevar a cabo estas investigaciones.

CAPÍTULO 4: HIPÓTESIS

4.1 Hipótesis General

Existen una serie de factores de éxito que influyen en la adopción de las PSI en las organizaciones.

4.2 Hipótesis Específicas

4.2.1 Severidad de Sanciones

Se entiende por severidad de sanciones a la creencia que el individuo será castigado por su comportamiento delincuencia (Safa et al., 2019). Una teoría que trata la severidad de sanciones es la Teoría de Disuasión (DT), que sostiene que “los individuos sólo son disuadidos de cometer actos criminales si perciben que las sanciones legales son certeras, rápidas y/o severas”. Esta teoría ha sido aplicada para evaluar si factores de penalidad, como la severidad pueden prevenir comportamientos contrarios a la adopción de las políticas de seguridad (Chen et al., 2018a). Por lo tanto, se espera que las sanciones sean lo suficientemente severas para evitar que los colaboradores violen las PSI.

La Teoría de Motivación de Protección (PMT) es la teoría que explica que la motivación para un acto está influenciada en el contexto de cumplimiento de las PSI por dos tipos de factores extrínsecos: recompensas (evaluación de beneficios) y penalidades (evaluación de costos) (Chen et al., 2018a). Tanto esta teoría como la DT indican que las sanciones pueden disuadir el incumplimiento; por lo tanto, las sanciones pueden considerarse como la motivación de los colaboradores a no cometer infracciones descritas en las PSI de su organización (Chen et al., 2018a).

En el contexto de las PSI, los tipos de sanción pueden variar y ser categorizados en sanciones formales e informales (Guo & Yan, 2012, como se citó en Trang & Brendell, 2019; Johnson, 2015, como se citó en Trang & Brendell, 2019). Se ha demostrado que las sanciones formales, tales como recortes de sueldo y reseñas negativas de desempeño, poseen un impacto mayor en las intenciones de mal comportamiento (Jaeger et al., 2020). Sin embargo, en muchas situaciones, las sanciones no actúan como un disuasivo directo (Merhi & Ahluwalia, 2019), como es el caso de personas que creen que existen pocas posibilidades de detección de sus violaciones de políticas de seguridad. Más aún en el caso de escenarios organizacionales donde las personas no están reguladas extensivamente por su uso de las TI, por lo que las sanciones no afectan directamente su comportamiento PSI. En algunas instancias, se ha encontrado que la severidad de sanciones influye negativamente y de forma directa en las intenciones de mal comportamiento relacionado a la seguridad de información (Chen et al., 2018a).

La noción de que los factores de castigo impactan en las normas descriptivas tiene una base teórica en la Teoría de Aprendizaje Social (Bandura, 1971, como se citó en Merhi & Ahluwalia, 2019). Esta teoría sostiene que los individuos ajustan su propio comportamiento aprendiendo de otros, considerando que comportamiento incluye en penalidades y cuál no.

Sin embargo, otros estudios empíricos discuten la aplicabilidad universal de esta teoría. Por ejemplo, Tyler (1990, como se citó en Merhi & Ahluwalia, 2019) afirma que el miedo al castigo no es la única razón del cumplimiento de las leyes y políticas, y que la perspectiva normativa ofrece una explicación del comportamiento de cumplimiento basado en dos dimensiones: legitimidad y moralidad. La legitimidad afirma que aquellos que han internalizado las políticas son competentes de hacerlo. La perspectiva de moralidad, por su parte, está apoyada en las creencias internas del individuo en lugar de una medida cognitiva de ganancias y pérdidas (Merhi & Ahluwalia, 2019). Apoyados en la perspectiva de legitimidad, las sanciones pueden ayudar a formar el entendimiento compartido (normas) de cómo se deben llevar a cabo diversas sanciones, y así generar un efecto indirecto en el comportamiento. Por ende, si las sanciones se usan como disuasivos legítimos, comunican claramente el comportamiento inaceptable a los miembros (Merhi & Ahluwalia, 2019).

La Teoría de Decisión Racional (RCT) indica que los violadores potenciales de las PSI serían disuadidos si comprendiesen que serán severamente castigados de ser detectados, dado que las sanciones en cuestión elevan el costo del incumplimiento de la política en comparación con los beneficios percibidos y, por lo tanto, no estarían dispuestos a violar la política (Alshare et al., 2018).

Teniendo en cuenta la importancia en la intención de cumplimiento de los individuos de las PSI dada la severidad de sanciones, se plantea la hipótesis:

- **H1:** *La severidad de sanciones influye en la intención de cumplimiento de las PSI en las organizaciones.*

4.2.2 Certeza de Sanciones

La certeza de sanciones se entiende, con base a la Teoría de Disuasión, como la creencia del individuo que un acto delictivo será detectado por la autoridad competente (Safa et al., 2019). Dicha teoría sugiere que si las personas consideran tanto la posibilidad de ser atrapados (certeza disuasoria) como la severidad del castigo si uno es atrapado (severidad disuasoria) son altas, tienden a no cometer delitos (Blumstein et al., 1978, como se citó en Hong & Furnell, 2019). Straub introdujo por primera vez la teoría de disuasión en el campo de la SI, y es una de las teorías más populares aplicadas en este campo, dado que sirve para explicar la ocurrencia de comportamientos no deseados, como se ve en los hallazgos de Straub sobre cómo la certeza y la gravedad disuasorias pueden reducir significativamente los comportamientos de abuso informático (Straub, 1990, como se citó en Hong & Furnell, 2019).

En la literatura concerniente a la seguridad de información, Henle & Blanchard (2008, como se citó en Safa et al., 2019) demostraron que la certeza de las sanciones disminuye la holgazanería cibernética y el abuso del equipo organizativo. De igual forma, Kankanhalli et al. (2003, como se citó en Hong & Furnell, 2019) demostraron que la certeza de las sanciones puede disuadir a las personas de cometer abusos contra la seguridad de información al aumentar la probabilidad de que sean sorprendidas.

Otros estudios previos postularon que los factores de castigo organizacional, como la certeza de castigos, influyen positivamente en cumplir con las PSI (Bulgurcu et al., 2010, como se citó en Merhi & Ahluwalia, 2019; D'Arcy et al., 2009, como se citó en Merhi & Ahluwalia, 2019; Straub, 1990, como se citó en Merhi & Ahluwalia, 2019). Estos estudios, sin embargo, informaron hallazgos inconsistentes; algunos encontraron que la certeza de castigos era un antecedente significativo de las intenciones de cumplimiento de los empleados, y otros informaron que el castigo no tenía ningún efecto sobre la intención de cumplimiento (Herath & Rao, 2009a; 2009b, como se citó en Merhi & Ahluwalia, 2019; Pahnla et al., 2007, como se citó en Merhi & Ahluwalia, 2019). En otras investigaciones, se ha encontrado que la certeza de sanciones no tiene un impacto directo en dichas intenciones de violar las PSI (Chen et al., 2018a).

Tomando en cuenta la importancia de la certeza de sanciones en la intención de cumplimiento y finalmente la adopción de las PSI se plantea las hipótesis:

- **H2:** *La certeza de sanciones influye en la intención de cumplimiento de las PSI en las organizaciones.*
- **H3:** *La certeza de sanciones influye en la adopción de las PSI en las organizaciones.*

4.2.3 Compromiso Organizacional

El compromiso organizacional se define como un contrato implícito entre un individuo y su organización que establece expectativas sobre dar y recibir en su relación. La definición más usada derivada de este contrato es la creencia de un individuo acerca de las obligaciones mutuas existentes entre el individuo y su organización (Han et al., 2017).

Porter et al. (1979, como citó en Ifinedo, 2014) ha caracterizado al compromiso organizacional como “una fuerte creencia y aceptación de los valores y objetivos de la organización, una voluntad de dedicar esfuerzo en nombre de la organización, y un fuerte deseo de mantener su membresía en la organización”. Según Cheng et al. (2013, citado en Safa et al., 2016) el compromiso se refiere a “la aspiración de adquirir un alto status en el trabajo, por lo que los logros personales y la reputación son importantes para una persona comprometida”.

De acuerdo con esto, un empleado con fuertes creencias en los valores y metas de su organización, incluyendo aquellas relacionadas con las PSI, formará y mantendrá actitudes positivas acerca de la importancia de dichas reglas y lineamientos (Ifinedo, 2014).

Considerando que los individuos son claves en la SI, su responsabilidad y compromiso juegan un rol vital en este dominio, luego las personas con alto compromiso organizacional (1) no tomarían el riesgo de romper reglas (Lee et al., (2004, como se citó en Safa et al., 2016), (2) tienen menores posibilidades de desviarse de las políticas de seguridad (Safa et al., 2016), (3) disuaden a las personas del no cumplimiento (Chol & Song, 2018) y (4) van a estar menos dispuestas a tener comportamientos contraproducentes y pongan en riesgo a su organización (Sharma & Warkentin, 2019).

Tomando en cuenta la importancia del compromiso en la actitud del empleado hacia el cumplimiento y finalmente la adopción de las PSI se plantea la hipótesis:

- **H4:** *El compromiso organizacional influye en la actitud del empleado hacia las PSI en las organizaciones.*

4.2.4 Actitud del Empleado

La actitud del individuo hacia el cumplimiento de las PSI se define como los sentimientos experimentados por el mismo cuando cumple con las PSI y dicha actitud puede ser positiva o negativa (Lee et al., 2016). Esta actitud puede ser influenciada por las visiones de los individuos y grupos referentes, según las normas subjetivas del empleado, de esta forma, si las visiones del grupo son positivas, la actitud del individuo será a su vez positiva (Ifinedo, 2014; Hong & Furnell, 2019).

La actitud del empleado se considera como “el grado de apoyo o falta de apoyo expresado por los usuarios finales acerca de las PSI” (Bélanger et al., 2017). Se puede dar casos de no cumplimiento de las PSI si los empleados piensan que las mismas afectan su productividad y culparán a las PSI, de tal forma que su insatisfacción con las PSI los conducirá al no cumplimiento (Chang & Seow, 2019). La actitud del empleado con respecto a las PSI está influenciada por la conciencia que posee acerca de las PSI (Koohang et al., 2020). La actitud del individuo está influenciada por la evaluación que realiza sobre objetos, personas, actividades, eventos e ideas que pueden cambiar de muy positivo a muy negativo (Safa et al., 2016).

La actitud es un constructo de la Teoría de Comportamiento Planeado (TPB) y es un predictor fuerte de la intención de una persona de optar por el cumplimiento de las PSI (Sommestad et al., 2019; D’arcy & Lowry, 2019; Hina et al., 2019).

La creencia sobre el cumplimiento de las PSI afecta la actitud de cumplimiento de las PSI (Ajzen, 1991, como se citó en Kim et al., 2014; Bulgurcu et al., 2010 como se citó en Kim et al., 2014). Las creencias y valores positivos con respecto a las PSI pueden producir una tendencia a cumplir con las normas y requerimientos de una organización (Lee et al., 2016; Safa et al., 2019).

Para la Teoría de Decisión Racional (RCT), tanto la actitud como la creencia se basan en las consideraciones del individuo sobre los costos (o sacrificios) y beneficios de la acción, por lo que la actitud del individuo será más favorable si los beneficios del cumplimiento son mayores que los costos de cumplimiento (Gwebu et al., 2020).

Asimismo, establecer una cultura de SI a través de la organización influenciará en la actitud de los colaboradores para mantener los objetivos de seguridad (Nasir et al., 2019).

En este proceso, se educará y mejorará los conocimientos, la conciencia y las habilidades de los empleados para tratar con activos de la información, dado que formulará un pensamiento normalizado y modo de comportamiento y comprensión de la precaución para hacer progresar el nivel de habilidades de los empleados correctamente (Nasir et al., 2019).

Tomando en cuenta la importancia de la actitud del empleado hacia el cumplimiento y finalmente la adopción de las PSI se plantea las hipótesis:

- **H5:** *La actitud del empleado influye en la cultura de seguridad organizacional.*
- **H6:** *La actitud del empleado influye en la intención de cumplimiento de las PSI en las organizaciones.*
- **H7:** *La actitud del empleado influye en la adopción de las PSI en las organizaciones.*

4.2.5 Autoeficacia de Seguridad

La autoeficacia se refiere a las capacidades y competencias del individuo para tratar con una tarea o tomar una decisión. En el contexto de las PSI, un empleado debe tener la capacidad de seguir las políticas y llevar a cabo las tareas (Chen et al., 2018a). En estos términos, es lógico esperar que los individuos con altas capacidades para tratar con tareas de seguridad se verán en la necesidad de seguir las PSI y, por consiguiente, serán más capaces de entender los peligros del no cumplimiento (Ifinedo, 2014). De lo anterior, la creencia de los empleados que pueden cumplir con éxito las PSI, puede incrementar el cumplimiento de dichas políticas (Vance et al., 2012).

Un aspecto importante de la autoeficacia del empleado es la familiaridad del mismo con las PSI, dado que, si los usuarios están familiarizados con las políticas, su trabajo puede ser llevado a cabo sin problemas. Después de que las PSI se aplique en la organización, los usuarios pueden sentirse incompetentes debido a su falta de familiaridad con las mismas, lo que puede deteriorar su actitud hacia el cumplimiento efectivo de dichas políticas (Chang & Seow, 2019). De la misma forma, según Shu et al. (2011, citado en Pham, 2019) “los empleados que cuentan con una alta autoeficacia de seguridad tendrán la intención de superar las complejidades de las tareas de seguridad y ocuparse de ellas más positivamente, evitando el desgaste de seguridad de información”.

La adaptación es un aspecto importante de la autoeficacia, debido a que se refiere al grado de preparación para cumplir con las PSI, y engloba un rango amplio de comportamientos dirigidos a una gran variedad de demandas de trabajo; por ello, la habilidad de adaptarse efectivamente al ambiente cambiante y a cultura de la organización es un factor importante en el desempeño del empleado (Lee et al., 2016).

La relación entre la autoeficacia y el control de comportamiento se hace más evidente cuando se toma en cuenta que dicho control de comportamiento se relaciona a la creencia que involucrarse en comportamientos de seguridad de información y prevenir la mala conducta de seguridad de información no son tareas difíciles (Safa et al., 2019). En algunos casos, la autoeficacia es utilizada como un antecedente que contribuye al control de comportamiento percibido; es decir, si un empleado siente que puede controlar a sus compañeros junto con alta autoeficacia, entonces, tendrá un mayor control de comportamiento percibido de PSI (Aurigemma & Mattson, 2017).

Por otro lado, la autoeficacia se complementa con la eficacia de respuestas a amenazas de seguridad debido a que ambas son factores de medición de tratamiento (Hina et al., 2019).

Tomando en cuenta la importancia de la autoeficacia de seguridad hacia el cumplimiento y finalmente la adopción de las PSI se plantea las hipótesis:

- **H8:** *La autoeficacia de seguridad influye en la conciencia de las PSI en las organizaciones.*
- **H9:** *La autoeficacia de seguridad influye en la intención de cumplimiento de las PSI en las organizaciones.*
- **H10:** *La autoeficacia de seguridad influye en la adopción de las PSI en las organizaciones.*

4.2.6 Severidad Percibida de Amenazas

La severidad percibida de amenazas forma parte de la Teoría de la Motivación de Protección (PMT). La medida de amenazas evalúa el miedo que ocurre debido a la percepción de un individuo de sus sentimientos de amenaza ante una determinada situación. De esta forma, la severidad percibida se define como el grado de daños físicos y psicológicos que puede causar un problema de seguridad de información (Siponen et al., 2014; Addae et al., 2019). En el campo de la SI, la severidad percibida, es una medida de qué tan susceptible es la organización del empleado, a las brechas de seguridad de información y al daño potencial (Vance et al., 2012; Siponen et al., 2014). De esta forma, “la medida del grado en el cual una amenaza puede dañar a un individuo motiva a la persona a cumplir con el comportamiento adecuado” (Hina et al., 2019, p.6).

Johnston & Warkentin (2010, como se citó en Siponen et al., 2014) investigaron el efecto de argumentos inductores de miedo en el cumplimiento de las PSI. Los autores se basaron en una extensión de la PMT para postular que la eficacia de respuestas, la autoeficacia y la influencia social tendrían un efecto positivo en las intenciones de los empleados de adoptar medidas de seguridad de información.

Otras investigaciones, como las realizadas por Anderson & Agarwal (2010, como se citó en Bélanger et al., 2017) y Herath et al. (2014, como se citó en Bélanger et al., 2017) sugieren que la percepción de severidad de amenazas afecta la actitud hacia los comportamientos de seguridad.

Tomando en cuenta la importancia de la severidad percibida de amenazas hacia el cumplimiento de las PSI se plantea las hipótesis:

- **H11:** *La severidad percibida de amenazas influye en la intención de cumplimiento de las PSI en las organizaciones.*

4.2.7 Vulnerabilidad Percibida de Amenazas

Uno de los componentes de la teoría de la motivación de protección (PMT) es la vulnerabilidad percibida de amenazas, dado que la medida de amenazas se preocupa con el proceso de evaluar el miedo que ocurre debido a la percepción de un individuo de sus sentimientos de amenaza debida a una determinada situación.

La vulnerabilidad percibida se refiere a como se siente un individuo ante un evento negativo que tomará lugar, si no se toman medidas para contrarrestarlo (Siponen et al., 2014; Addae et al., 2019). En el campo de la SI, esta es una medida de la susceptibilidad de la organización del empleado a las brechas de seguridad de información y al daño potencial ocurrido producto de las mismas (Vance et al., 2012; Siponen et al., 2014).

Anderson & Agarwal (2010, como se citó en Bélanger et al., 2017) sugieren que la actitud hacia los comportamientos de seguridad está afectada por la percepción de la severidad de amenazas y la percepción de la vulnerabilidad de las mismas.

En contraste, Herath & Rao (2009, como se citó en Rajab & Eydgahi, 2019) concluyeron que la vulnerabilidad de amenazas no explica la diferencia del cumplimiento de políticas de seguridad entre los empleados.

Teniendo en cuenta la importancia de este factor hacia el cumplimiento de las PSI se plantea la hipótesis:

- **H12:** *La vulnerabilidad percibida de amenazas influye en la intención de cumplimiento de las PSI en las organizaciones.*

4.2.8 Conciencia de las Políticas de Seguridad de Información

La conciencia de las PSI puede ser definido como “el conocimiento y entendimiento del empleado de los requerimientos prescritos en las PSI de la organización y los objetivos de esos requerimientos” (Chen et al., 2018a; Sommestad et al., 2019; Koohang et al., 2020; Jaeger et al., 2020).

La conciencia de las PSI es una parte vital de un programa de gerencia de SI práctico y eficiente, según Lee & Lee (2002, como se citó en Koohang et al., 2020). La conciencia es un estado en el cual un empleado está consciente y comprometido idealmente a los objetivos de SI de la organización, expresados a menudo en las PSI (Jaeger et al., 2020). Al respecto, Lee & Lee (2002, como se citó en Koohang et al., 2020) indican que, en las organizaciones, la conciencia de las PSI previene el mal uso de computadoras.

Dado que este tipo de conciencia involucra el conocimiento del empleado, una de las mejores formas de incrementar la conciencia de PSI es el compartir el conocimiento de SI, dado que los expertos afrontan problemas similares en este dominio y deben proveer de soluciones apropiadas (Safa et al., 2016).

La conciencia es un constructo importante que debe ser considerado en el contexto de comportamientos hacia la SI, como es el caso de los cambios e implementaciones de PSI. Los individuos necesitan un conocimiento básico del cambio esperado antes de que puedan llevarlo a cabo (Bélanger et al., 2017). Se ha encontrado que los individuos no cumplen con las PSI debido a la falta de conciencia (Bulgurcu et al., 2010 como se citó en Bélanger et al., 2017).

La conciencia de PSI puede dar lugar a un hábito, debido a que, según la Teoría del Hábito, la iniciación de un nuevo patrón de comportamiento requiere una decisión consciente y el nuevo comportamiento gradualmente se volverá más automático (Vance et al., 2012). Las señales que generan dicho comportamiento automático son numerosas, claras y consistentes, por lo que la conciencia de amenazas da inicio al proceso cognitivo, que a su vez lleva a la intención de comportamiento (Vance et al., 2012).

D'Arcy et al. (2009, citado por Han et al., 2017) indica que es importante que las organizaciones sepan cómo los empleados perciben las PSI en la organización, tales como las reglas e indicaciones para el uso de los recursos de SI organizacionales, dado que esto puede actuar como el primer paso en disuadir las faltas de SI.

Tomando en cuenta la importancia de la conciencia de las PSI hacia el cumplimiento de las PSI se plantea las hipótesis:

- **H13:** *La conciencia de las PSI influye en la adopción de las PSI en las organizaciones.*

4.2.9 Programa SETA

Un programa SETA es un proceso educativo por el cual los empleados cumplen las condiciones necesarias para la seguridad de información en la organización, y ayuda a los empleados a trabajar en un ambiente ético y seguro y a reconocer las amenazas y vulnerabilidades de los sistemas de información en sus organizaciones. Como tal, un programa SETA provee a los individuos de conocimiento y crear conciencia para la seguridad de información (Han et al., 2017). Estos programas les brindan a las empresas la habilidad de reducir la discrepancia entre las percepciones y la realidad, y pueden ser especialmente efectivos si informan a los empleados acerca de sus roles y expectativas alrededor de los mismos en el cumplimiento de los requerimientos de SI (Lowry et al., 2015). Existen tres objetivos a alcanzar mediante la implementación de estos programas: hacer que los empleados estén conscientes de que las amenazas existen, entrenar a los empleados en cómo llevar a cabo su trabajo de forma segura, y educar a los empleados sobre por qué estas amenazas existen (Lowry et al., 2015). La instrucción de estos programas se lleva usualmente a cabo mediante la persuasión verbal; los individuos reciben sugerencias de los instructores que animan y apoyan sus habilidades de seguridad de información y acogen el desarrollo responsable. Dado que los individuos que reciben este empoderamiento tienen más probabilidades de creer que pueden llevar a cabo competentemente tareas de seguridad de información, tendrán más posibilidades de mostrar sentimientos positivos hacia el cumplimiento de estas tareas, lo cual a su vez incrementa la motivación para llevar a cabo las acciones necesarias para llevar a cabo las tareas (Dhillon et al., 2020).

A lo largo de los años, las investigaciones han encontrado que los programas SETA afectan positivamente la conciencia de seguridad de información de los empleados y las intenciones de cumplimiento y comportamiento, como lo evidencian Chan et al. (2005, como se citó en Kim et al., 2019), Haeussinger & Kranz (2013, como se citó en Kim et al., 2019) y Siponen (2000, como se citó en Kim et al., 2019), por lo que las organizaciones pueden mejorar el cumplimiento de las PSI de sus empleados realizando continuamente programas de entrenamiento y comunicando con ellos (Kim et al., 2019). Así, los programas SETA ahora son considerados una necesidad básica en las organizaciones con el fin de tomar decisiones de seguridad bien informadas cuando se necesitan (Hina et al., 2019). Aunque la literatura discute que los programas SETA pueden ser distintos en su naturaleza y resultados en términos de enfoque, propósito y métodos, si son apropiadamente implementados, pueden educar a los empleados en las vulnerabilidades de los recursos humanos y de computador, la severidad potencial de brechas de seguridad y contramedidas importantes (Hina et al., 2019).

Tomando en cuenta la importancia de este factor hacia el cumplimiento de las PSI se plantean las hipótesis:

- **H14:** *Los programas SETA influyen en la cultura de seguridad organizacional.*

- **H15:** *Los programas SETA influyen en la intención de cumplimiento de las PSI en las organizaciones.*

4.2.10 Cultura de Seguridad Organizacional

Este factor involucra el establecimiento de políticas, estándares, entrenamiento y programas educativos (Khan & Alshare, 2019). Chang & Lin (2007, como se citó en Alshare et al., 2018) recuerdan que la SI no solo es un problema técnico, sino también un problema de gerencia, y requiere la participación de la alta gerencia en establecer dichas políticas, estándares y procedimientos.

Khan & Alshare (2019) sostienen que construir la cultura de seguridad inicia por generar conciencia de los problemas de seguridad y para ello se debe proveer de recursos para reaccionar y promover la comunicación en ambos sentidos entre el personal de seguridad, gerentes y empleados. Es más, “la construcción de una cultura de seguridad debe ser considerada una inversión a largo plazo, misma que requiere un esfuerzo constante para mantener y desarrollar” (Khan & Alshare, 2019, p.9).

Por estas razones, cuando una compañía cuenta con una cultura de seguridad organizacional, los empleados están conscientes de las políticas a través de esfuerzos educativos, así como las declaraciones claras de penalidades por violaciones (Alshare et al., 2018). Asimismo, al tener conocimiento mejora las habilidades necesarias para la SI (Han et al., 2017).

Otra influencia notable es el clima ético presente en las organizaciones, con un sistema fuerte de normas sociales, que mantienen informados a los miembros de la organización sobre el qué hacer y qué esperar de otros y que sirve de referencia útil de información para el comportamiento eficiente de cumplimiento de lineamientos (Yazdanmehr & Wang, 2016).

De acuerdo con Kolkowska (2011, como se citó en Nasir et al., 2019), la mayoría de estudios de cultura de seguridad de información suponen que desarrollar una cultura de SI cambiará el comportamiento y valores de seguridad de los empleados de tal forma que cumplan con las PSI organizacionales. Asimismo, Glaspie & Karwowski (2018, como se citó en Nasir et al., 2019) discutieron que, en la mayoría de investigaciones, se destacó que una cultura de SI positiva puede incrementar el cumplimiento de las PSI.

Tomando en cuenta la importancia de la cultura de seguridad de la información hacia el cumplimiento de las PSI se plantea la hipótesis:

- **H16:** *La cultura de seguridad organizacional influye en la adopción de las PSI en las organizaciones.*

4.2.11 Conocimiento de Políticas de Seguridad

Otro factor que contribuyen al no cumplimiento de las PSI es el conocimiento que pueden tener los colaboradores de las PSI. Según la ISO 27002, el control relacionado con la PSI establece que la PSI debe ser publicada en diferentes medios y comunicada a todos los colaboradores de la organización y a las partes interesadas. Las PSI deben estar claramente establecidas y la Alta Dirección debe mostrar compromiso para su publicación y mantenimiento a través de la organización.

Se han realizado estudios sobre la relación significativa entre conocimiento y actitud en una variedad de campos (Shepherd y DeTienne, 2005, como se citó en Lee et al., 2016; Zhu & Chang, 2015, como se citó en Lee et al., 2016). Se ha informado que las diferencias en el comportamiento de los individuos están condicionadas por sus niveles de conocimiento previos (Hallahan, 2001, como se citó en Lee et al., 2016). Green (2004, como se citó en Lee et al., 2016) estudió el conocimiento previo en términos de familiaridad (el estado de poseer mucho conocimiento sobre una situación), encontrando que es probable que la familiaridad sea más poderosa en la formación de actitudes porque los individuos pueden aprovechar su propia y rica experiencia personal y no necesitan confiar únicamente en la información obtenida recientemente. Por lo tanto, los empleados con conocimientos previos de seguridad se sienten familiarizados con las actividades de cumplimiento de SI de su empresa.

Para determinar la forma en que el conocimiento de las PSI afecta la actitud del empleado y la intención de cumplimiento se plantean las hipótesis:

- **H17:** *El conocimiento de las políticas de seguridad influye en la actitud del empleado hacia las PSI en las organizaciones.*
- **H18:** *El conocimiento de las políticas de seguridad influye en la intención de cumplimiento de las PSI en las organizaciones.*

4.2.12 Intención de Cumplimiento

La intención del cumplimiento se refiere a la determinación de los empleados a adoptar las PSI, y comprometerse a cumplir desde el presente al futuro. Diversos estudios muestran que la

intención conduce al comportamiento deseado. Por ejemplo, la Teoría de Acción Razonada (TRA) sostiene que “cuanto mayor es la intención de participar en un comportamiento, mayor será la probabilidad de que el comportamiento se lleve a cabo”. En relación con el cumplimiento de las PSI, “la actitud de un empleado hacia el cumplimiento de estas políticas, combinada con las normas sociales, hará que el empleado tenga la intención de cumplir con las políticas de seguridad; conduciendo al cumplimiento real de las políticas” (Siponen et al., 2014).

La intención representa el compromiso de realizar una acción, ya sea ahora o en el futuro, y contiene el concepto de planificación y previsión (Hau et al., 2013, como se citó en Safa et al. 2019). El deseo de alcanzar una meta que brinde satisfacción a una persona genera una intención de participar en un comportamiento que promueva el alcance de esa meta en dicha persona.

Diversos estudios de SI se centraron en la intención del comportamiento en lugar de probar el comportamiento real (Crossler et al. 2013, como se citó en Bélanger et al., 2017). Esto a menudo se justifica con estudios de adopción de tecnología, que sugieren que la intención eventualmente conduce al comportamiento. Sin embargo, en el contexto de la SI, medir la intención por sí sola puede ser problemático porque, en realidad, las intenciones no siempre conducen a comportamientos reales (Straub, 2009, como se citó en Bélanger et al., 2017; Anderson y Agarwal, 2010, como se citó en Bélanger et al., 2017).

Para determinar la forma en que la intención de cumplimiento influye en la adopción de las PSI se plantea la hipótesis:

- **H19:** *La intención de cumplimiento influye en la adopción de las PSI en las organizaciones.*

De las hipótesis planteadas se construye el modelo de investigación que se presenta en la sección 4.3.

Asimismo, en el Anexo I se presenta la matriz de consistencia.

4.3 Propuesta de Modelo

El modelo propuesto para esta investigación se presenta en la Figura 4.1.

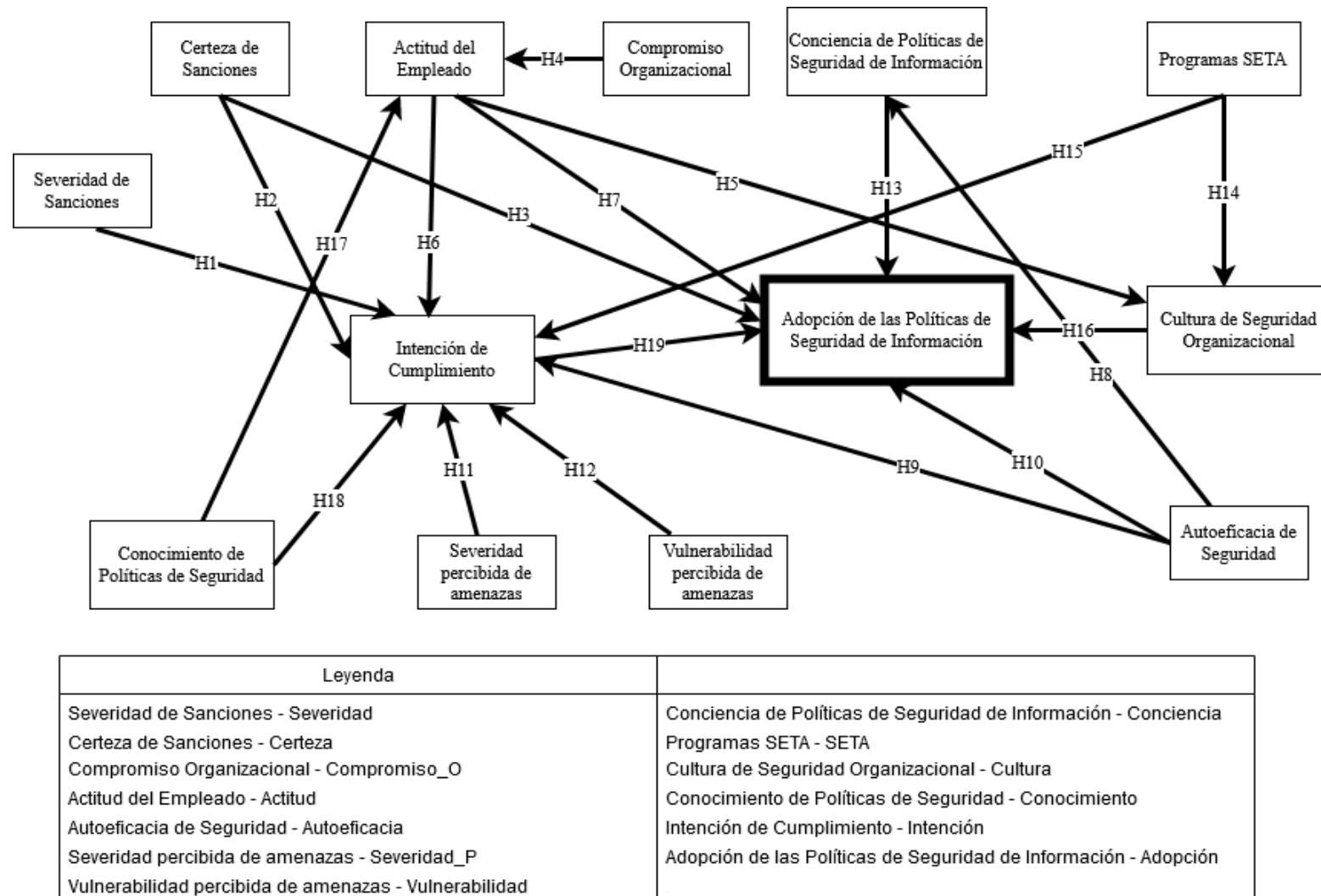


Fig. 4.1 Modelo propuesto de la investigación.

CAPÍTULO 5: METODOLOGÍA

5.1 Tipo de Investigación

La investigación posee un enfoque cuantitativo, dado que utiliza métodos sistemáticos, empíricos y críticos de investigación con el fin de hacer inferencias partiendo de toda la información recabada y entender a fondo las causas que determinan el éxito de las PSI. La investigación está diseñada para ser llevada a cabo de forma descriptiva y explicativa.

5.2 Unidad de Análisis

Profesional del área de seguridad de tecnologías de información de empresas (o quien haga de las veces) ubicadas en Lima.

5.3. Población de Estudio

Conformada por los Profesionales del área de seguridad de tecnologías de información de instituciones de administración pública y empresas privadas en ubicadas en Lima.

5.4. Tamaño de Muestra

La muestra del estudio es no probabilística por conveniencia representada por 108 profesionales del área de seguridad de la información de las empresas ubicadas en Lima, que contaban con experiencia profesional igual o mayor a 3 años.

De un total de 364 invitaciones a participar en la encuesta, se contó con la participación de 108 profesionales del área de seguridad de tecnologías de información.

5.5. Técnicas de Recolección de Datos

Para recolectar los datos, se utiliza una encuesta dirigida a los profesionales de seguridad de TI en las empresas. Las preguntas de esta encuesta se basan en los factores estipulados en las hipótesis y los objetivos de la investigación, y las respuestas se encuentran distribuidas en una escala de Likert comprendiendo desde 1 (nunca) hasta 5 (siempre).

La encuesta está basada en los trabajos de los autores Son (2011), Chen et al. (2016), Safa et al. (2016), Ifinedo (2014), Hina et al. (2019) y Nasir et al. (2019) y se encuentra en el Anexo II.

5.6. Técnicas de Análisis de Datos

Para realizar el análisis de los datos se utilizó el software estadístico SPSS v23 y AMOS v23.

Para probar la confiabilidad y validez de las variables se utilizó el método de modelamiento de ecuaciones estructurales (SEM).

CAPÍTULO 6: RESULTADOS Y DISCUSIÓN

6.1 Análisis y Presentación de Resultados

Tras el desarrollo de la encuesta dirigida a 108 profesionales del área de seguridad de información, se obtuvieron los siguientes resultados:

6.1.1 Datos demográficos de la población

En esta sección se presenta el análisis de los resultados de la encuesta de 108 participantes:

Sexo. –

En la Tabla 6.1 se presenta la frecuencia de participantes en la encuesta respecto al sexo.

Tabla 6.1 Frecuencia de participantes en la encuesta con respecto al sexo.

Sexo	Frecuencia	Porcentaje
Hombre	74	68,5%
Mujer	34	31,5%
Total	108	100%

Como se observa en la Tabla 6.1, el 68,5% de los participantes son hombres, mientras que el 31,5% restante se encuentra conformado por mujeres.

Edad. –

Las edades de los participantes en la encuesta se muestran en la Tabla 6.2.

Tabla 6.2 Frecuencia de participantes en la encuesta por edades.

Rango de edades	Frecuencia	Porcentaje
23-27	14	13,1%
28-32	16	14,8%
33-37	17	15,8%
38-42	20	18,5%
43-47	19	17,6%
48-52	12	11,2%
53-57	5	4,7%
58-62	5	4,7%
Total	108	100%

Como puede verse en la Tabla 6.2, las personas más jóvenes en ser encuestadas tienen entre 23 y 27 años, comprendiendo aproximadamente el 13,1% del total, mientras que las personas de mayor edad tienen entre 58 y 62 años, conformando aproximadamente el 4,7%. Por otro lado, el rango de edades más amplio comprende entre los 38 y 42 años, conformando aproximadamente el 20% del total.

Mayor Nivel de Educación. -

Los mayores niveles de educación de los participantes se distribuyen como se indica en la Tabla 6.3.

Tabla 6.3 Frecuencia de participantes en la encuesta por niveles de educación.

Nivel de Educación	Frecuencia	Porcentaje
Doctorado	4	3,7%
Maestría	47	43,5%
Universitario (c/ título profesional)	57	52,8%
Total	108	100%

Información Laboral de los encuestados. –

La línea organizacional de los participantes al momento de responder a la encuesta se muestra en la Tabla 6.4.

Tabla 6.4 Frecuencia de participantes en la encuesta con respecto a las líneas organizacionales.

Línea organizacional	Frecuencia	Porcentaje
(No específica)	3	2,8%
Ejecutivo	50	46,3%
Gerencia Media	39	36,1%
Gerencia Senior	16	14,8%
Total	108	100%

Los años de experiencia laboral de cada uno de los participantes se muestran en la Tabla 6.5.

Tabla 6.5 Frecuencia de participantes en la encuesta repartidos por experiencia laboral.

Rango de Años de Experiencia	Frecuencia	Porcentaje
1-10	47	43,5%
11-20	36	20,4%
21-30	22	17,6%
31-40	3	2,8%
Total	108	100%

Situación de la seguridad de información en las organizaciones. –

En la Tabla 6.6 se muestran las razones de la ausencia de políticas de seguridad en las organizaciones de haberse dado el caso.

Tabla 6.6 Frecuencia de las razones de la ausencia de políticas de seguridad en las organizaciones

Razón	Frecuencia	Porcentaje
(no especifica)	101	93,5%
Ausencia de Oficina de Seguridad	1	0,9%
En trámite	2	1,9%
Falta de conocimiento	1	0,9%
No se han presentado inconvenientes	1	0,9%
No se maneja información importante	1	0,9%
Responsabilidad de la Gerencia	1	0,9%
Total	108	100%

Finalmente, los estándares de seguridad de información utilizados en las organizaciones de los encuestados se distribuyen de la siguiente manera, en varias instancias utilizándose más de un estándar, como se indica en la Tabla 6.7.

Tabla 6.7 Frecuencia de estándares de seguridad utilizados en las organizaciones.

Estándares de seguridad	Frecuencia	Porcentaje
(No especifica)	5	4,6%
COBIT	25	23,2%
ISO 27001	84	77,8%
ISO 27002	33	30,5%

Como se puede apreciar en la Tabla 6.8, la norma ISO 27001 es la más utilizada, comprendiendo el 77,8% de los encuestados, mientras la ISO 27002 es utilizada por el 30,5% de los usuarios y COBIT es utilizada por el 23,2%.

6.1.2 Factores críticos para la adopción de PSI

A continuación, se presenta los resultados descriptivos para cada factor.

6.1.2.1 Severidad de Sanciones a Violaciones de Seguridad de Información

La Figura 6.1 presenta el promedio de las respuestas para el factor Severidad de Sanciones.

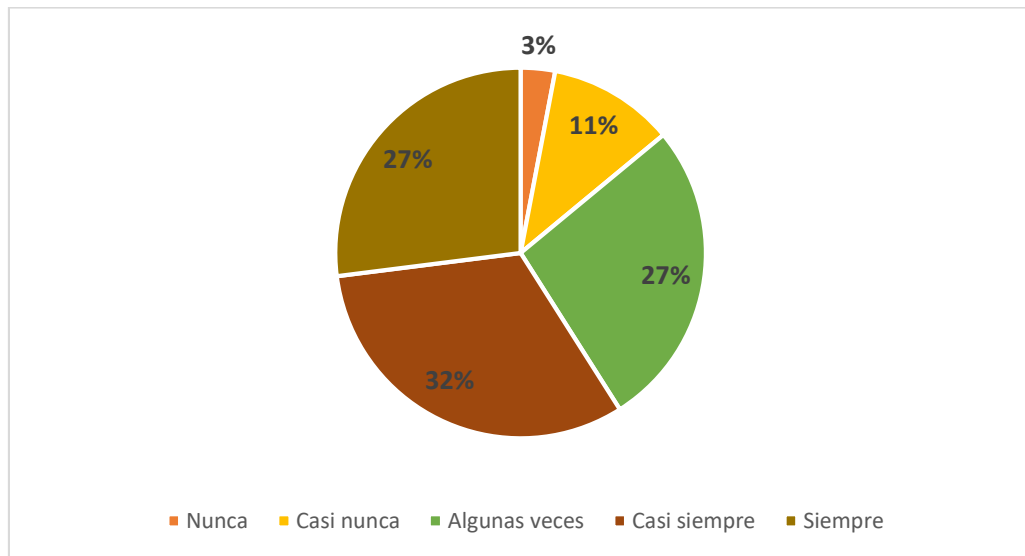


Fig. 6.1 Resultados correspondientes al factor Severidad de Sanciones.

El 59% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 27% comprende el valor “Algunas Veces” y un 14% comprende los valores entre “Casi Nunca” y “Nunca”.

6.1.2.2 Certeza de Sanciones a violaciones de seguridad de información

La Figura 6.2 presenta el promedio de las respuestas para el factor Certeza de Sanciones.

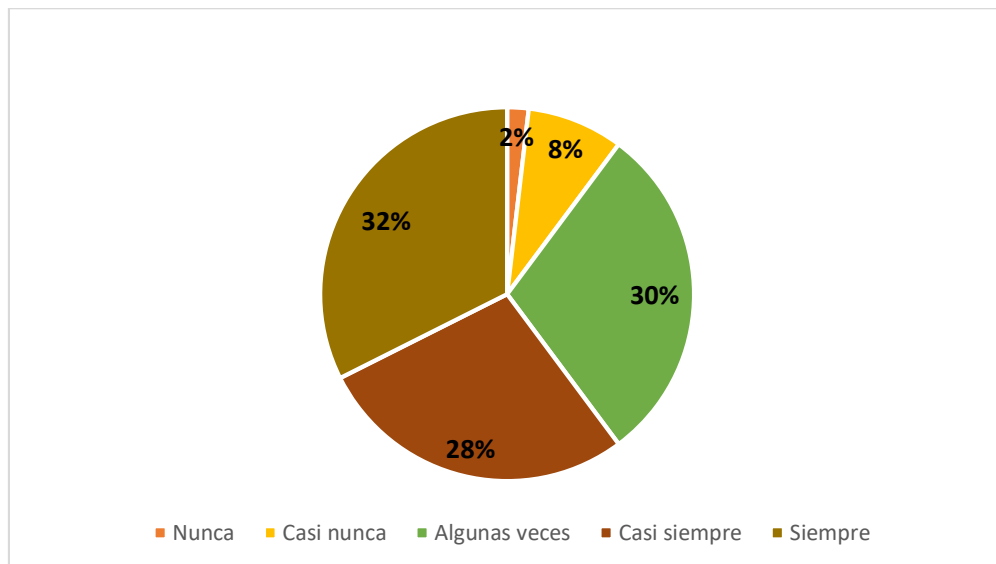


Fig. 6.2 Resultados correspondientes al factor Certeza de Sanciones.

El 60% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 30% comprende el valor “Algunas Veces” y un 10% comprende los valores entre “Casi Nunca” y “Nunca”.

6.1.2.3. Compromiso Organizacional

La Figura 6.3 presenta el promedio de las respuestas para el factor Compromiso Organizacional.

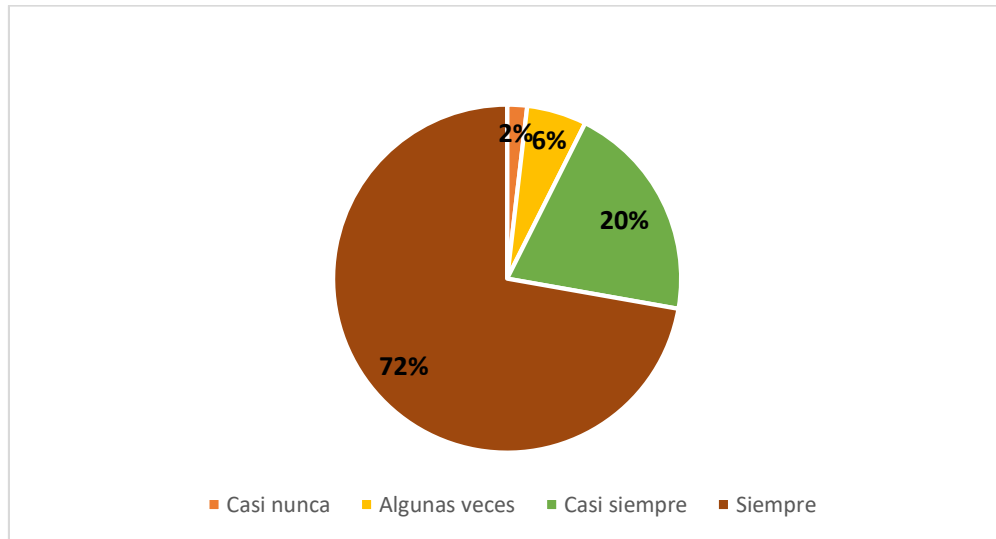


Fig. 6.3 Resultados correspondientes al factor Compromiso Organizacional.

El 92% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 6% comprende el valor “Algunas Veces” y un 2% comprende el valor “Casi Nunca”.

6.1.2.4. Actitud hacia las políticas de Seguridad de Información

La Figura 6.4 presenta el promedio de las respuestas para el factor Actitud hacia las PSI.

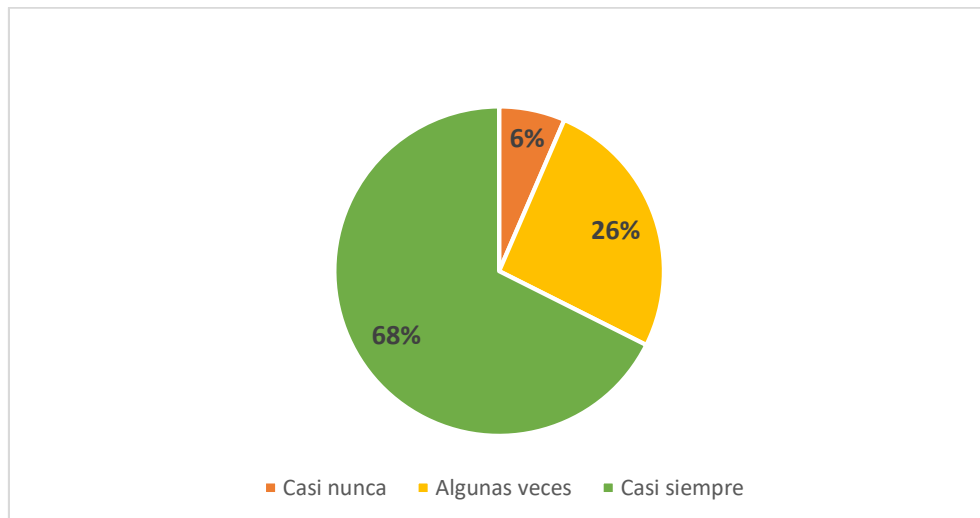


Fig. 6.4 Resultados correspondientes al factor Actitud hacia las PSI.

El 68% de las respuestas comprende el valor “Casi Siempre”, mientras que el 26% comprende el valor “Algunas Veces” y un 6% comprende el valor “Casi Nunca”.

6.1.2.5. Autoeficacia de Seguridad

La Figura 6.5 presenta el promedio de las respuestas para el factor Autoeficacia de Seguridad.

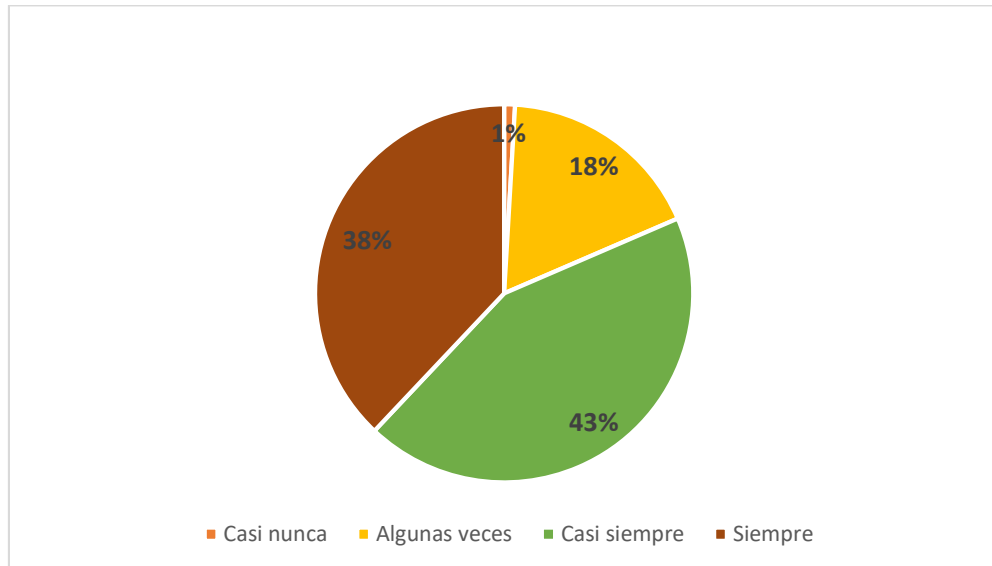


Fig. 6.5 Resultados correspondientes al factor Autoeficacia de Seguridad

El 81% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 18% comprende el valor “Algunas Veces” y un 1% comprende el valor “Casi Nunca”.

6.1.2.6. Severidad percibida de amenazas

La Figura 6.6 presenta el promedio de las respuestas para el factor Severidad percibida de amenazas.

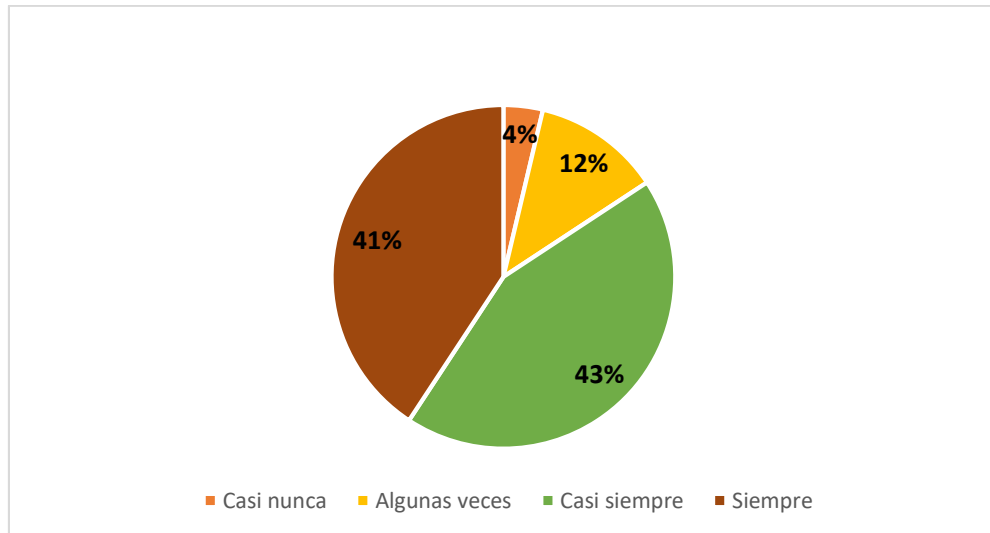


Fig. 6.6 Resultados correspondientes al factor Severidad percibida de amenazas.

Como se observa en la Figura 6.6, el 84% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 12% comprende el valor “Algunas Veces” y un 4% comprende el valor “Casi Nunca”.

6.1.2.7. Vulnerabilidad percibida de amenazas

La Figura 6.7 presenta el promedio de las respuestas para el factor Vulnerabilidad percibida de amenazas.

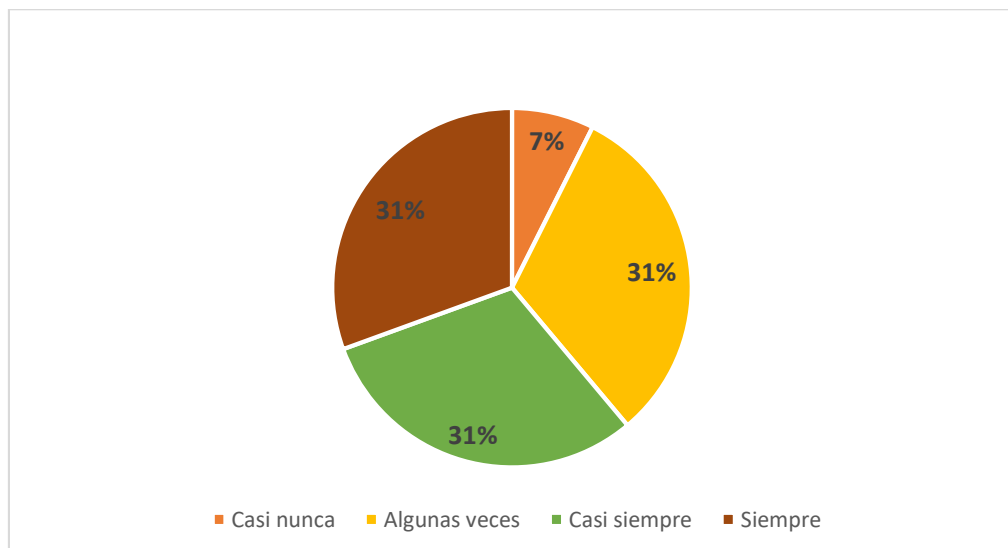


Fig. 6.7 Resultados correspondientes al factor Vulnerabilidad percibida de amenazas.

El 62% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 31% comprende el valor “Algunas Veces” y un 7% comprende el valor “Casi Nunca”.

6.1.2.8 Conciencia de las Políticas de Seguridad de Información

La Figura 6.8 presenta el promedio de las respuestas para el factor Conciencia de las PSI.

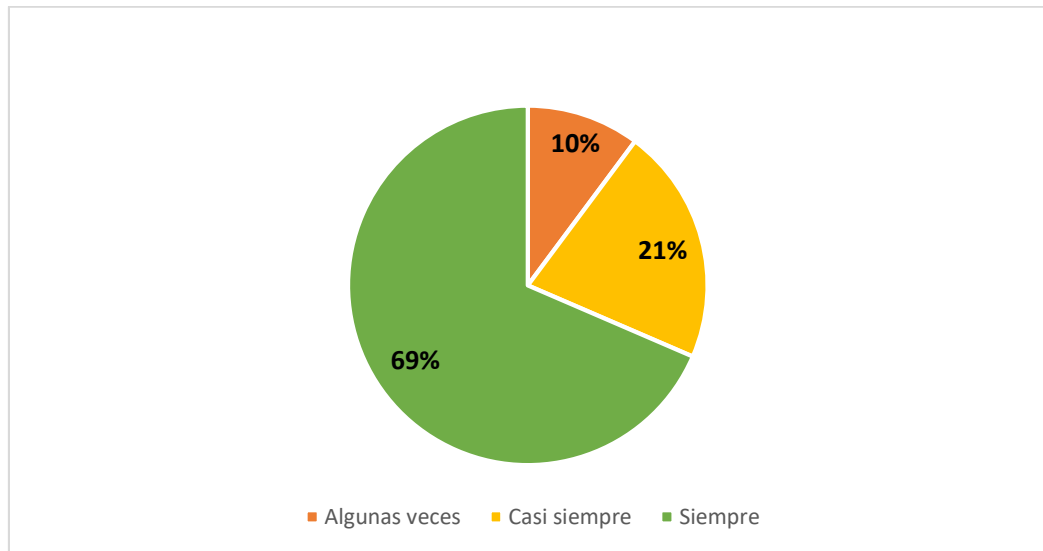


Fig. 6.8 Resultados correspondientes al factor Conciencia de las PSI.

El 90% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 10% comprende el valor “Algunas Veces”.

6.1.2.9 Programas SETA

La Figura 6.9 presenta el promedio de las respuestas para el factor Programas SETA.

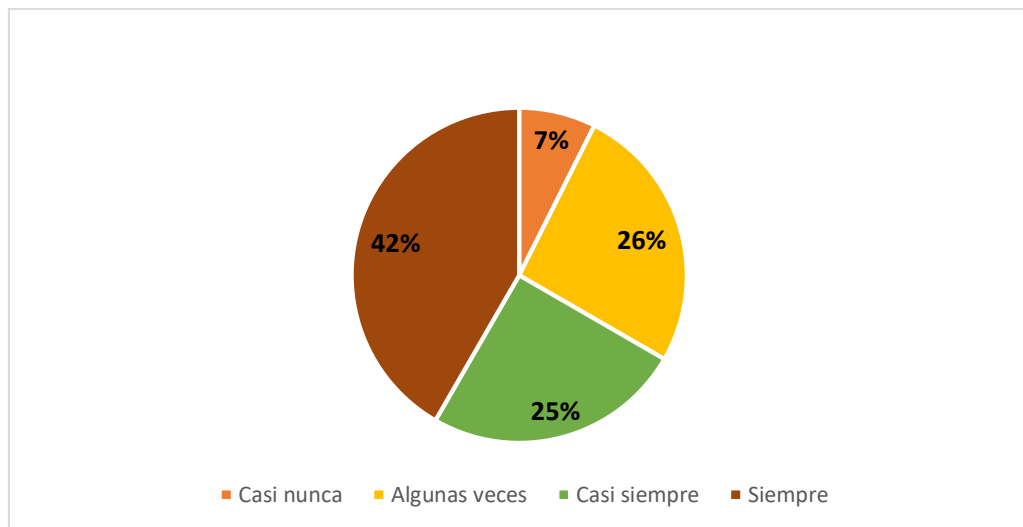


Fig. 6.9 Resultados correspondientes al factor Programas SETA.

El 67% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 26% comprende el valor “Algunas Veces” y un 7% comprende el valor “Casi Nunca”.

6.1.2.10 Cultura de seguridad Organizacional

La Figura 6.10 presenta el promedio de las respuestas para el factor Cultura de seguridad Organizacional.

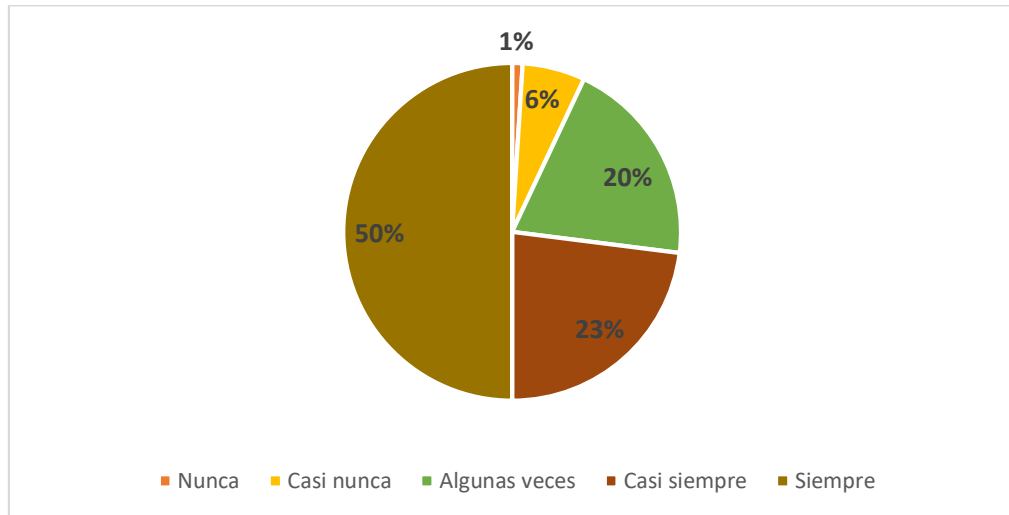


Fig. 6.10 Resultados correspondientes al factor Cultura de seguridad Organizacional.

El 73% de las respuestas comprende los valores entre “Siempre” y “Casi Siempre”, mientras que el 20% comprende el valor “Algunas Veces” y un 7% comprende los valores entre “Casi Nunca” y “Nunca”.

6.1.2.11. Conocimiento de Políticas de Seguridad

La Figura 6.11 presenta el promedio de las respuestas para el factor Conocimiento de Políticas de Seguridad.

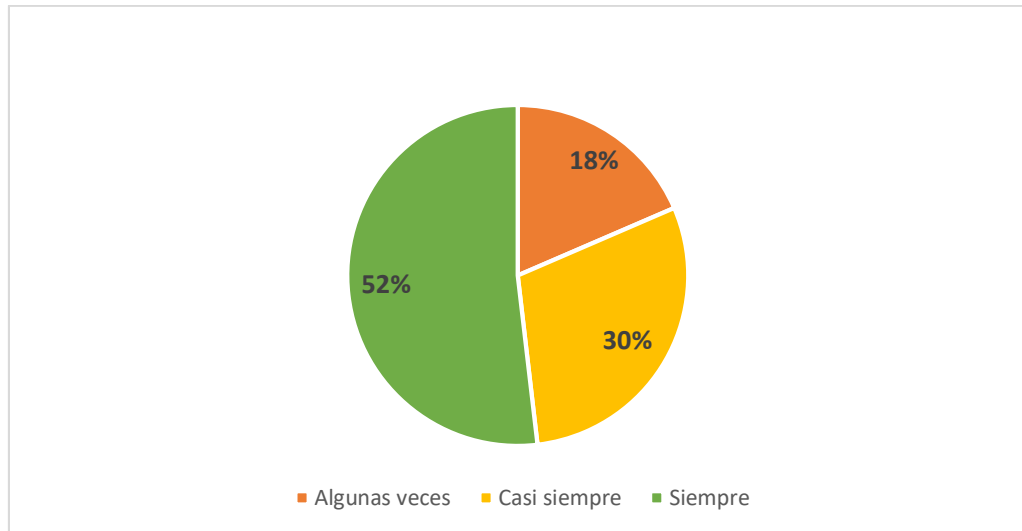


Fig. 6.11 Resultados correspondientes al factor Conocimiento de Políticas de Seguridad.

La Figura 6.11 indica que el 82% de las respuestas se encuentra distribuido entre “Siempre” y “Casi Siempre”, mientras que el 18% está comprendido en “Algunas Veces”.

6.1.2.12. Intención de Cumplimiento

La Figura 6.12 presenta el promedio de las respuestas para el factor Intención de Cumplimiento.

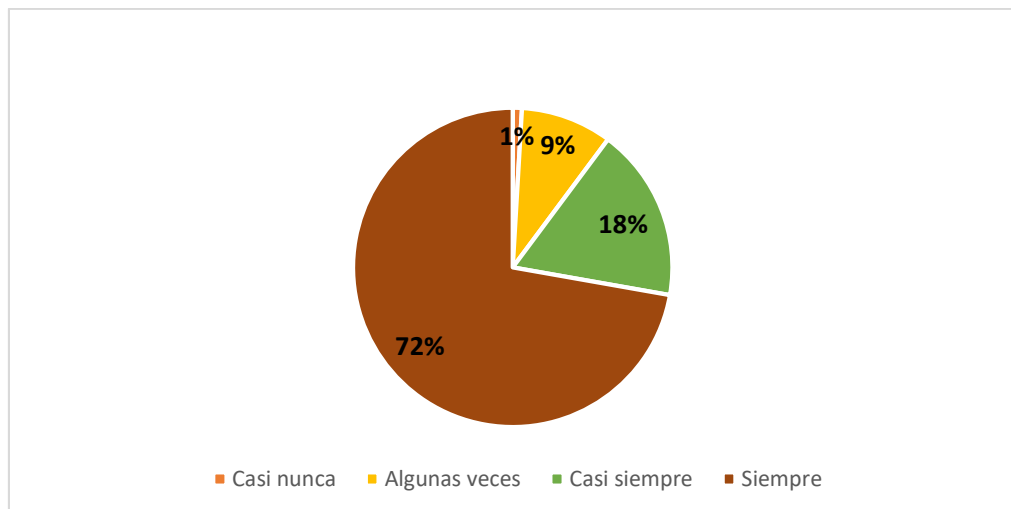


Fig. 6.12 Resultados correspondientes al factor Intención de Cumplimiento.

La Figura 6.12 indica que el 90% de las respuestas se encuentra distribuido entre “Siempre” y “Casi Siempre”, mientras que el 9% está comprendido en “Algunas Veces” y el 1% engloba la respuesta “Casi nunca”.

6.1.2.13. Adopción de las Políticas de Seguridad

La Figura 6.13 presenta el promedio de las respuestas relacionadas a la Adopción de las Políticas de Seguridad.

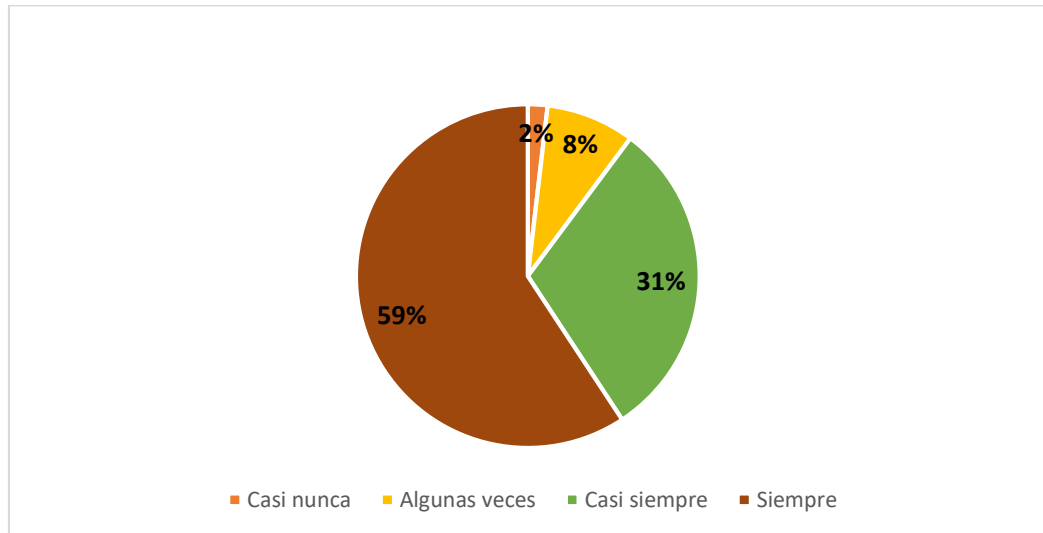


Fig. 6.13 Resultados correspondientes a la Adopción de las Políticas de Seguridad.

La Figura 6.13 indica que el 90% de las respuestas se encuentra distribuido entre “Siempre” y “Casi Siempre”, mientras que el 8% está comprendido en “Algunas Veces” y el 2% “engloba la respuesta “Casi nunca”.

Por otro lado, el indicador de consistencia interna de los ítems que sintetiza el análisis factorial exploratorio es el coeficiente theta ($\theta=0,992$) y el coeficiente omega ($\omega=0,963$), que en ambos casos muestran un nivel aceptable de fiabilidad del instrumento. Así mismo, el coeficiente de fiabilidad de Alfa de Crombach (α de Crombach=0,959) muestra que el instrumento presenta una alta fiabilidad de consistencia interna.

6.2 Modelo de Ecuaciones Estructurales

Para realizar la estimación del modelo de ecuaciones estructurales los ítems de cada uno de los factores se sumaron con la finalidad de representar al factor estudiado. Se obtuvieron doce factores independientes asociados con tres variables independientes, las cuales fueron el resultado del promedio de sus ítems a fin de garantizar homogeneidad en sus rangos de variación.

Por otro lado, los datos de las variables de estudio no presentan normalidad “al 95% de confianza”. Así mismo, la estimación del modelo de ecuaciones estructurales se realizó mediante la

estimación de Distribución Libre Asintótica, por ser un método de estimación adecuado a la falta la normalidad multivariante.

Modelo inicial

La Tabla 6.8 presenta el modelo inicial de ecuaciones estructurales comprobando las hipótesis estudiadas en la tesis.

Tabla 6.8 Modelo inicial

Relación			Coefficientes	Coefficientes estandarizados	S.E.	C.R.	P
Actitud	<---	Conocimiento	-0,344	-0,428	0,055	-6,291	***
Actitud	<---	Compromiso_O	0,294	0,282	0,055	5,389	***
Intención	<---	Severidad	0,167	0,198	0,058	2,858	0,004
Cultura	<---	SETA	0,262	0,307	0,073	3,575	***
Intención	<---	SETA	-0,024	-0,029	0,037	-0,629	0,529
Intención	<---	Actitud	0,513	0,442	0,085	6,037	***
Intención	<---	Conocimiento	0,411	0,442	0,078	5,28	***
Intención	<---	Severidad_P	0,091	0,113	0,056	1,613	0,107
Conciencia	<---	Autoeficacia	0,103	0,318	0,032	3,172	0,002
Intención	<---	Certeza	0,102	0,161	0,033	3,147	0,002
Cultura	<---	Actitud	-0,467	-0,378	0,103	-4,543	***
Intención	<---	Autoeficacia	0,106	0,148	0,032	3,322	***
Intención	<---	Vulnerabilidad	-0,079	-0,144	0,021	-3,79	***
Cumplimiento	<---	Intención	0,475	0,372	0,071	6,651	***
Cumplimiento	<---	Cultura	0,131	0,109	0,097	1,357	0,175
Cumplimiento	<---	Conciencia	-0,907	-0,32	0,334	-2,712	0,007
Cumplimiento	<---	Autoeficacia	0,253	0,275	0,068	3,707	***
Cumplimiento	<---	Certeza	0,161	0,198	0,038	4,229	***
Cumplimiento	<---	Actitud	0,162	0,109	0,077	2,103	0,036

Nota: *** <0,001

Cumplimiento <-> Adopción

De la Tabla 6.8, se observa que el Conocimiento incide de manera negativa a la Actitud (-0,344), Compromiso_Organizacional incide positivamente en la Actitud (0,294), Severidad incide de manera positiva en la Intención (0,167), SETA incide positivamente en la Cultura (0,262), Actitud incide positivamente en la Intención (0,513), Conocimiento incide positivamente en la Intención (0,411), Autoeficacia incide positivamente en la Conciencia (0,103), Certeza incide positivamente en la Intención (0,102), Actitud incide negativamente en la Cultura (-0,467), Autoeficacia incide positivamente en la Intención (0,106), Vulnerabilidad incide negativamente en la Intención (-0,079), Intención incide positivamente en el Cumplimiento (0,475), Cultura incide positivamente en el Cumplimiento (0,131), Conciencia incide negativamente en el Cumplimiento (-0,907), Autoeficacia incide positivamente en el Cumplimiento (0,253), Certeza incide positivamente en el Cumplimiento (0,161) y la Actitud incide positivamente en el Cumplimiento (0,162).

En la Tabla 6.9 se observan los indicadores de bondad de ajuste del modelo inicial de ecuaciones estructurales utilizado en la tesis.

Tabla 6.9 Indicadores de bondad de ajuste del modelo inicial

Nombre	Medida de ajuste	Valor	Límite aceptable*
Índice de ajuste normado	NFI	0,668	$\geq 0,9$
Índice de ajuste comparativo	GFI	0,976	$\geq 0,9$
Índice ajustado de bondad de ajuste	AGFI	0,963	$\geq 0,85$
Índice relativo de ajuste	RFI	0,561	$\geq 0,9$
Raíz cuadrada del error cuadrático medio	RMR	0,354	$\leq 0,1$

* *Byrme, B. (2010)*

Los resultados de los indicadores de ajuste indican que el modelo estructural estimado es aceptable.

Modelo Final

La Tabla 6.10 presenta los resultados del modelo final de ecuaciones estructurales comprobando las hipótesis estudiadas en la tesis.

Tabla 6.10 Modelo final

Relación		Coefficientes	Coefficientes estandarizados	S.E.	C.R.	P
Actitud	<--- Conocimiento	-0,323	-0,405	0,042	-7,603	***
Actitud	<--- Compromiso_O	0,296	0,285	0,053	5,541	***
Intención	<--- Severidad	0,185	0,213	0,052	3,569	***
Cultura	<--- SETA	0,244	0,287	0,07	3,498	***
Intención	<--- Actitud	0,541	0,458	0,069	7,827	***
Intención	<--- Conocimiento	0,436	0,463	0,063	6,958	***
Intención	<--- Severidad_P	0,096	0,118	0,054	1,79	0,073
Conciencia	<--- Autoeficacia	0,109	0,319	0,031	3,499	***
Intención	<--- Certeza	0,108	0,167	0,03	3,56	***
Cultura	<--- Actitud	-0,453	-0,369	0,1	-4,515	***
Intención	<--- Autoeficacia	0,110	0,151	0,032	3,453	***
Intención	<--- Vulnerabilidad	-0,077	-0,139	0,021	-3,724	***
Cumplimiento	<--- Intención	0,478	0,376	0,068	7,068	***
Cumplimiento	<--- Cultura	0,133	0,108	0,097	1,364	0,173
Cumplimiento	<--- Conciencia	-0,889	-0,328	0,289	-3,079	0,002
Cumplimiento	<--- Autoeficacia	0,259	0,28	0,067	3,89	***
Cumplimiento	<--- Certeza	0,166	0,203	0,038	4,409	***
Cumplimiento	<--- Actitud	0,164	0,109	0,078	2,106	0,035

Nota: *** <0,001

Cumplimiento <-> Adopción

De la Tabla 6.10, se observa que el Conocimiento incide de manera negativa a la Actitud (-0,323), Compromiso_Organizacional incide positivamente en la Actitud (0,296), Severidad incide de manera positiva en la Intención (0,185), SETA incide positivamente en la Cultura (0,244), Actitud incide positivamente en la Intención (0,541), Conocimiento incide positivamente en la Intención (0,436), Severidad_Percibida incide positivamente en la Intención (0,096), Autoeficacia incide positivamente en la Conciencia (0,109), Certeza incide positivamente en la Intención (0,108), Actitud incide negativamente en la Cultura (-0,453), Autoeficacia incide positivamente en la Intención (0,110), Vulnerabilidad incide negativamente en la Intención (-0,077), Intención incide positivamente en el Cumplimiento (0,478), Cultura incide positivamente en el cumplimiento (0,133), Conciencia incide negativamente en el Cumplimiento (-0,889), Autoeficacia incide positivamente en el Cumplimiento (0,259), Certeza incide positivamente en el Cumplimiento (0,166) y la Actitud incide positivamente en el Cumplimiento (0,164).

Modelo estructural:

$$Actitud = -0.323xConocimiento + e_4$$

$$Actitud = 0.296xCompromiso_O + e_4$$

$$Intención = 0.185xSeveridad + e_5$$

$$Cultura = 0.244xSETA + e_2$$

$$Intención = 0.541xActitud + e_5$$

$$Intención = 0.436xConocimiento + e_5$$

$$Conciencia = 0.109xAutoeficacia + e_3$$

$$Intención = 0.108xCerteza + e_5$$

$$Cultura = -0.453xActitud + e_2$$

$$Intención = 0.110xAutoeficacia + e_5$$

$$Intención = -0.077xVulnerabilidad + e_5$$

$$Cumplimiento = 0.478xIntención + e_1$$

$$Cumplimiento = -0.889xConciencia + e_1$$

$$Cumplimiento = 0.259xAutoeficacia + e_1$$

$$Cumplimiento = 0.166xCerteza + e_1$$

$$Cumplimiento = 0.164xActitud + e_1$$

En la Tabla 6.11 se observan los indicadores de bondad de ajuste del modelo final de ecuaciones estructurales utilizado en la tesis.

Tabla 6.11 Indicadores de bondad de ajuste del modelo final

Nombre	Medida de ajuste	Valor	Límite aceptable*
Índice de ajuste normado	NFI	0,668	$\geq 0,9$
Índice de ajuste comparativo	GFI	0,976	$\geq 0,9$
Índice ajustado de bondad de ajuste	AGFI	0,964	$\geq 0,85$
Índice relativo de ajuste	RFI	0,568	$\geq 0,9$
Raíz cuadrada del error cuadrático medio	RMR	0,354	$\leq 0,1$

* *Byrne, B. (2010)*

Los resultados de los indicadores de ajuste indican que el modelo estructural es aceptable.

Se observa que dos de los indicadores de ajuste son superiores a los valores aceptables. Por lo tanto, dichos resultados son útiles para describir la realidad estudiada.

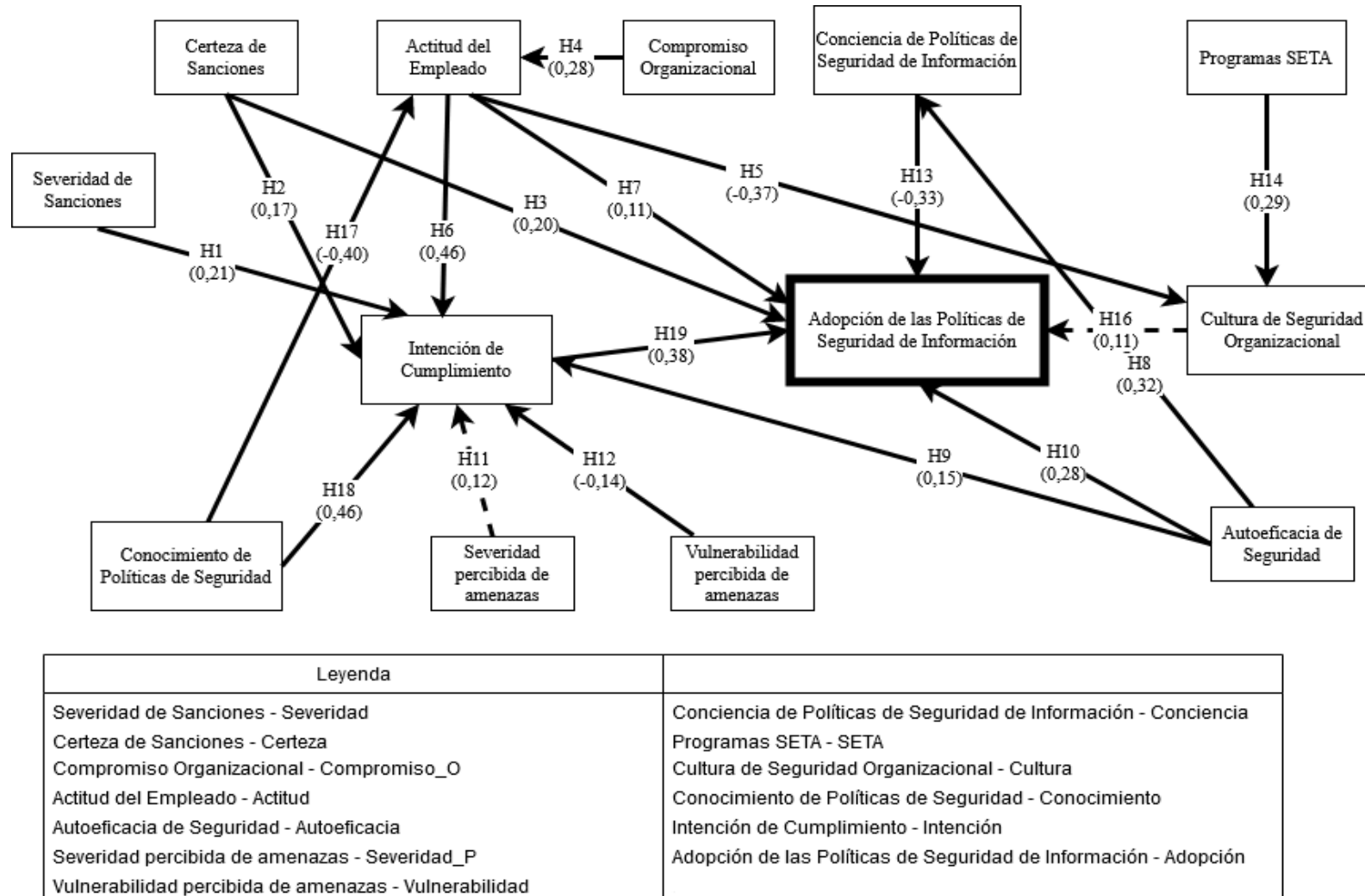


Fig. 6.14 Modelo de ecuaciones estructurales de los factores para la adopción de las PSI.

6.3 Comprobación de Hipótesis

Como resultado de la revisión de literatura se comprueba que existen una serie de factores de éxito que influyen en la adopción de las PSI en las organizaciones. Estos factores son: severidad de sanciones, certeza de sanciones, compromiso organizacional, actitud del empleado, autoeficacia de seguridad, conocimiento de políticas de seguridad e intención de cumplimiento. Mientras tanto, el compromiso organizacional influye de forma indirecta en la adopción de las PSI mediante su influencia en la actitud del empleado, y los programas SETA no influyen de forma directa en la adopción de las PSI, sino mediante su influencia en la cultura organizacional de seguridad.

En la Tabla 6.12 se explica, en base a estos resultados, las hipótesis que son apoyadas o rechazadas.

Tabla 6.12 Confirmación de hipótesis de la investigación según resultados.

Hipótesis	Resultado
H1: La severidad de sanciones influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>Aceptado</i>
H2: La certeza de sanciones influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>Aceptado</i>
H3: La certeza de sanciones influye en la adopción de las PSI en las organizaciones.	<i>Aceptado</i>
H4: El compromiso organizacional influye en la actitud del empleado hacia las PSI en las organizaciones.	<i>Aceptado</i>
H5: La actitud del empleado influye en la cultura de seguridad organizacional.	<i>No Aceptado</i>
H6: La actitud del empleado influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>Aceptado</i>
H7: La actitud del empleado influye en la adopción de las PSI en las organizaciones.	<i>Aceptado</i>
H8: La autoeficacia de seguridad influye en la conciencia de las PSI en las organizaciones.	<i>Aceptado</i>
H9: La autoeficacia de seguridad influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>Aceptado</i>
H10: La autoeficacia de seguridad influye en la adopción de las PSI en las organizaciones.	<i>Aceptado</i>
H11: La severidad percibida de amenazas influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>No Aceptado*</i>
H12: La vulnerabilidad percibida de amenazas influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>No Aceptado</i>
H13: La conciencia de las PSI influye en la adopción de las PSI en las organizaciones.	<i>No Aceptado</i>
H14: Los programas SETA influyen en la cultura de seguridad organizacional.	<i>Aceptado</i>

H15: Los programas SETA influyen en la intención de cumplimiento de las PSI en las organizaciones.	<i>No Aceptado**</i>
H16: La cultura de seguridad organizacional influye en la adopción de las PSI en las organizaciones.	<i>No Aceptado*</i>
H17: El conocimiento de las políticas de seguridad influye en la actitud del empleado hacia las PSI en las organizaciones.	<i>No Aceptado</i>
H18: El conocimiento de las políticas de seguridad influye en la intención de cumplimiento de las PSI en las organizaciones.	<i>Aceptado</i>
H19: La intención de cumplimiento influye en la adopción de las PSI en las organizaciones.	<i>Aceptado</i>

Fuente. Elaboración Propia.

*No aceptado <-> no significativo

**No aceptado <-> relación removida

6.4 Discusión

6.4.1 Severidad de Sanciones

El resultado de esta investigación indica que la severidad de sanciones influye en la intención de cumplimiento de las PSI. Estos resultados coinciden con otros estudios, que postularon que la severidad del castigo, influye directamente en la intención de los colaboradores de cumplir con las PSI, tales como los trabajos de Bulgurcu et al. (2010, como se citó en Merhi & Ahluwalia, 2019).

Estos resultados contradicen otras investigaciones previas, las cuales sostienen que el castigo no tenía efecto alguno sobre la intención de cumplimiento, tales como Herath & Rao (2009, como se citó en Merhi & Ahluwalia, 2019) y Pahnla et al. (2007, como se citó en Merhi & Ahluwalia, 2019).

6.4.2 Certeza de Sanciones

El resultado de esta investigación comprueba la influencia de la certeza de sanciones en la intención de cumplimiento de las PSI. Este resultado apoya los hallazgos de varios de los estudios mencionados en el apartado anterior, los cuales postularon que la certeza de detección influye directamente en la intención de los colaboradores de cumplir con las PSI, tales como los trabajos de Bulgurcu et al. (2010, como se citó en Merhi & Ahluwalia, 2019). Similar a la severidad de sanciones, estos estudios arrojaron hallazgos inconsistentes; algunos encontraron que los factores de castigo son antecedentes significativos de las intenciones de cumplimiento de los empleados, y otros informaron que el castigo no tenía efecto alguno sobre la intención de cumplimiento, tales

como Herath & Rao (2009, como se citó en Merhi & Ahluwalia, 2019) y Pahnla et al. (2007, como se citó en Merhi & Ahluwalia, 2019).

6.4.3 Compromiso Organizacional

La influencia del compromiso organizacional sobre la actitud del empleado hacia las PSI ha sido comprobada en esta investigación. Estos resultados están en línea con antecedentes referentes a este factor, en los cuales se ha postulado que las personas comprometidas no se arriesgarían a poner en peligro su papel en las organizaciones. Así, los hallazgos del estudio de Safa (2016) están en consonancia con los resultados del estudio de Ifinedo (2014). Por su parte, Chol (2018) encontró que los vínculos sociales de un empleado, entre ellos el compromiso, son indudablemente una fuerza impulsora de sus percepciones a ciertas sanciones formales e informales.

6.4.4 Actitud del empleado

Los resultados de este estudio apoyan que la actitud del empleado hacia las PSI influye en la intención de cumplimiento y por consiguiente, en la adopción de las políticas, según los resultados de H6 y H7. Esto indica que, si los individuos de una organización poseen una actitud positiva hacia las políticas de seguridad, estarán más dispuestos a cumplir con las PSI. En el entorno internacional, los constructos de la TPB son considerados impulsores del comportamiento racional, según las investigaciones de Ajzen (1991, como se citó en D'arcy & Lowry, 2019) y Ajzen & Fishbein (2005, como se citó en D'arcy & Lowry, 2019) y porque se ha demostrado su capacidad para predecir el cumplimiento de las PSI en varios estudios, como las investigaciones de D'arcy & Lowry (2019). Apoyando la TPB, Bulgurcu et al. (2010, como se citó en D'arcy & Lowry, 2019) encontraron que la actitud relacionada con el cumplimiento de las PSI se asocia positivamente con la intención de cumplimiento. La investigación referente a la actitud hacia el cumplimiento de las PSI indica la asociación de este factor en la adopción de las políticas de seguridad (Ifinedo, 2014; Siponen et al., 2014).

Sin embargo, cabe resaltar que, de acuerdo con los resultados de H5, la actitud del empleado no influye en la cultura organizacional de seguridad, indicando que la actitud de un individuo hacia dichas políticas no es la única causa de la formación de una cultura de seguridad en toda la organización. Estos resultados se contrastan con los resultados de investigaciones como Lee et al. (2016), Bélanger et al. (2017), Amankwa et al. (2018) y Parsons et al. (2014).

6.4.5 Autoeficacia de seguridad

La investigación también arrojó resultados positivos acerca de la influencia de la autoeficacia del empleado en la adopción de las políticas de seguridad, indicando que, si las capacidades del individuo de realizar actividades de seguridad de información por cuenta propia son lo suficientemente altas, adoptará sin duda alguna las políticas de seguridad, debido a que se siente capaz de cumplirlas. Como antecedentes de dichos hallazgos, Bulgurcu et al. (2010, como se citó en D'arcy & Lowry, 2019) encontraron que, al igual que la actitud relacionada con el cumplimiento de las PSI, la autoeficacia se asoció positivamente con la intención de cumplimiento.

6.4.6 Severidad Percibida de Amenazas

La investigación dio resultados negativos referentes a la influencia de la severidad percibida de amenazas en el entorno nacional, implicando que, entre más grande la percepción de amenaza de los individuos de una organización, mayor será su convicción para cumplir con las PSI. En estudios previos, Bélanger et al. (2017), propusieron la influencia de esta percepción, indicando que, cuanto más vulnerables se sienten las personas, más favorables son al cambio obligatorio de seguridad. Por el contrario, las personas que no logran percibir la gravedad de las amenazas de seguridad tienen menos probabilidades de tener una actitud positiva hacia el cambio de política requerido.

6.4.7 Vulnerabilidad Percibida de Amenazas

Los resultados de esta investigación no apoyan la influencia de la vulnerabilidad percibida de amenazas en la intención de cumplimiento de las PSI. Si los individuos de una organización no perciben vulnerabilidad alguna en las amenazas, no considerarán necesaria la adopción de las PSI.

Estos resultados difieren de aquellos obtenidos en investigaciones realizadas en el extranjero. Bélanger et al. (2017) propusieron la asociación de la vulnerabilidad percibida de amenazas, y discute que los usuarios que son conscientes de una amenaza evalúan si son vulnerables a dicha amenaza. Si es así, la "apelación del miedo" subsiguiente, según Johnston & Warkentin (2010, como se citó en Bélanger et al., 2017) influye positivamente en sus actitudes hacia la seguridad,

de acuerdo con Anderson & Agarwal (2010, como se citó en Bélanger et al., 2017) y Herath & Rao (2009, como se citó en Bélanger et al., 2017).

6.4.8 Conciencia de las PSI

Los resultados de esta investigación indican que la conciencia de la SI no tiene una influencia positiva en la adopción de las PSI, es decir, a mayor o menor conciencia de las PSI, el individuo se sentirá más o menos inclinado a adoptar las PSI. Esto se diferencia de los resultados de investigaciones previas, en las que tiene un rol importante que consiste en mitigar el riesgo de violaciones de SI, tal como lo demuestran estudios previos realizados por Akhunzada et al. (2015, como se citó en Safa et al., 2016) y Caputo et al. (2014, como se citó en Safa et al., 2016).

6.4.9 Programa SETA

El estudio arrojó resultados positivos sobre la influencia de los programas SETA en la cultura de seguridad organizacional, lo que indica que los programas SETA efectivamente ayudan a construir una cultura de seguridad organizacional en los individuos que participan regularmente de estos programas.

Sin embargo, el estudio no apoya la existencia de una influencia de los programas SETA en las intenciones de cumplimiento de las PSI, lo que implica que la sola participación de los individuos de la organización en estos programas no determina que dichos individuos tengan intenciones claras de cumplir con las PSI. Anteriormente, el factor SETA no ha sido ampliamente estudiado en la literatura de SI, y en los casos en que se intentó determinar su influencia en la adopción de PSI, los resultados han sido mixtos. Esto contrasta con los hallazgos del estudio de Kim et al. (2019) que evidencian que los programas SETA influyen de forma positiva en las intenciones de cumplimiento de las PSI de los individuos.

6.4.10 Cultura de Seguridad Organizacional

Se ha comprobado que la cultura de seguridad organizacional no influye en la adopción de las PSI, implicando que la prevalencia de la cultura de seguridad en una organización no promoverá la adopción de las PSI. Estos resultados contrastan con los del estudio de Khan & Alshare (2019), que, al determinar la influencia de la cultura de seguridad organizacional, explicaron que las

organizaciones deben permitir el crecimiento de dicha cultura y apoyar al personal de TI, proveer los recursos y la información de TI necesarios.

6.4.11 Conocimiento de Políticas de Seguridad

Los resultados comprobaron la influencia del conocimiento de políticas de seguridad por parte de los individuos en la intención de cumplimiento de las PSI. Esto refuerza la idea que es importante que los individuos cuenten con los conocimientos pertinentes de las PSI con el fin de asegurar su cumplimiento efectivo. Esto está en línea con la investigación de Lee et al. (2016), quienes sostuvieron que, el conocimiento previo de seguridad es uno de los principales factores que influyen en la actitud hacia el cumplimiento de las PSI, dado que muchos colaboradores no están interesados en la protección de la información debido a su falta de conocimiento sobre seguridad.

Sin embargo, los resultados indican que el conocimiento de las PSI no influye de forma positiva en la actitud del empleado hacia dichas políticas, implicando que, sin importar el grado de conocimiento de los individuos de las políticas de seguridad, su actitud hacia dichas políticas puede no mejorar, o incluso puede empeorar.

6.4.12 Intención de Cumplimiento

Los resultados confirmaron la influencia de la intención de cumplimiento de las PSI por parte del individuo en la adopción de las mismas, indicando que los individuos de las organizaciones cumplirán las políticas de seguridad siempre y cuando mantengan la intención de llevar a cabo dicho cumplimiento. Esto está de acuerdo con los resultados de las investigaciones de Siponen et al. (2014), quienes encontraron que la intención de cumplimiento de las PSI influye de forma positiva y significativa en el cumplimiento actual de dichas políticas.

CONCLUSIONES

Con base a los resultados, se llega a las siguientes conclusiones:

- Se determinaron los factores críticos de éxito a partir de la revisión de literatura y se consideraron 12 factores que tienen influencia en la adopción de las PSI.
- La severidad de sanciones influye positivamente en la intención de cumplimiento de las PSI en las organizaciones con un coeficiente de 0,21.
- La certeza de sanciones influye positivamente en la intención de cumplimiento con un coeficiente de 0,17.
- La certeza de sanciones influye positivamente en la adopción de las PSI con un coeficiente igual a 0,20.
- El compromiso organizacional influye positivamente en la actitud del empleado hacia las PSI con un coeficiente de 0,28.
- La actitud del empleado influye negativamente en la cultura de seguridad organizacional con un coeficiente de -0,37.
- La actitud del empleado influye positivamente en la intención de cumplimiento de las PSI con un coeficiente de 0,46.
- La actitud del empleado influye positivamente en la adopción de las PSI con un coeficiente de 0,11.
- La autoeficacia de seguridad influye positivamente en la conciencia de PSI con un coeficiente de 0,32.
- La autoeficacia de seguridad influye positivamente en la intención de cumplimiento de las PSI con un coeficiente de 0,15.
- La autoeficacia de seguridad influye positivamente en la adopción de las PSI con un coeficiente de 0,28.
- La severidad percibida de amenazas no influye en la adopción de las PSI.
- La vulnerabilidad percibida de amenazas influye negativamente en la intención de cumplimiento de las PSI con un coeficiente de -0,14.
- La conciencia de PSI influye negativamente en la adopción de las PSI con un coeficiente de -0,33.
- Los programas SETA influyen positivamente en la cultura organizacional de seguridad con un coeficiente de 0,29.
- Los programas SETA con respecto a la intención de cumplimiento de las PSI, no se consideran en el modelo final.
- La cultura de seguridad organizacional no influye en la adopción de las PSI.

- El conocimiento de PSI influye negativamente en la actitud de los empleados hacia las PSI con un coeficiente de -0,40.
- El conocimiento de PSI influye positivamente en la intención de cumplimiento de las PSI con un coeficiente de 0,46.
- La intención de cumplimiento influye positivamente en el cumplimiento actual de PSI con un coeficiente de 0,38.

LIMITACIONES

Las limitaciones en este trabajo.

- En primer lugar, la muestra igual a 108 participantes, resulta muy pequeña para lograr establecer una inferencia sólida. Esto se debe a que, pese a enviar 364 invitaciones para responder la encuesta, más de la mitad de las personas contactadas decidieron no responder. Por ello, las investigaciones futuras necesitan asegurar una mayor participación en las encuestas.
- Otra limitación importante es la poca proporción de entidades estatales en comparación con las organizaciones privadas en la encuesta, lo cual demuestra el hermetismo de las primeras dado el tipo de información con el que operan.
- Ambos puntos fueron exacerbados por el actual contexto de la pandemia del COVID-19, dificultando aún más la participación de la población de estudio.

RECOMENDACIONES

- Debido a que una de las limitaciones de esta investigación es la falta de una muestra lo suficientemente grande para establecer un análisis sólido, futuras investigaciones sobre políticas de seguridad deben ampliar la muestra utilizada en el trabajo de investigación, asegurando la mayor cantidad de respuestas posibles a la encuesta, así como incluir el muestreo probabilístico.
- Dado que este estudio utilizó un enfoque cuantitativo, se debe conducir una investigación con enfoque cualitativo utilizando cuestionarios de preguntas abiertas a fin de obtener una nueva perspectiva sobre qué factores influyen en la adopción de las PSI.
- Como se ha mencionado en la investigación y en la revisión de literatura, el aspecto humano es el verdadero determinante de la adopción de las PSI, dado que constituye el usuario final de estas políticas. Por lo tanto, se debe concientizar a todos los individuos de las organizaciones de la importancia de las PSI y las consecuencias de brechas de seguridad que pueden evitarse cumpliendo estas políticas.
- El contexto actual de pandemia ha provocado una acelerada transformación del escenario laboral, dejando de lado los entornos físicos para establecer el entorno digital. Sin embargo, el concepto de seguridad de información (el cual engloba las políticas de seguridad) seguirá presente dado que la información existente permanecerá y continuará creciendo. Por ello, se debe promover desde las aulas la cultura de la seguridad considerando que, aún después de la pandemia, el entorno digital estará presente en los hogares y las instituciones, y la información que se maneja simplemente seguirá creciendo.

TRABAJOS FUTUROS

En base a los resultados y conclusiones surgidos en la presente investigación se plantean los siguientes trabajos futuros:

- Dado que la recolección de datos se llevó a cabo enfocándose en las empresas privadas y entidades públicas de Lima, futuras investigaciones deben tomar en cuenta a las organizaciones presentes en las diferentes regiones del Perú, con el fin de comprobar si la situación de la adopción de PSI es similar o distinta a la de la capital.
- Debido a que la mayoría de respuestas provenientes son de empresas privadas, es necesario que futuras investigaciones procuren la participación más activa de entidades públicas y estatales, dado que la información que manejan dichas organizaciones involucra a la población y a otros elementos importantes de la sociedad peruana.
- De igual forma, es importante que futuras investigaciones expandan la población objetivo de la recolección de datos a la totalidad del personal de las organizaciones, dado que todo el personal constituye los usuarios finales de las PSI.
- Otro punto importante que futuras investigaciones deben abordar es determinar las diferencias en la adopción de PSI entre las organizaciones públicas y privadas, ya que aspectos como el entorno laboral y el tipo de información utilizado pueden determinar los tipos de políticas aplicadas en cada organización y subsecuentemente, su adopción.
- Las investigaciones futuras pueden utilizar técnicas propias del enfoque cualitativo para profundizar el estudio del comportamiento de las personas hacia el cumplimiento de las PSI.

REFERENCIAS BIBIOGRÁFICAS. –

- Abdelwahed, A.S., Mahmoud, A.Y., y Bdair, R.A. (2016).** Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management*, 15, 1-26.
- Addae, J.A., Simpson, G., y Ampong, G.O. (2019).** Factors Influencing Information Security Policy Compliance Behavior. *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 43-47. <https://doi.org/10.1109/ICSIoT47925.2019.00015>
- Albrechtsen, E. (2008).** *Friend or foe? Information security management of employees*. NTNU – Norwegian University of Science and Technology. Trondheim, Noruega. Recuperado de <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/265659> en Noviembre de 2019.
- Alias, R. A. (2019).** Information security policy compliance: Systematic literature review. *Procedia Computer Science*, 161, 1216-1224.
- Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., y Aleassa, H.M. (2013).** Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *2013 46th Hawaii International Conference on System Sciences*, 3018-3027. <https://dx.doi.org/10.1109/HICSS.2013.272>
- Alqathani, F. (2017).** Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, 124, 691–697. <https://doi.org/10.1016/j.procs.2017.12.206>
- Alshare, K., Lane, P., y Lane, M. (2018).** Information security policy compliance: a higher education case study. *Information & Computer Security*, 26, 91-108. <https://doi.org/10.1108/ICS-09-2016-0073>

Amankwa, E., Loock, M., y Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, 26, 420-426. <https://doi.org/10.1108/ICS-09-2017-0063>

Anderson, James E. (1974). *Public Policymaking*. Cengage Learning. Edición 2010.

Aurigemma, S., y Mattson, T. (2017). Privilege or procedure: evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security*, 66, 218-234. <http://dx.doi.org/doi:10.1016/j.cose.2017.02.006>

Bélangier, F., Collignon, S.E., Enget, K., y Negangard, E. (2017). Determinants of Early Conformance with information security policies. *Information & Management*, 54, 887-901. <http://dx.doi.org/doi:10.1016/j.im.2017.01.003>

Byrme, B. (2010). Structural Equation Modeling with AMOS, 2da. Ed, <https://doi.org/10.4324/9780203805534>

Castillo, A., Bruzza, M., y Tupia, M. (2021). Estado del arte sobre la identificación amenazas no intencionales de ciberseguridad de parte de personal interno en instituciones públicas. *Revista Ibérica de Sistemas e Tecnologías de Informação*, N°E41, 70-82.

Celi, E y Díaz, R. (2017). *Políticas de seguridad de la información en función del comportamiento de los usuarios de tecnologías de la información en el sector microfinanciero de LAMBAYEQUE*. Universidad Nacional Pedro Ruiz Gallo. Lambayeque. Perú.

Celi, E., y Díaz, R. (2021). Information Security Policies Based on the Behavior of IT Users in the Microfinance Sector of Lambayeque-Peru. *Proceedings of the 5th Brazilian Technology Symposium*, 331-340. Artículo basado y traducido de **Celi, E y Díaz, R. (2017).**

- Chang, K., y Seow, Y.M. (2019).** Protective Measures and Security Policy Non-Compliance Intention: IT Vision Conflict as a Moderator. *Journal of Organizational and End User Computing*, 31, 1-21. <https://dx.doi.org/10.4018/JOEUC.2019010101>
- Chen, X., Chen, L., y Wu, D. (2018a).** Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. *Journal of Computer Information Systems*, 58, 312-324. <http://dx.doi.org/10.1080/08874417.2016.1258679>
- Chen, X., Wu, D., Chen, L., y Teng, J.K. (2018b).** Sanction Severity and Employees' Information Security Policy Compliance: Investigating mediating, moderating, and control Variables. *Information & Management*, 55, 1049-1060. <https://doi.org/10.1016/j.im.2018.05.011>
- Chol, M., y Song, J. (2018).** Social control through deterrence on the compliance with information security policy. *Soft Computing*, 22, 6765-6772. <https://doi.org/10.1007/s00500-018-3354-z>
- Dang-Pham, D., Pittayachawan, S., y Bruno, V. (2017).** Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67, 196-206. <http://dx.doi.org/10.1016/j.chb.2016.10.025>
- D'Arcy, J., y Lowry, P.B. (2019).** Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29, 43-69. <https://doi.org/10.1111/isj.12173>
- Da Veiga, A., y Martins, N. (2015a).** Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162-176. <http://dx.doi.org/10.1016/j.cose.2014.12.006>
- Da Veiga, A., y Martins, N. (2015b).** Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31, 243-256. <http://dx.doi.org/10.1016/j.clsr.2015.01.005>

- DeNardis (2007).** *Chapter 24: A History of Internet Security.* In de Leeuw, K.M.M.; Bergstra, J. (editores). *The History of Information Security: A Comprehensive Handbook.* pp. 681–704.
- Dhillon, G., Talib, Y.Y., y Picoto, W. (2020).** The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions. *Journal of the Association for Information Systems*, 21, 152-164. <https://dx.doi.org/10.17705/1jais.00595>
- Flores, W., Antonsen, E., y Ekstedt, M. (2014).** Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110. <http://dx.doi.org/10.1016/j.cose.2014.03.004>
- Fong, N., & Bayona-Oré, S. (2022).** Consideraciones para el Cumplimiento de la Política de Seguridad de la Información. *Revista Ibérica de Sistemas e Tecnologías de Informação*, (E51), 528-539.
- Guo, K., y Yuan, Y. (2012).** The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, 49, 320-326. <http://dx.doi.org/10.1016/j.im.2012.08.001>
- Ghazvini, A., Shukur, Z., y Hood, Z. (2018).** Review of information security policy based on content coverage and online presentation in higher education. *International Journal of Advanced Computer Science and Applications*, 9, 410-423. <https://doi.org/10.14569/ijacsa.2018.090853>
- Gwebu, K.L., Wang, J., y Hu, M. (2020).** Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, 30, 220-269. <https://doi.org/10.1111/isj.12257>
- Han, J., Kim, Y.J., y Kim, H. (2017).** An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66, 52-65. <http://dx.doi.org/doi:10.1016/j.cose.2016.12.016>

- Hanus, B., Windsor, J.C., y Wu, Y. (2018).** Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order. *The DATA BASE for Advances in Information Systems*, 49 (Edición especial), 103-133. <https://dx.doi.org/10.1145/3210530.3210538>
- Hastedt, G.P. (2011).** *Spies, Wiretaps, and Secret Operations: An Encyclopedia of American Espionage*. ABC-CLIO, LLC.
- Hina, S., Dominic, P., y Lowry, P.B. (2019).** Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, 87. 101594. <https://doi.org/10.1016/j.cose.2019.101594>
- Hong, Y., y Furnell, S. (2019).** Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. *Journal of Computer Information Systems*, 1-10. <https://doi.org/10.1080/08874417.2019.1683781>
- Humaidi, N., y Balakrishnan, V. (2018).** Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal*, 47, 17-27. <https://doi.org/10.1177/1833358317700255>
- Ifinedo, P. (2014).** Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51, 69-79. <http://dx.doi.org/10.1016/j.im.2013.10.001>
- Ifinedo, P. (2016).** Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? *Information Systems Management*, 33, 30-41. <http://dx.doi.org/10.1080/10580530.2015.1117868>
- Ifinedo, P. (2018).** Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions. *Information Resources Management Journal*, 31, 52-83. <http://dx.doi.org/10.4018/IRMJ.2018010103>

ISACA (2012). *COBIT 5 Implementación*. ISBN 978-1-60420-289-2. Versión traducida al español por Capítulo de Madrid de ISACA en 2012.

ISOTools Excellence (09 de abril de 2017). *Qué debe incluir la Política de Seguridad de la Información según ISO 27001*. Blog Calidad y Excelencia. Recuperado de <https://www.isotools.org/2017/04/09/incluir-la-politica-seguridad-la-informacion-segun-iso-27001/>

Jaeger, L., Eckhardt, A., y Kroenung, J. (2020). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: results of a multigroup analysis. *Information y Management*. 103318. <https://doi.org/10.1016/j.im.2020.103318>

Johnson, John (1997). *The Evolution of British Sigint*. Editorial HMSO, Chletenham. Reino Unido.

Kajtazi, M., Cavusoglu, H., Benbasat, I., y Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information & Computer Security*. 26. 171-193. <https://doi.org/10.1108/ICS-09-2017-0066>

Khan, H., y Alshare, K.A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, 29, 4-23. <https://doi.org/10.1080/10919392.2019.1552743>

Kim, S.H., Yang, K.H. y Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal*, 2014. <https://doi.org/10.1155/2014%2F463870>

Kim, H.J., Choi, H., y Han, J. (2019). Leader power and employees' information security policy compliance. *Security Journal*, 32, 391-409. <https://doi.org/10.1057/s41284-019-00168-8>

Kolkowska, E., Karlsson, F., y Hedström, K. (2017). Towards analysing the rationale of information security noncompliance: Devising a Value-Based Compliance analysis

method. *Journal of Strategic Information Systems*, 26, 39-57.
<https://doi.org/10.1016/j.jsis.2016.08.005>

Koohang, A., Nowak, A., Paliszkiewicz, J., y Nord, J.H. (2020). Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. *Computer Information Systems*, Vol. 60, 1-8. <https://doi.org/10.1080/08874417.2019.1668738>

Kuo, K., Talley, P., y Huang, C.H. (2020). A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. *Comput. Secur.*, 96, 101928.
<https://doi.org/10.1016/j.cose.2020.101928>

Kuppusamy, P., Samy, G. N., Maarop, N., Shanmugam, B., & Perumal, S. (2022). Information security policy compliance behavior models, theories, and influencing factors: A systematic literature review. *Journal of Theoretical and Applied Information Technology*, 100(5), 1536-1557.

Lee, C., Lee, C.C., y Kim, S. (2016). Understanding information security stress: focusing on the type of information security compliance activity. *Computers & Security*, 59, 60-70.
<http://dx.doi.org/doi: 10.1016/j.cose.2016.02.004>

Lowi, T.J. (1964). American Business, Public Policy, Case-Studies, and Political Theory. *World Politics*, 16, 677-715.

Lowry, P.B., Posey, C., Bennett, R., y Roberts, T. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, 25 (edición especial), 193-273.
<https://doi.org/10.1111/isj.12063>

Liu, C., Wang, N., y Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *Int. J. Inf. Manag.*, 54, 102152. <https://doi.org/10.1016/j.ijinfomgt.2020.102152>

- Merhi, M.I., y Ahluwalia, P. (2019).** Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, 92, 37-46. <https://doi.org/10.1016/j.chb.2018.10.031>
- Moody, G., Siponen, M., y Pahlila, S. (2018).** Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, 42, 285-311. <https://dx.doi.org/10.25300/MISQ/2018/13853>
- Nasir, A., Arshah, R.B., y Hamid, M. (2019).** A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, 28, 55-80. <https://doi.org/10.1080/19393555.2019.1643956>
- Nieles, M., Dempsey, K., y Pillitteri, V.Y. (2017).** An Introduction to Information Security. *NIST Special Publication 800-12 Rev-1*. <https://doi.org/10.6028/NIST.SP.800-12R1>
- Niemimaa, E. (2017).** Crafting Organizational Information Security Policies. *Tampere University of Technology. Publication; 1507*. Tampere University of Technology.
- Niemimaa, E., y Niemimaa, M. (2017).** Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, 26, 1–20. <https://doi.org/10.1057/s41303-016-0025-y>
- Paananen, H., Lapke, M., y Siponen, M. (2020).** State of the art in information security policy development. *Computers & Security*, 88, 101608 <https://doi.org/10.1016/j.cose.2019.101608>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., y Jerram, C. (2014).** Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176. <http://dx.doi.org/10.1016/j.cose.2013.12.003>

- Pérez Villamar, J. (2015).** *El Positivismo y la Investigación Científica. Revista Empresarial, ICE-FEE-UCSG. ISSN No. 1390 – 3748. Edición N°35. 9(No. 3). Págs. 29-34. Julio - septiembre, 2015.*
- Pham, H., Brennan, L., y Furnell, S. (2019).** Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*; 46, 96-107. <https://doi.org/10.1016/j.jisa.2019.03.012>
- Pmg-ssi.com (03 de agosto de 2017).** *Norma ISO 27002: El dominio política de seguridad.* <https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/>.
- Prieto, A. (2016).** *Marco de mejora continua del gobierno TI en entidades financieras.* Universidad de Castilla - La Mancha. Castilla, España.
- Rajab, M., y Eydgahi, A. (2019).** Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, 80, 211-233. <https://doi.org/10.1016/j.cose.2018.09.016>
- Rojas, Paolo (2019).** *Ciberseguridad: situación de las empresas peruanas frente a sus pares de la región.* Diario Gestión. Recuperado de <https://gestion.pe/economia/empresas/ciberseguridad-situacion-de-las-empresas-peruanas-frente-a-sus-pares-de-la-region-noticia/> en Febrero de 2020.
- Safa, N.S., Solms, R.V., y Furnell, S. (2016).** Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82. <http://dx.doi.org/10.1016/j.cose.2015.10.006>
- Safa, N.S., Maple, C., Furnell, S., Azad, M., Perera, C., Dabbagh, M., y Sookhak, M. (2019).** Deterrence and prevention-based model to mitigate information security insider threats in organisations. *ArXiv, abs/1903.12079*. <https://doi.org/10.1016/j.future.2019.03.024>

- Samonas, S., Dhillon, G., y Almusharraf, A. (2020).** Stakeholder perceptions of information security policy: Analyzing personal constructs. *Int. J. Inf. Manag.*, 50, 144-154. <https://doi.org/10.1016/J.IJINFOMGT.2019.04.011>
- Sebag-Montefiore., H. (2011).** *Enigma: The Battle for the Code*. Orion. (p. 576).
- Setiawan, Y., y Maharani, A. (2022).** Unboxing Employees Perspectives on Factors Affecting Their Compliance to Organizational Information Security Policies. *In Proceedings of 2nd International Conference on Smart Computing and Cyber Security: Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2021)* (pp. 182-193). Singapore: Springer Nature Singapore.
- Sharma, S., y Warkentin, M. (2019).** *Do I really belong?: Impact of employment status on information security policy compliance.* *Computers & Security.* 87. <https://doi.org/10.1016/j.cose.2018.09.005>
- Siponen, M., Mahmood, M., y Pahlila, S. (2014).** Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51. 217-224. <http://dx.doi.org/10.1016/j.im.2013.08.006>
- Sommestad, T., Karlzén, H., y Hallberg, J. (2015).** The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, 23, 200-217. <http://dx.doi.org/10.1108/ICS-04-2014-0025>
- Sommestad, T., Karlzén, H., y Hallberg, J. (2019).** The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, 59, 344-353. <http://dx.doi.org/10.1080/08874417.2017.1368421>
- Sommestad, T. (2018).** Work-related groups and information security policy compliance. *Information and Computer Security*, 26, 533-550. <https://doi.org/10.1108/ICS-08-2017-0054>

- Son, J. (2011).** Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48, 296-302.
<http://dx.doi.org/10.1016/j.im.2011.07.002>
- Suetonius (2008).** Oxford University Press, *Lives of the Caesars* Oxford (p. 28).
- Trang, S., y Brendell, A.B. (2019).** A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers*, 21, 1265-1284.
<https://doi.org/10.1007/s10796-019-09956-4>
- van Vuuren, I. E.; Kritzing, E. y Mueller, C. (2015).** Identifying Gaps in IT Retail Information Security Policy Implementation Processes: Towards developing a secure IT enterprise built on trust. *Computer Science, Business. 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*.
<https://doi.org/10.1109/InfoSec.2015.7435517>
- Vance, A., Siponen, M., y Pahlila, S. (2012).** Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49, 190-198.
<https://doi.org/10.1016/j.im.2012.04.002>
- Vance, A., Siponen, M., y Straub, D. (2020).** Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Culture. *Information and Management*, 57, 103212. <https://doi.org/10.1016/j.im.2019.103212>
- Weidman, J., y Grossklags, J. (2020).** Assessing the current state of information security policies in academic organizations. *Inf. Comput. Secur.*, 28, 423-444.
<https://doi.org/10.1108/ICS-12-2018-0142>
- Wiafe, I., Koranteng, F., Wiafe, A., Obeng, E.N., y Yaokumah, W. (2020).** The role of norms in information security policy compliance. *Inf. Comput. Secur.*, 28, 743-761.
<https://doi.org/10.1108/ics-08-2019-0095>

- Willison, R., Warkentin, M., y Johnston, A. (2018).** Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 28, 266-293. [https://dx.doi.org/ 10.1111/isj.12129](https://dx.doi.org/10.1111/isj.12129)
- Yazdanmehr, A., y Wang, J. (2016).** Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, 36-46. <http://dx.doi.org/10.1016/j.dss.2016.09.009>
- Yupanqui, J., y Bayona, S. (2017).** Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 2017(25), 112–134.

ANEXOS. –

Anexo I.- Matriz de Consistencia

Tabla 7.1 Matriz de Consistencia

Problema General	Objetivo General	Hipótesis General	Metodología
<i>¿En qué medida influyen los factores de éxito en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de los factores de éxito en la adopción de las PSI en las organizaciones.</i>	<i>Existen una serie de factores de éxito que influyen en la adopción de las PSI en las organizaciones.</i>	Tipo de Investigación: Cuantitativo Alcance: Descriptivo Unidad de análisis: Profesionales del área de seguridad de tecnologías de información de las empresas Población: Oficiales de seguridad de instituciones de administración pública, Expertos del área de seguridad de empresas privadas Muestra: No probabilística; Expertos de seguridad de TI áreas de seguridad de instituciones públicas y privadas
Problemas Específicos	Objetivos Específicos	Hipótesis Específicas	
<i>¿En qué medida influye la severidad de sanciones en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la severidad de sanciones en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>La severidad de sanciones influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la certeza de sanciones en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la certeza de sanciones en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>La certeza de sanciones influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la certeza de sanciones en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la certeza de sanciones en la adopción de las PSI en las organizaciones.</i>	<i>La certeza de sanciones influye en la adopción de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye el compromiso organizacional en la actitud del empleado hacia las PSI en las organizaciones?</i>	<i>Determinar la influencia del compromiso organizacional en la actitud del empleado hacia las PSI en las organizaciones.</i>	<i>El compromiso organizacional influye en la actitud del empleado hacia las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la actitud del empleado en la cultura organizacional de seguridad?</i>	<i>Determinar la influencia de la actitud del empleado en la cultura organizacional de seguridad.</i>	<i>La actitud del empleado influye en la cultura de seguridad organizacional.</i>	

<i>¿En qué medida influye la actitud del empleado en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la actitud del empleado en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>La actitud del empleado influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>Técnica de Recolección de Datos:</i> <i>encuesta dirigida a profesionales de seguridad de TI en empresas</i> <i>Análisis de Datos:</i> <i>Modelamiento de ecuación estructural (SEM); SmartPLS</i>
<i>¿En qué medida influye la actitud del empleado en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la actitud del empleado en la adopción de las PSI en las organizaciones.</i>	<i>La actitud del empleado influye en la adopción de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la autoeficacia de seguridad en la conciencia de PSI en las organizaciones?</i>	<i>Determinar la influencia de la autoeficacia de seguridad en la conciencia de PSI en las organizaciones.</i>	<i>La autoeficacia de seguridad influye en la conciencia de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la autoeficacia de seguridad en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la autoeficacia de seguridad en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>La autoeficacia de seguridad influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la autoeficacia de seguridad en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la autoeficacia de seguridad en la adopción de las PSI en las organizaciones.</i>	<i>La autoeficacia de seguridad influye en la adopción de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la severidad percibida de amenazas en la intención de cumplimiento de PSI en las organizaciones?</i>	<i>Determinar la influencia de la severidad percibida de amenazas en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>La severidad percibida de amenazas influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la vulnerabilidad percibida de amenazas en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la vulnerabilidad percibida de amenazas en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>La vulnerabilidad percibida de amenazas influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la conciencia de las PSI en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la conciencia de las PSI en la adopción de las PSI en las organizaciones.</i>	<i>La conciencia de las PSI influye en la adopción de las PSI en las organizaciones.</i>	

<i>¿En qué medida influyen los programas SETA en la cultura de seguridad organizacional?</i>	<i>Determinar la influencia de los programas SETA en la cultura de seguridad organizacional.</i>	<i>Los programas SETA influyen en la cultura de seguridad organizacional.</i>	
<i>¿En qué medida influyen los programas SETA en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia de los programas SETA en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>Los programas SETA influyen en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la cultura de seguridad organizacional en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la cultura de seguridad organizacional en la adopción de las PSI en las organizaciones.</i>	<i>La cultura de seguridad organizacional influye en la adopción de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye el conocimiento de las políticas de seguridad en la actitud del empleado hacia las PSI en las organizaciones?</i>	<i>Determinar la influencia del conocimiento de las políticas de seguridad en la actitud del empleado hacia las PSI en las organizaciones.</i>	<i>El conocimiento de las políticas de seguridad influye en la actitud del empleado hacia las PSI en las organizaciones.</i>	
<i>¿En qué medida influye el conocimiento de las políticas de seguridad en la intención de cumplimiento de las PSI en las organizaciones?</i>	<i>Determinar la influencia del conocimiento de las políticas de seguridad en la intención de cumplimiento de las PSI en las organizaciones.</i>	<i>El conocimiento de las políticas de seguridad influye en la intención de cumplimiento de las PSI en las organizaciones.</i>	
<i>¿En qué medida influye la intención de cumplimiento en la adopción de las PSI en las organizaciones?</i>	<i>Determinar la influencia de la intención de cumplimiento en la adopción de las PSI en las organizaciones.</i>	<i>La intención de cumplimiento influye en la adopción de las PSI en las organizaciones.</i>	

Fuente: Elaboración Propia

Anexo II.- Encuesta utilizada en la recolección de datos

Parte I

FACTORES DEL ÉXITO QUE INFLUYEN EN LA ADOPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El presente cuestionario se encuentra dirigido al personal de instituciones de administración pública y de empresas privadas, en las cuales se hayan implementado políticas de seguridad de información.

El objetivo de este cuestionario es determinar la influencia de una serie de factores en la adopción de políticas de seguridad de información por parte de los empleados de sus organizaciones. Cada uno de estos factores se encuentra representado por una serie de preguntas que buscan conocer la situación actual de su organización con respecto a la adopción de dichas políticas de seguridad, por lo que debe seleccionar como respuesta a cada una de estas preguntas la opción que represente mejor la situación actual de su organización. Las respuestas se sitúan en un rango de 1 a 5, siendo 1 nunca, 2 casi nunca, 3 algunas veces, 4 casi siempre y 5 siempre.

Note que se respetará el anonimato de su persona y el nombre de su organización, por lo que sólo se tomará en cuenta las respuestas otorgadas por usted a cada una de las preguntas.

***Obligatorio**

Sexo *

☐ Mujer

☐ Hombre

Edad *

Tu respuesta _____

Mayor nivel de Educación *

Elige _____

Empleo Actual *

Tu respuesta _____

Rubro de su Organización

Tu respuesta _____

Línea Organizacional

Elige _____

Años de experiencia laboral

Tu respuesta _____

Aplicación de Políticas

¿Se han aplicado Políticas de Seguridad de Información?

☐ Sí

☐ No

De no haberse aplicado políticas de seguridad, especifique la razón.

Tu respuesta _____

¿Qué estándares de seguridad de información se utilizan en su organización?

☐ ISO 27001

☐ ISO 27002

☐ COBIT

Parte II

I. Severidad de Sanciones a violaciones de Seguridad de Información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Ante una violación de políticas de seguridad de información en mi organización, las sanciones a recibir son muy severas.	☐	☐	☐	☐	☐
Ante una violación de las políticas de seguridad, el infractor tiene problemas como producto de la sanción.	☐	☐	☐	☐	☐
El empleador toma acciones estrictas contra el infractor ante una violación de las políticas de seguridad de información.	☐	☐	☐	☐	☐
Ante la violación repetida de las políticas de seguridad de información, mi organización actúa con el despido del infractor.	☐	☐	☐	☐	☐

II. Certeza de Sanciones a violaciones de seguridad de información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Ante la violación de las políticas de seguridad de información en mi organización, un jefe de área detectará dicha falta.	☐	☐	☐	☐	☐
Si se viola las políticas de seguridad, se incurre en una sanción	☐	☐	☐	☐	☐
Mis superiores comunican de forma explícita que las sanciones seguirán si una política de seguridad de información es violada.	☐	☐	☐	☐	☐
Si se viola una política de seguridad, mi organización aplica una sanción de forma inmediata.	☐	☐	☐	☐	☐

III. Compromiso Organizacional *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Como empleado estoy comprometido con el cumplimiento y promoción de las políticas de seguridad de información.	☐	☐	☐	☐	☐
Mi compromiso con la organización implica el salvaguardar sus activos de información.	☐	☐	☐	☐	☐
Invierto esfuerzos en asegurar el éxito de las políticas de seguridad de información de mi organización.	☐	☐	☐	☐	☐
Me mantengo actualizado de los cambios en las políticas de seguridad de información organizacionales.	☐	☐	☐	☐	☐

IV. Actitud hacia las políticas de Seguridad de Información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Seguir las políticas de seguridad de información de la organización es una necesidad.	☐	☐	☐	☐	☐
Seguir las políticas de seguridad de información de la organización es una buena idea.	☐	☐	☐	☐	☐
Seguir las políticas de seguridad de información de la organización es beneficioso para la organización.	☐	☐	☐	☐	☐
El cumplimiento de las políticas de seguridad de la información es importante para la organización.	☐	☐	☐	☐	☐

V. Autoeficacia del empleado hacia las políticas de Seguridad de Información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Cuento con una habilidad adecuada para prevenir violaciones de seguridad de información en mi lugar de trabajo.	☐	☐	☐	☐	☐
Soy capaz de tomar medidas preventivas para evitar que la gente acceda a mi información confidencial.	☐	☐	☐	☐	☐
Cuento con las habilidades suficientes para protegerme de las violaciones de seguridad de información en mi organización.	☐	☐	☐	☐	☐
Me es fácil habilitar funciones de seguridad en mi computadora de trabajo por mi cuenta.	☐	☐	☐	☐	☐

VI. Severidad percibida de amenazas de seguridad de Información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Cualquier brecha de seguridad de información es un serio problema para mi organización.	☐	☐	☐	☐	☐
Cualquier brecha de seguridad de información en mi organización es un serio problema para mí.	☐	☐	☐	☐	☐
Una violación o daño de mis recursos personales de información en el trabajo es muy peligroso.	☐	☐	☐	☐	☐
Si limito las acciones de un violador de seguridad, habrá serios problemas de seguridad de información para mi organización.	☐	☐	☐	☐	☐

VII. Vulnerabilidad percibida de amenazas de seguridad de información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Mi organización puede estar sujeta a una seria amenaza de seguridad de información.	☐	☐	☐	☐	☐
Puedo estar sujeto a una seria amenaza de seguridad de información.	☐	☐	☐	☐	☐
Puedo ser una víctima de un ataque malicioso si no logro cumplir con las políticas de seguridad de información de mi organización.	☐	☐	☐	☐	☐
Mi organización puede ser vulnerable a brechas de seguridad si no cumpla con las políticas de seguridad de información de mi organización.	☐	☐	☐	☐	☐

VIII. Conciencia de las Políticas de Seguridad de Información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Soy consciente de las reglas y regulaciones detalladas en las políticas de seguridad de información de mi organización.	☐	☐	☐	☐	☐
Soy consciente de mis responsabilidades detalladas en las políticas de seguridad de información para mejorar la seguridad de información de mi organización.	☐	☐	☐	☐	☐
Soy consciente de los riesgos graves que implica violar las políticas de seguridad y cumpla con estas políticas.	☐	☐	☐	☐	☐
Soy consciente de que no debo de acceder a computadoras los cuales no estoy autorizado a usar.	☐	☐	☐	☐	☐

IX. Programa de educación, entrenamiento y conciencia de seguridad (SETA) *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Mi organización provee entrenamiento para ayudarme a mejorar mi conciencia de problemas de seguridad de información.	☐	☐	☐	☐	☐
Mi institución informa de forma periódica sobre las brechas de seguridad de la información a través de campañas de concientización (correo electrónico, folleto / seminario / talleres)	☐	☐	☐	☐	☐
Mi organización me instruye sobre mis responsabilidades de seguridad de información.	☐	☐	☐	☐	☐
Los programas de concientización sobre seguridad de la información de mi institución desarrollan las habilidades necesarias para adoptar un comportamiento y proteger la información.	☐	☐	☐	☐	☐

X. Cultura de seguridad Organizacional *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
La alta gerencia de mi organización considera la seguridad de información una prioridad organizacional importante.	☐	☐	☐	☐	☐
Los gerentes senior de mi organización han articulado una visión clara sobre la seguridad de información.	☐	☐	☐	☐	☐
Los gerentes senior de mi organización han formulado una estrategia clara para alcanzar un alto grado de seguridad de información.	☐	☐	☐	☐	☐
Los gerentes senior de mi organización han establecido metas y objetivos claros para alcanzar un alto grado de seguridad de información.	☐	☐	☐	☐	☐

XI. Intención de Cumplimiento *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Tengo la intención de cumplir con los requerimientos de las políticas de seguridad de información de mi organización.	☐	☐	☐	☐	☐
Tengo la intención de llevar a cabo mis responsabilidades detalladas en las políticas de seguridad de información de mi organización cuando use recursos de información y de tecnología.	☐	☐	☐	☐	☐
Tengo la intención de recomendar a otros que cumplan las políticas de seguridad de información.	☐	☐	☐	☐	☐
Tengo la intención de ayudar a otros a cumplir las políticas de seguridad de información.	☐	☐	☐	☐	☐

XII. Cumplimiento Actual *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Cumplo con las políticas de seguridad de información.	☐	☐	☐	☐	☐
Recomiendo a otros a cumplir las políticas de seguridad de información.	☐	☐	☐	☐	☐
Ayudo a otros a cumplir las políticas de seguridad de información.	☐	☐	☐	☐	☐

XIII. Conocimiento de Políticas de Seguridad de Información *

	Nunca	Casi Nunca	Algunas Veces	Casi Siempre	Siempre
Tengo conocimiento de las políticas de seguridad.	☐	☐	☐	☐	☐
Mi organización ha utilizado conocimientos de seguridad adecuados en la implementación de programas y campañas de seguridad de información.	☐	☐	☐	☐	☐
Los programas de seguridad de información organizados por mi organización han ayudado a mejorar mis conocimientos y habilidades de seguridad de información.	☐	☐	☐	☐	☐

Fuente: elaboración propia