



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

Modelo de comportamiento y su influencia en la intención de cumplimiento de las políticas en el sistema de gestión de seguridad de la información en entidades públicas del estado peruano

TESIS

Para optar el Grado Académico de Magíster en Ingeniería de
Sistemas e Informática con mención en Gestión de Tecnología de
Información y Comunicaciones

AUTOR

Javier LÓPEZ JURADO

ASESOR

Dr. Ciro RODRIGUEZ RODRIGUEZ

Lima, Perú

2026



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

López, J. (2026). *Modelo de comportamiento y su influencia en la intención de cumplimiento de las políticas en el sistema de gestión de seguridad de la información en entidades públicas del estado peruano*. [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	Javier López Jurado
Tipo de documento de identidad	DNI
Número de documento de identidad	10610229
URL de ORCID	https://orcid.org/0009-0005-7535-7674
Datos de asesor	
Nombres y apellidos	Ciro Rodriguez Rodriguez
Tipo de documento de identidad	DNI
Número de documento de identidad	06020241
URL de ORCID	https://orcid.org/0000-0003-2112-1349
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Pedro Martin Lezama Gonzales
Tipo de documento	DNI
Número de documento de identidad	09656793
Miembro del jurado 1	
Nombres y apellidos	William Martin Enriquez Maguiña
Tipo de documento	DNI
Número de documento de identidad	06179457
Miembro del jurado 2	
Nombres y apellidos	Ivan Carlo Petrlik Azabache
Tipo de documento	DNI
Número de documento de identidad	10140461
Datos de investigación	
Línea de investigación	C.0.3.19. Informática y sociedad.
Grupo de investigación	No aplica

Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	Edificio: Facultad de Ingeniería de Sistemas e Informática. País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Calle: Av. Amezaga, Lima 15081 Latitud: -12.053168 Longitud: -77.085563
Año o rango de años en que se realizó la investigación	2021 - 2022
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05



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 DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAGÍSTER EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN
GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES**

A los veintinueve (29) días del mes de mayo de 2026, siendo las 12:00 pm., se reunieron en el Auditorio Alfredo Celso Alva Bravo, el Jurado de Tesis conformado por los siguientes docentes:

Dr. Pedro Martín Lezama Gonzales (Presidente)
Mg. William Martín Enriquez Maguiña (Miembro)
Dr. Ivan Carlo Petrlik Azabache (Miembro)
Dr. Ciro Rodríguez Rodríguez (Miembro Asesor))

Se inició la Sustentación invitando al candidato a Magíster **JAVIER LÓPEZ JURADO**, para que realice la exposición oral de la tesis para optar el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones, siendo la Tesis intitulada:

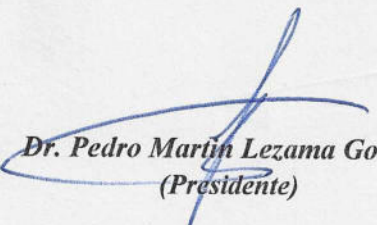
**“MODELO DE COMPORTAMIENTO Y SU INFLUENCIA EN LA INTENCIÓN DE
CUMPLIMIENTO DE LAS POLÍTICAS EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE
LA INFORMACIÓN EN ENTIDADES PÚBLICAS DEL ESTADO PERUANO”**

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:

Dieciséis (17) Muy bueno

Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Bachiller **JAVIER LÓPEZ JURADO** el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones,

Siendo las 13:15 horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.


Dr. Pedro Martín Lezama Gonzales
(Presidente)


Dr. Ivan Carlo Petrlik Azabache
(Miembro)


Mg. William Martín Enriquez Maguiña
(Miembro)


Dr. Ciro Rodríguez Rodríguez
(Miembro Asesor)



Anexo 1

CERTIFICADO DE SIMILITUD

Yo, **Ciro Rodriguez Rodriguez** en mi condición de asesor acreditado con Dictamen N° 000605-2025-UPG-VDIP-FISI/UNMSM de la tesis, cuyo título es **“Modelo de comportamiento y su influencia en la intención de cumplimiento de las políticas en el sistema de gestión de seguridad de la información en entidades públicas del estado peruano”** presentado por el bachiller **Javier López Jurado**, para optar el **Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones**,

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el **12 %** de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del **Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones**.

Lima, 30 de julio de 2026

Firma del Asesor

Nombres y Apellidos del asesor: Ciro Rodriguez Rodriguez
DNI: 06020241

* Según corresponda: bachiller, magíster, doctor; título profesional o título de segunda especialidad

La vigencia del presente certificado corresponde a un período de noventa (90) días desde la fecha de su emisión; siempre que no haya observaciones en el texto durante el proceso de revisión por el jurado informante o surja alguna contingencia.

DEDICATORIA

Este trabajo va dedicado a mis padres, quienes desde el cielo continúan guiando mis pasos y acompañándome en cada etapa de mi vida. Asimismo, lo dedico a mis hermanos, por su apoyo constante y por inculcarme el valor de la perseverancia, enseñándome a luchar por mis objetivos y a alcanzar los logros con humildad y gratitud.

AGRADECIMIENTO

A Dios, por su presencia permanente en mi vida, por otorgarme fortaleza, salud y bienestar, y por estar en cada uno de mis logros.

A mi asesor de tesis, Dr. Ciro Rodriguez Rodriguez, por su orientación académica, valiosas recomendaciones y acompañamiento permanente, los cuales fueron fundamentales para el fortalecimiento y culminación de este trabajo de investigación.

INDICE GENERAL

CAPÍTULO 1: INTRODUCCIÓN.....	1
1.1. SITUACIÓN PROBLEMÁTICA	1
1.2. FORMULACIÓN DEL PROBLEMA	13
1.2.1. PROBLEMA GENERAL	13
1.2.2. PROBLEMAS ESPECÍFICOS.....	13
1.3. JUSTIFICACIÓN TEÓRICA	15
1.4. JUSTIFICACIÓN PRÁCTICA.....	15
1.5. OBJETIVOS.....	16
1.5.1. OBJETIVOS GENERALES	16
1.5.2. OBJETIVOS ESPECÍFICOS.....	16
CAPÍTULO 2: MARCO TEÓRICO.....	18
2.1. MARCO FILOSÓFICO O EPISTEMOLÓGICO DE LA INVESTIGACIÓN	18
2.2. ANTECEDENTES DE INVESTIGACIÓN	18
2.3. BASES TEÓRICAS	37
2.3.1. MARCO TEÓRICO.....	37
2.3.2. MARCO TECNOLÓGICO	45
2.3.3. MARCO REGULATORIO / LEGAL	54
2.3.4. MARCO CONCEPTUAL	56
CAPÍTULO 3: METODOLOGÍA	66
3.1. TIPO DE INVESTIGACIÓN	66

3.1.1.	<i>TIPO DE INVESTIGACIÓN</i>	66
3.1.2.	<i>DISEÑO DE INVESTIGACIÓN</i>	66
3.2.	UNIDAD DE ANALISIS	66
3.3.	POBLACION DE ESTUDIO	66
3.4.	TAMAÑO DE MUESTRA	67
3.5.	SELECCIÓN DE MUESTRA	67
3.6.	TECNICAS DE RECOLECCION DE DATOS	67
CAPÍTULO 4: MODELO DE COMPORTAMIENTO		68
4.1.	DISEÑO DEL MODELO	68
4.2.	DIMENSIONES DEL MODELO FORMULADO	70
4.2.1.	<i>COMPARTIR CONOCIMIENTO DE SEGURIDAD DE INFORMACIÓN</i>	70
4.2.2.	<i>COLABORACIÓN EN SEGURIDAD DE LA INFORMACIÓN</i>	72
4.2.3.	<i>INTERVENCIÓN EN SEGURIDAD DE INFORMACIÓN.</i>	74
4.2.4.	<i>EXPERIENCIA EN SEGURIDAD DE INFORMACIÓN.</i>	78
4.2.5.	<i>APEGO</i>	80
4.2.6.	<i>COMPROMISO</i>	82
4.2.7.	<i>NORMAS PERSONALES</i>	84
4.2.8.	<i>LINEAMIENTOS, NORMATIVIDAD Y PROCEDIMIENTOS DE LA ORGANIZACIÓN</i>	85
4.2.9.	<i>HÁBITOS.</i>	86
4.2.10.	<i>ACTITUD</i>	88
4.2.11.	<i>NORMAS SUBJETIVAS</i>	89
4.2.12.	<i>EVALUACIÓN DE AMENAZAS</i>	91
4.2.13.	<i>EVALUACIÓN DE AFRONTAMIENTO</i>	93

4.3.	HIPÓTESIS	95
4.3.1.	<i>HIPÓTESIS GENERAL</i>	95
4.3.2.	<i>HIPÓTESIS ESPECÍFICA</i>	95
4.4.	IDENTIFICACIÓN DE VARIABLES	96
4.4.1.	<i>VARIABLE INDEPENDIENTE</i>	96
4.4.2.	<i>VARIABLE DEPENDIENTE</i>	97
4.5.	MATRIZ DE CONSISTENCIA	98
4.5.1.	<i>OPERALIZACIÓN DE LA VARIABLE DEPENDIENTE</i>	98
4.5.2.	<i>OPERALIZACIÓN DE LA VARIABLE INDEPENDIENTE</i>	100
CAPÍTULO 5: RESULTADOS Y DISCUSIÓN.....		102
5.1.	ANÁLISIS Y PRESENTACIÓN DE RESULTADOS	102
5.1.1.	<i>DIMENSIONES PARA EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN</i>	102
5.1.1.1.	<i>INTERCAMBIO DE CONOCIMIENTO DE SEGURIDAD DE INFORMACIÓN ...</i>	102
5.1.1.2.	<i>COLABORACIÓN EN SEGURIDAD DE LA INFORMACIÓN</i>	103
5.1.1.3.	<i>INTERVENCIÓN EN SEGURIDAD DE INFORMACIÓN.</i>	103
5.1.1.4.	<i>EXPERIENCIA EN SEGURIDAD DE INFORMACIÓN.</i>	104
5.1.1.5.	<i>AFECTO ORGANIZACIONAL</i>	105
5.1.1.6.	<i>COMPROMISO ORGANIZACIONAL</i>	105
5.1.1.7.	<i>NORMAS PERSONALES (ÉTICA).</i>	106
5.1.1.8.	<i>LINEAMIENTOS, NORMATIVIDAD Y PROCEDIMIENTOS DE LA ORGANIZACIÓN</i>	107
5.1.1.9.	<i>HÁBITO EN LA EVALUACIÓN DE AMENAZAS</i>	107
5.1.1.10.	<i>HÁBITO EN LA EVALUACIÓN DE AFRONTAMIENTO</i>	108
5.1.1.11.	<i>ACTITUD</i>	109
5.1.1.12.	<i>NORMAS SUBJETIVAS</i>	109

5.1.1.13.	<i>EVALUACIÓN DE AMENAZAS</i>	110
5.1.1.14.	<i>EVALUACIÓN DE AFRONTAMIENTO.....</i>	111
5.1.1.15.	<i>INTENCIÓN DE COMPORTAMIENTO DE CUMPLIMIENTO.....</i>	111
5.2.	CONTRASTACIÓN DE HIPÓTESIS	112
5.3.	DISCUSIÓN	116
	CONCLUSIONES	119
	RECOMENDACIONES.....	120

LISTA DE CUADROS

CUADRO 1 INTENCIÓN DE CUMPLIMIENTO DE POLÍTICAS DE UN SGSI	98
CUADRO 2 MODELO DE COMPORTAMIENTO	100
CUADRO 3 RESULTADOS DESCRIPTIVOS	113
CUADRO 4 CORRELACIÓN ENTRE VARIABLES INDEPENDIENTE Y DEPENDIENTE	114
CUADRO 5 CORRELACIÓN ENTRE DIMENSIONES	115

LISTA DE FIGURAS

FIGURA 1	INCIDENTES DE SI POR FACTOR HUMANO EN EL SECTOR SALUD.....	2
FIGURA 2	MECANISMOS TECNOLÓGICOS DE SI	3
FIGURA 3	INCIDENTES MÁS RECURRENTES RELACIONADOS AL FACTOR HUMANO	4
FIGURA 4	INCIDENTES RELACIONADOS A LA INFORMACIÓN	7
FIGURA 5	RAZONES QUE INVOLUCRAN COMPORTAMIENTOS DE RIESGOS	9
FIGURA 6:	APLICACIÓN DE CONTROLES FACTOR HUMANO VS CONTROLES TECNOLÓGICOS	10
FIGURA 7	TIPOS DE INCIDENCIA VOLUNTARIA E INVOLUNTARIA	12
FIGURA 8	CAUSAS FUNDAMENTALES DE LOS INCIDENTES DE SI	13
FIGURA 9	MODELO INTEGRADO POR LA TEORÍA DE LA DISUASIÓN Y LA TEORÍA DE CONTROL SOCIAL	19
FIGURA 10	FACTORES SOBRESALIENTES DE LOS CONTROLES FORMALES E INFORMALES	20
FIGURA 11	MODELO INTEGRADO POR LA TEORÍA DE COMPORTAMIENTO PLANIFICADO, TEORÍA DE MOTIVACIÓN DE PROTECCIÓN Y LA TEORÍA DE CONTROL SOCIAL	22
FIGURA 12	MODELO QUE INTEGRA LA TEORÍA DEL VÍNCULO SOCIAL Y LA TEORÍA DE LA PREVENCIÓN DEL DELITO SITUACIONAL	23
FIGURA 13	PROCESO DE ORIGEN DE AMENAZAS INTERNAS DE SI	24
FIGURA 14	MODELO QUE INTEGRA LA TEORÍA DEL COMPORTAMIENTO PLANIFICADO Y LA TEORÍA DE LA MOTIVACIÓN DE PROTECCIÓN	26
FIGURA 15	MODELO QUE INTEGRA LA TEORÍA DE LA MOTIVACIÓN DE PROTECCIÓN Y LA TEORÍA DEL COMPORTAMIENTO PLANIFICADO	27
FIGURA 16	MODELO QUE INTEGRA LA TEORÍA DE LA CONDUCTA PLANIFICADA Y LA TEORÍA DE LA MOTIVACIÓN DE PROTECCIÓN	29
FIGURA 17	MODELO QUE INTEGRA LA TEORÍA DE LA MOTIVACIÓN DE PROTECCIÓN Y LA TEORÍA DEL COMPORTAMIENTO PLANIFICADO Y EL MODELO DE TRIANDIS .	30

FIGURA 18 MODELO QUE INTEGRA TEORÍA DEL COMPORTAMIENTO PLANIFICADO SE INTEGRÓ CON EL HÁBITO.....	32
FIGURA 19 MODELO EN BASE A LA AMABILIDAD Y LA ESCRUPULOSIDAD	33
FIGURA 20 MODELO ELABORADO EN BASE A LA TEORÍA DEL COMPORTAMIENTO PLANIFICADO	35
FIGURA 21 MODELO QUE INTEGRA LA TEORÍA DE LA DISUASIÓN GENERAL, TEORÍA DE LA ELECCIÓN Y LA TEORÍA DE LA MOTIVACIÓN DE PROTECCIÓN	36
FIGURA 22 ELEMENTOS DE LA TEORÍA DE CONTROL SOCIAL	40
FIGURA 23 FORMAS DE PARTICIPACIÓN	41
FIGURA 24 PREDICTORES DE INTENCIÓN DE COMPORTAMIENTO	42
FIGURA 25 COMPORTAMIENTO DEL FACTOR HUMANO POR NIVELES	43
FIGURA 26 PRIMER COMPONENTE CLAVE DEL CICLO DE VIDA DE LA PSI	47
FIGURA 27 SEGUNDO COMPONENTE CLAVE DEL CICLO DE VIDA DE LA PSI	48
FIGURA 28 TERCER COMPONENTE CLAVE DEL CICLO DE VIDA DE LA PSI.....	48
FIGURA 29 CUARTO COMPONENTE CLAVE DEL CICLO DE VIDA DE LA PSI	49
FIGURA 30 TIPOS DE RIESGOS	50
FIGURA 31 RELACIÓN DE ESTÁNDARES DE LA FAMILIA SGSI.....	51
FIGURA 32 EVOLUCIÓN ISO/IEC 27001	52
FIGURA 33 PROCESO DE GESTIÓN DE RIESGOS.....	54
FIGURA 34 FACTORES DEL MODELO DE COMPORTAMIENTO EN UN SGSI	57
FIGURA 35 DESCRIPCIÓN DE FACTORES DE UN MODELO DE COMPORTAMIENTO	58
FIGURA 36 FACTORES DE MODELO DE ACUERDO CON EL ISO/IEC 27001:2022	59
FIGURA 37 CONCEPTUALIZACIÓN DE LA INTENCIÓN DE CUMPLIMIENTO DE PSI	61
FIGURA 38 VARIABLES QUE INFLUYEN EN LA INTENCIÓN DE COMPORTAMIENTO EFECTIVO.....	62
FIGURA 39 VARIABLES QUE INFLUYEN EN LA INTENCIÓN DE CUMPLIMIENTO DE PSI	64
FIGURA 40 PROPUESTA DE MODELO DE COMPORTAMIENTO EN BASE A TEORÍAS PROBADAS.....	69
FIGURA 41 DIMENSIONES DEL MODELO DE COMPORTAMIENTO	70

FIGURA 42	COMPARTIR CONOCIMIENTO	71
FIGURA 43	COLABORACIÓN EN SI	73
FIGURA 44	COMPONENTE CENTRAL DE INTERVENCIONES	74
FIGURA 45	ACTIVIDADES FUNDAMENTALES EN LA INTERVENCIÓN	75
FIGURA 46	NIVELES DE PROGRAMAS DE INTERVENCIÓN	77
FIGURA 47	IMPORTANCIA DE LA EXPERIENCIA PARA EL CUMPLIMIENTO DEL PSI	79
FIGURA 48	DETERMINANTE CLAVE PARA EL CUMPLIMIENTO DE NORMAS Y POLÍTICAS	81
FIGURA 49	DIMENSIONES DE COMPROMISO ORGANIZACIONAL	83
FIGURA 50	INFLUENCIA DE LAS NORMAS PERSONALES EN EL COMPORTAMIENTO ÉTICO	84
FIGURA 51	PILARES DE LAS POLÍTICAS EN LAS ORGANIZACIONES	85
FIGURA 52	HÁBITOS PAPEL CENTRAL EN LAS VIOLACIONES DE PSI	87
FIGURA 53	FORMACIÓN DE LA ACTITUD PARA CUMPLIMIENTO DE PSI	89
FIGURA 54	FORMACIÓN DE LAS NORMAS SUBJETIVAS PARA EL CUMPLIMIENTO DE PSI	90
FIGURA 55	ORGANIZACIÓN DE EVALUACIÓN DE AMENAZAS PARA EL CUMPLIMIENTO DE PSI	92
FIGURA 56	COMPONENTES DE LA EVALUACIÓN DE AFRONTAMIENTO	94
FIGURA 57	RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN INTERCAMBIO DE CONOCIMIENTO DE SI	102
FIGURA 58	RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN COLABORACIÓN EN SI	103
FIGURA 59	RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN INTERVENCIÓN EN SI	104
FIGURA 60	RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN EXPERIENCIA EN SI	104
FIGURA 61	RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN AFECTO ORGANIZACIONAL	105

FIGURA 62 RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN COMPROMISO	
ORGANIZACIONAL.....	106
FIGURA 63 RESULTADOS CORRESPONDIENTES A LA DIMENSIÓN NORMAS	
PERSONALES (ÉTICA)	106
FIGURA 64 RESULTADOS CORRESPONDIENTES A LA NORMATIVIDAD DE LA	
ORGANIZACIÓN.	107
FIGURA 65 RESULTADOS CORRESPONDIENTES AL HÁBITO EN LA EVALUACIÓN DE	
AMENAZAS	108
FIGURA 66 RESULTADOS CORRESPONDIENTES AL HÁBITO EN LA EVALUACIÓN DE	
AFRONTAMIENTO	108
FIGURA 67 RESULTADOS CORRESPONDIENTES A LA ACTITUD	109
FIGURA 68 RESULTADOS CORRESPONDIENTES A LAS NORMAS SUBJETIVAS	110
FIGURA 69 RESULTADOS CORRESPONDIENTES A LA EVALUACIÓN DE AMENAZAS	110
FIGURA 70 RESULTADOS CORRESPONDIENTES A LA EVALUACIÓN DE	
AFRONTAMIENTO	111
FIGURA 71 RESULTADOS CORRESPONDIENTES A LA INTENCIÓN DE	
COMPORTAMIENTO PARA EL CUMPLIMIENTO.....	112

RESUMEN

El presente estudio analiza el papel determinante del factor humano en un Sistema de Gestión de Seguridad de la información (SGSI), evidenciado que gran parte de los incidentes de seguridad de información (SI) se origina en el incumplimiento de las Políticas de Seguridad de la información (PSI), asociado principalmente a la ausencia de estrategias de SI orientadas al factor humano, generando pérdidas económicas y daño reputacional en las entidades públicas del estado peruano. Teniendo como objetivo formular un modelo de comportamiento en un SGSI que influya en la intención de cumplimiento de las PSI en entidades públicas. Para ello, se empleó un enfoque cuantitativo, con un diseño correlacional, aplicándose instrumentos validados a servidores públicos para medir variables asociadas a actitudes, normas subjetivas, evaluación de amenazas y evaluación de afrontamiento.

En la elaboración del modelo se identificó factores como la participación, el apego, el compromiso y las normas personales; así como también aspectos específicos de la participación, como son el intercambio de conocimiento, la colaboración, la intervención y la experiencia en SI. Adicionalmente, se incorporan la normatividad organizacional y los hábitos como componentes sustentados en la actitud, las normas subjetivas y el control conductual percibido. El modelo se fundamenta en teorías ampliamente validadas sobre el comportamiento humano y los resultados que evidencian una correlación muy fuerte y estadísticamente significativa entre el modelo de comportamiento de SI y la intención de cumplimiento de la PSI ($r = 0.917$; $p < 0.001$). Asimismo, dimensiones como la experiencia ($r = 0.730$), las normas personales vinculadas a la (ética) ($r = 0.751$) y la capacidad percibida de afrontamiento ($r = 0.774$) mostraron asociaciones significativas con la actitud y la intención de cumplimiento.

Palabras Claves: Seguridad de la Información, comportamiento, políticas de seguridad de la información, factor humano.

ABSTRACT

This study analyzes the crucial role of the human factor in an Information Security Management System (ISMS), demonstrating that a large proportion of information security (IS) incidents originate from non-compliance with Information Security Policies (ISPs), primarily associated with the absence of IS strategies focused on the human factor. This results in economic losses and reputational damage for public entities in Peru. The objective is to formulate a behavioral model within an ISMS that influences the intention to comply with ISPs in public entities. To this end, a quantitative approach with a correlational design was employed, applying validated instruments to public servants to measure variables associated with attitudes, subjective norms, threat assessment, and coping mechanisms.

In developing the model, factors such as participation, adherence, commitment, and personal norms were identified, as well as specific aspects of participation, such as knowledge sharing, collaboration, intervention, and IS experience. Additionally, organizational norms and habits are incorporated as components based on attitude, subjective norms, and perceived behavioral control. The model is grounded in widely validated theories of human behavior, and the results demonstrate a very strong and statistically significant correlation between the behavior model of SI and the intention to comply with PSI ($r = 0.917$; $p < 0.001$). Furthermore, dimensions such as experience ($r = 0.730$), personal norms linked to personal standards (ethics) ($r = 0.751$), and perceived coping capacity ($r = 0.774$) showed significant associations with attitude and intention to comply.

Keywords: Information security, behavior, information security policies, human factor.

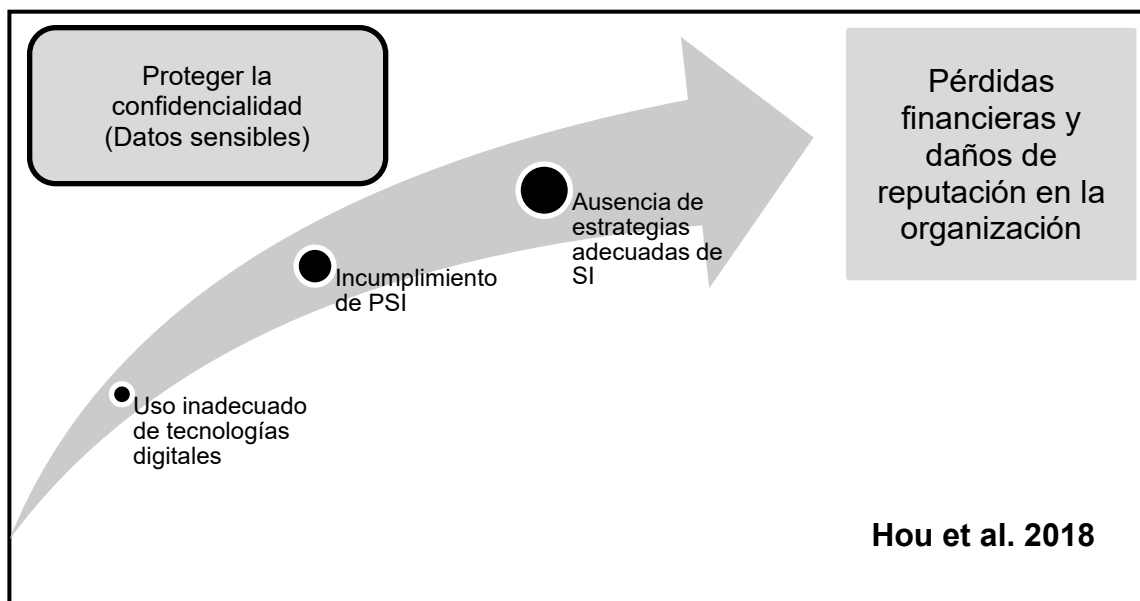
CAPÍTULO 1: INTRODUCCIÓN

1.1. SITUACIÓN PROBLEMÁTICA

En su estudio Chenhui et al. (2020) consideran que a pesar de los avances significativos en las tecnologías de SI, el empleado interno continúa siendo el eslabón más vulnerable en la gestión de la SI dentro de las organizaciones. En virtud de su conocimiento profundo sobre los procesos organizacionales y de los privilegios de acceso otorgados para el desarrollo de sus actividades laborales, el factor humano dentro de las organizaciones puede representar un riesgo potencialmente mayor que el factor humano que se encuentra externamente. Por ello, consideran que los responsables de la SI enfrentan una creciente presión para garantizar el cumplimiento de las PSI, con el fin de proteger los activos de información frente a posibles violaciones cometidas por el propio personal. El estudio advierte que el personal interno se ha convertido en una de las principales fuentes de incidentes relacionados con la SI, evidenciando que el incumplimiento de las PSI por parte de los empleados constituye un riesgo crítico para las organizaciones.

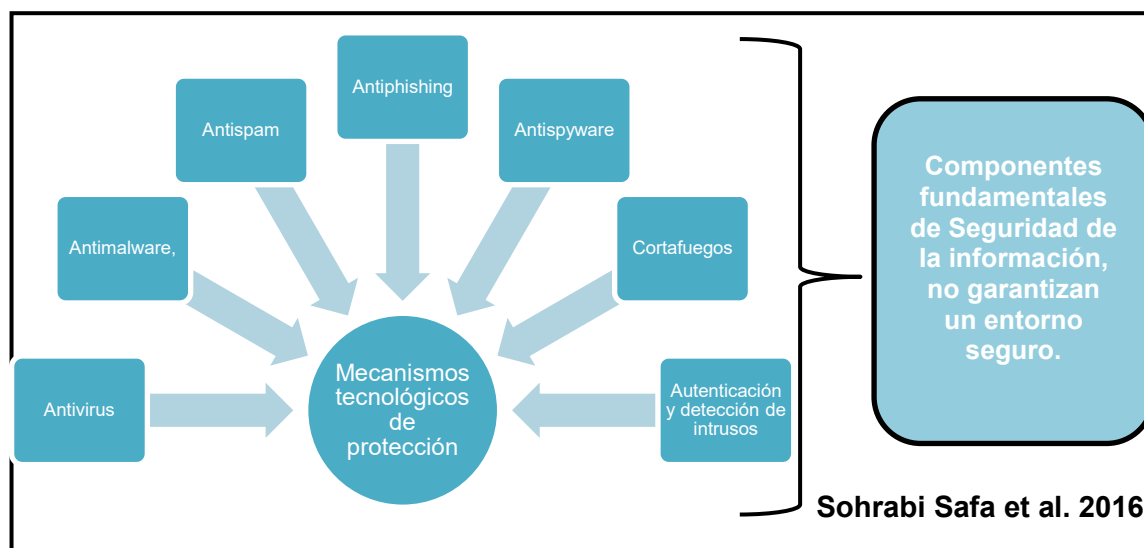
Del mismo modo, Hou et al. (2018), en su estudio desarrollado en el sector salud, evidenciaron que la mayoría de los incidentes de SI son originados por el factor humano (ver figura 1), resaltando la importancia de preservar la confidencialidad de los datos personales de los pacientes, dado que su vulneración puede derivar en costosas demandas legales y posibles daños de reputación, además sostienen que la respuesta estratégica de las organizaciones frente a los requerimientos regulatorios de la SI, está determinada por el nivel de autoconciencia interna respecto a la relevancia de las disposiciones regulatorias y por los incentivos organizacionales para cumplirlas.

Figura 1

Incidentes de SI por factor humano en el sector salud.

Por otra parte, Sohrabi Safa et al. (2016) definen que los mecanismos tecnológicos de protección constituyen componentes fundamentales de la SI, pero no pueden garantizar un entorno seguro para la información en las organizaciones (ver figura 2). En este sentido, los piratas informáticos tienen a dirigir sus acciones hacia el factor humano más que hacia los controles tecnológicos, aprovechando las debilidades asociadas al comportamiento de los usuarios para generar brechas en la SI. También, la investigación considera que la mitigación del riesgo de violaciones de la SI requiere una integración equilibrada entre los controles tecnológicos y la adopción de comportamientos adecuados del factor humano en SI.

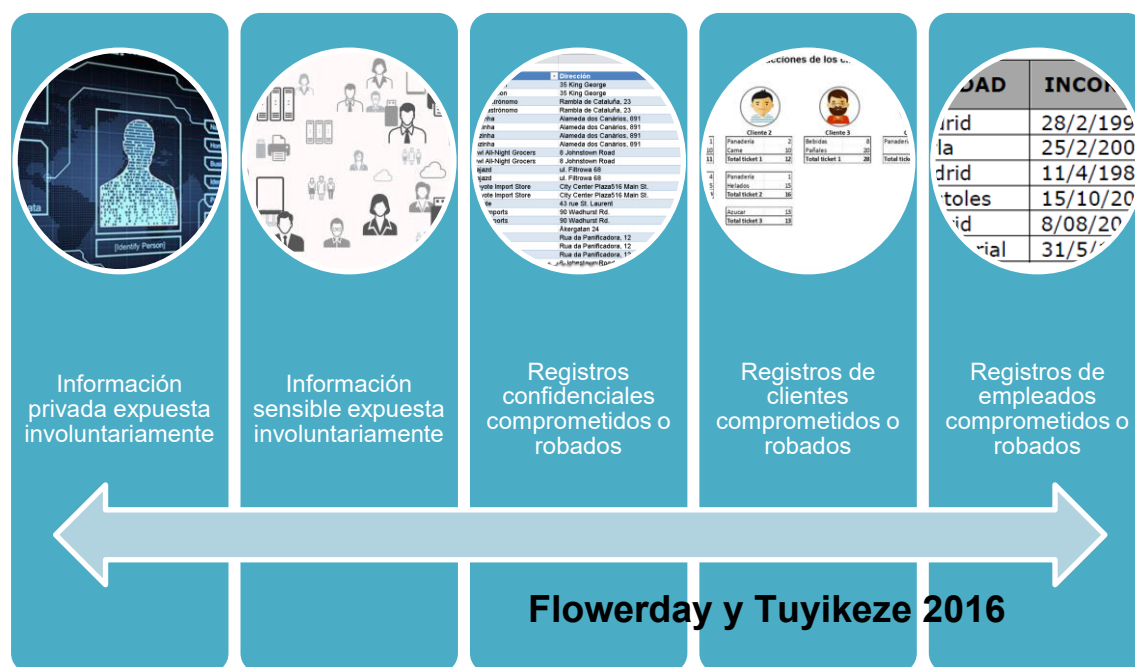
Figura 2

Mecanismos tecnológicos de SI

Para Flowerday y Tuyikeze (2016), consideran que las organizaciones a través del avance del tiempo son más dependientes de las tecnologías digitales, teniendo como resultado el aumento de las amenazas potenciales para los activos de información. Los investigadores identificaron encuestas de ciberdelincuencia en los Estados Unidos de America, encontrando que más daño fue causado por los ataques interno que por los ataques externos, identificando que el factor humano interno de la organización constituyo el porcentaje más alto de incidentes de SI. (ver figura 3)

Figura 3

Incidentes más recurrentes relacionados al factor humano



Además, Chen et al. (2015) evidencian que un número significativo de violaciones de SI se encuentra asociado a la negligencia de los empleados internos y al uso indebido de información privilegiada. Del mismo modo, la creciente exigencia de cumplimiento de los mandatos regulatorios ha impulsado a numerosas organizaciones a establecer programas integrales de SI. Por ello, proponen y validan empíricamente un modelo de investigación orientado a evaluar la influencia de los componentes clave de los programas integrales de SI sobre la cultura de SI. Los resultados del estudio indicaron que los programas de concientización, educación y capacitación en SI ejercen una influencia significativa tanto en el fortalecimiento de la cultura de seguridad como en el nivel de conocimiento de las PSI dentro de las organizaciones.

Por otro lado, Dang-Pham et al. (2017) señalan que durante el proceso de la transformación digital y la continua evolución tecnológica en las organizaciones, resulta fundamental el desarrollo de entornos de trabajo para la SI centrados en el factor humano. Estos entornos permiten que los empleados fortalezcan su

concientización y sensibilización en SI y mejoren sus comportamientos protectores mediante la interacción y la participación en las redes sociales organizacionales. A diferencia de los enfoques tradicionales, que se enfocan principalmente en las percepciones y comportamientos individuales, el estudio propone un análisis basado en redes sociales, examinando directamente el entorno social de los individuos, el cual se configura a partir de las interacciones y relaciones entre los miembros de la organización. El desarrollo de espacios de trabajo orientados a la SI adquiere una relevancia creciente en las organizaciones modernas, en las que los empleados incorporan tecnologías innovadoras que, si bien impulsa la eficiencia y la innovación, también introducen nuevas amenazas de SI. Finalmente, consideran que el desarrollo de lugares de trabajo para la SI está tomando importancia en las organizaciones donde el factor humano llevan las tecnologías innovadoras, junto con las posibles amenazas de SI para el lugar de trabajo, indicando que las organizaciones necesitan de estos centros de trabajo, por lo que fomentara la flexibilidad y capacidad de la innovación sin comprometer la SI.

Para Skorodumov et al. (2015) indican que las nuevas oportunidades y tecnologías innovadoras, si bien impulsan el desarrollo organizacional y social, también generan problemas y riesgos significativos para la SI, los cuales se han consolidado como uno de los desafíos globales contemporáneos con crecientes implicancias de carácter sociológico, político y humano. Debido a esto, la necesidad de proteger tanto a los individuos como a la sociedad en su conjunto frente a los riesgos asociados a la SI se incrementa, promoviendo la búsqueda de medidas y métodos orientados a la reducción de los riesgos humanos derivados de la criminalidad informática. Asimismo, destacan la relevancia de analizar la especificidad y la dinámica de la subcultura hacker, entendida como un grupo de individuos que emplea sus conocimientos técnicos con fines delictivos o maliciosos en el ciberespacio.

Según Flores et al. (2014), señalan que la falta de conocimiento de SI entre los empleados, puede ser explicada por el bajo nivel de participación del personal

especializado en el diseño y establecimiento de controles de SI, lo que puede derivar en la implementación de controles que no se encuentran alineados con las necesidades reales de los usuarios y desarrollan la forma en que se comunican la normatividad orientados a la protección de los activos de información. Aunque las PSI suelen emplearse con este propósito, en muchos casos se configuran como documento estático que reflejan los objetivos de la SI vigentes al momento de su elaboración, además que no son supervisadas ni actualizadas de manera sistemática para adaptarse a los cambios del entorno organizacional y a la aparición de nuevas amenazas externas, resultando difícil lograr y mantener un nivel adecuado de conocimiento en SI entre los empleados. Además, advierten que también puede existir una carencia de conocimiento experto específico entre el personal encargado de brindar los servicios de SI, lo que ocasiona que dichos servicios no resulten pertinentes para el contexto actual ni se implementen de forma efectiva.

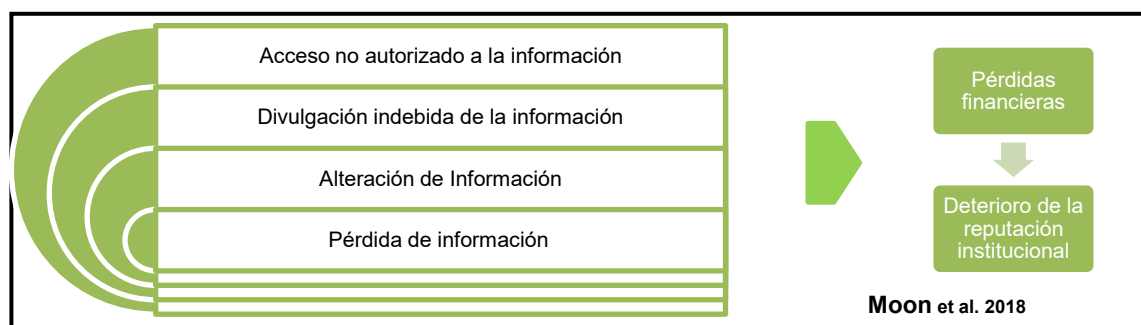
Por otro lado, los autores reconocen que el fortalecimiento de las soluciones tecnológicas ha impulsado a los atacantes a desarrollar nuevas estrategias, especialmente aquellas basadas en la explotación de factores sociales y humanos, dando lugar a la adopción de un enfoque holístico de la gestión de la SI, el cual integra de manera articulada los componentes tecnológicos, organizacionales y sociales. Considerando como rol central al factor humano en la protección de la información, incorporando variables como actitudes, creencias, normas, patrones de conducta, liderazgo, cultura organizacional y niveles de concientización como elementos clave para comprender y fortalecer el cumplimiento de las PSI.

Desde la perspectiva de Moon et al. (2018), plantean que la creciente dependencia de las tecnologías digitales ha intensificado los riesgos asociados a la SI, convirtiéndola en una preocupación permanente debido a las significativas pérdidas financieras y al deterioro de la reputación institucional derivados de los incidentes de SI (ver figura 4), donde las organizaciones se han visto obligadas a reforzar la protección de sus activos de información mediante enfoques

estratégicos de gestión de la SI. El estudio aplica la teoría del capital social para analizar como la alineación social entre los ejecutivos de negocio y los ejecutivos de tecnologías de la información contribuye al fortalecimiento de la SI en las organizaciones, dado que la mayoría de las violaciones de datos y las vulnerabilidades en los sistemas de SI se originan en las acciones u omisiones de los empleados, consolidando el factor humano como uno de los elementos más críticos para la efectividad y sostenibilidad de un sistema de SI en las organizaciones. Otros autores abordaron la problemática del incremento de los incidentes de SI derivados del incumplimiento de las PSI en las Instituciones de Educación Superior a nivel global, particularmente en los países en desarrollo, los cuales presentan una mayor vulnerabilidad frente a este tipo de riesgos. Además, consideran a Malasia como un caso de investigación relevante y escasamente explorado, al tratarse de una economía emergente del sudeste asiático con una estrategia de crecimiento económico fuertemente orientada al uso de tecnologías digitales. Las aspiraciones de desarrollo tecnológico del país, influenciadas por su objetivo de alcanzar el estatus de nación plenamente desarrollada, han impulsado una profunda transformación del sistema educativo mediante la incorporación intensiva de tecnologías (Hina et al. 2019).

Figura 4

Incidentes relacionados a la información



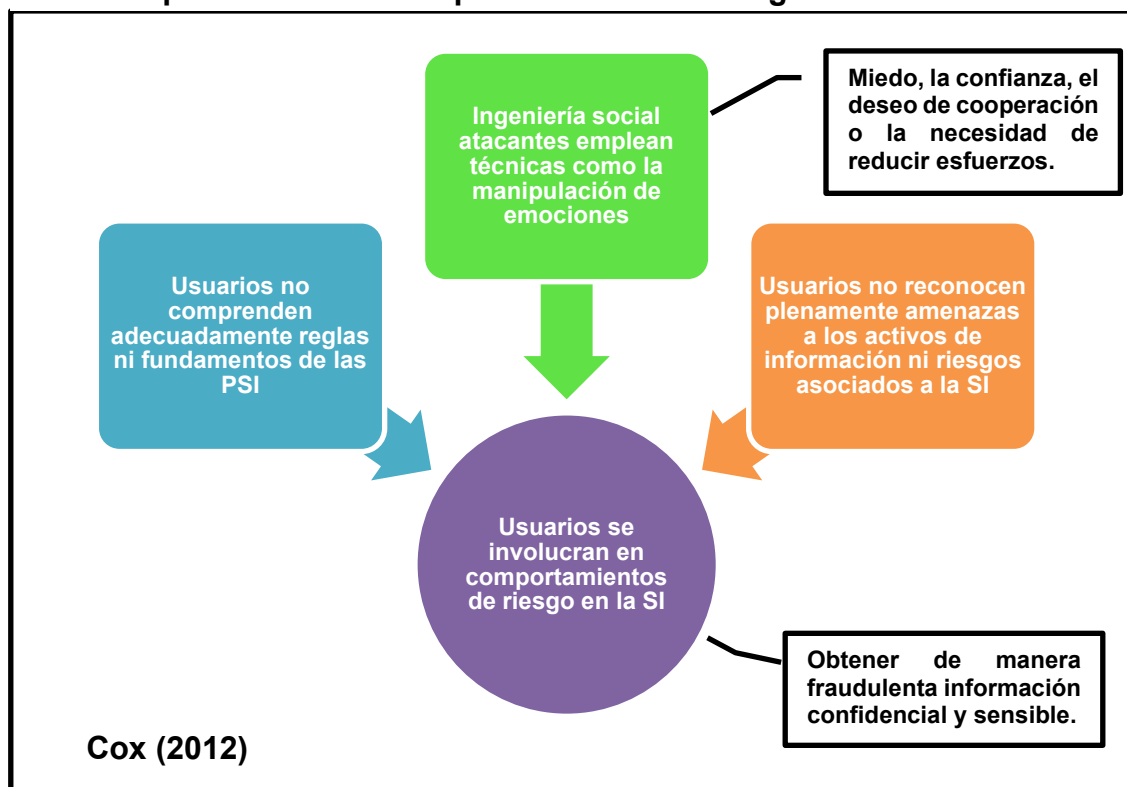
Para Lee et al. (2016), consideran que las decisiones organizacionales orientadas a la protección de los activos de información se encuentran cada vez más condicionadas por las regulaciones gubernamentales y las normas relacionadas a la SI, por el incremento sostenido de las amenazas dirigidas a la

información en las organizaciones, considerando que la SI se ha consolidado como un componente importante. Identificando que la aplicación excesiva de los controles de SI puede generar elevados niveles de estrés en los empleados, lo cual se asocia con efectos negativos, como la disminución de la productividad laboral. El estudio reconoce dos factores principales de estrés: la sobrecarga de trabajo y la percepción de invasión de la privacidad, ambos con un impacto adverso en el cumplimiento de las PSI y de las obligaciones técnicas asociadas, señalando que la sobrecarga de trabajo constituye un factor crítico que afecta directamente a eficacia de la SI, razón por la cual la implementación de sistemas de SI debe considerar cuidadosamente la carga laboral adicional que imponen a los empleados, así como los controles relacionados con la privacidad, que repercute en el comportamiento del factor humano en el cumplimiento de las PSI.

A su vez, Cox (2012), identifica múltiples razones por las cuales los usuarios se involucran en comportamientos de riesgo en la SI (ver figura 5). Denominaron comportamiento omisivos o brecha entre el saber y el hacer posicionando al usuario final como el eslabón más vulnerable en un sistema de SI, afectando a los pilares de la SI como la disponibilidad, confidencialidad e integridad de la información, así como los intereses de los involucrados en un sistema de SI. Por lo que los usuarios de servicios digitales pueden incurrir de forma intencional o no intencional, en conductas de riesgo que debilitan los controles de SI existentes o exponen información sensible, generando daños severos tanto a la reputación organizacional como, potencialmente, al cliente y otras partes interesadas.

Figura 5

Razones que involucran comportamientos de riesgos



Por otro lado, Furnell y Clarke (2012), evidencian que los aspectos relacionados al factor humano tienden a recibir una atención significativamente menor a los controles tecnológicos (ver figura 6). Atribuyendo esta diferencia a que los factores humanos resultan considerablemente más complejos de abordar, dado que no pueden gestionarse de manera inmediata mediante soluciones basadas exclusivamente en productos tecnológicos. Por otro lado, otras investigaciones señalan que la negligencia de los empleados y el uso indebido de información privilegiada constituyen algunas de las principales amenazas para la SI, tales como el uso inapropiado de computadoras, recursos de red, contraseñas y correo electrónico relacionados a comportamientos del factor humano, que no pueden ser mitigados exclusivamente mediante soluciones tecnológicas de SI. Estos comportamientos requieren ser regulados a través de las PSI, las cuales se conciben como declaraciones formales que establecen las funciones y

responsabilidades de los empleados para la protección de los activos de información dentro de las organizaciones (Chen et al. 2018).

Figura 6:

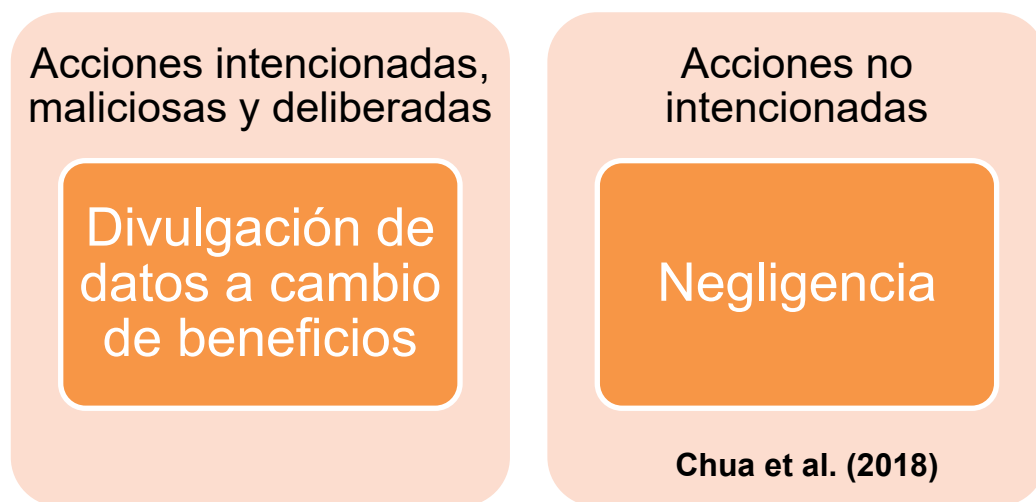
Aplicación de controles factor humano vs Controles tecnológicos



Por su parte, Van Slyke y Bélanger (2020) identifican al factor humano como uno de los eslabones más vulnerables de la SI y proponen diversas razones que explican los comportamientos de riesgo, entre las que destacan el nivel de esfuerzo requerido para cumplir con los controles de seguridad, la falta de conocimiento y la ausencia de un sentido de responsabilidad. Desarrollando una perspectiva analítica innovadora que explica la interacción entre los individuos y los artefactos asociados a la SI que incluyen políticas, controles técnicos, controles físicos, controles operativos y sistemas de información, en el marco de la implementación de un sistema de SI centrado en el cumplimiento de las PSI, señalando que este enfoque es aplicable a una gran cantidad de contextos relacionados con el comportamiento en la SI.

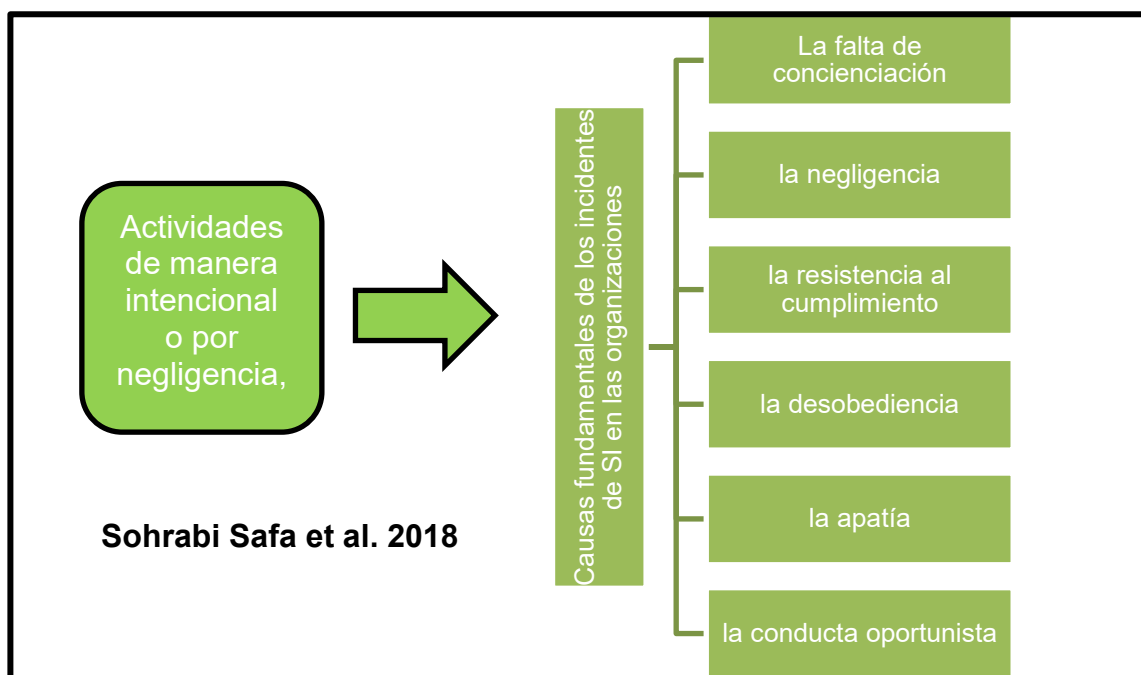
Por otro lado, Chua et al. (2018), plantean que las organizaciones deben identificar e implementar mecanismos efectivos para gestionar a los empleados que tienen acceso a los datos de los clientes, dado que la privacidad se ha consolidado como uno de los desafíos más relevantes en materia de SI, resultando que es indispensable que las organizaciones presten mayor atención

a las estrategias orientadas a garantizar comportamientos de cumplimiento en todos los niveles del personal. Consideraron que una gran cantidad de información sensible de los clientes es manipulada por empleados con capacidad para acceder, utilizar y compartir dichos datos, por lo que las filtraciones de información pueden producirse tanto por acciones maliciosas y deliberadas, o no intencionadas (ver figura 7). En términos generales, los incidentes de violaciones de SI ocasionados por la negligencia de los empleados han generado pérdidas millonarias a las organizaciones, que genero la importancia de fortalecer la gestión del factor humano, determinando que los empleados suelen ser identificados como el eslabón más vulnerable de la SI, principalmente debido a limitaciones en su conocimiento y en su nivel de concienciación y sensibilización sobre la importancia del cumplimiento de las PSI. Del mismo modo otros estudios han centrado su atención en el factor humano, al ser considerado uno de los eslabones mas vulnerables de la SI, utilizando las PSI como un instrumento clave para definir las expectativas de comportamiento de los distintos actores organizacionales como los usuarios finales, el personal de tecnologías digitales, los contratistas y los tomadores de decisiones involucrados con la SI. Asimismo, aseguran que los usuarios suelen no adoptar practicas seguras debido a la falta de conciencia sobre los riesgos, al desconocimiento de las implicaciones derivadas de las violaciones de SI o la escasa comprensión de cómo se espera que actúen en el marco de las políticas establecidas (Tsohou et al. 2015).

*Figura 7***Tipos de incidencia voluntaria e involuntaria**

Sohrabi Safa et al. (2018), sostiene que los usuarios, ya sea de manera intencional o por negligencia, constituyen una fuente significativa de riesgo potencial para los activos de información (ver figura 8), señalando que los ataques originados por personas con información privilegiada pueden generar consecuencias graves para el funcionamiento adecuado de las tecnologías digitales. Plantean que diversos actores internos, como los auditores, clientes, empleados permanentes o temporales, exempleados y proveedores suelen contar con acceso legítimo a uno o varios sistemas de información, generalmente a través de mecanismos de autenticación formal a diferencia de los atacantes externos, los usuarios con información privilegiada no requieren invertir grandes esfuerzos ni tiempo adicional para acceder a la información objetivo, lo que incrementa el nivel de riesgo asociado. Además, la confianza organizacional depositada en estos actores y el grado de anonimato con el que pueden operar reducen la probabilidad de detección de conductas indebidas. Concluyendo que la gestión de las amenazas internas a la SI debe centrarse; en las actitudes, las intenciones y los comportamientos de los empleados, reconociendo al factor humano como un elemento crítico en la protección de la información dentro de las organizaciones.

Figura 8

Causas fundamentales de los incidentes de SI

Según Moona et al. (2018), como la mayoría de las violaciones de datos y las vulnerabilidades de un sistema de SI, se producen debido al factor humano, se convierte en uno de los elementos más críticos en la efectividad de un sistema de SI.

1.2. FORMULACIÓN DEL PROBLEMA**1.2.1. PROBLEMA GENERAL**

¿Cómo un modelo de comportamiento influye en la intención de cumplimiento de las políticas en un Sistema de Gestión de Seguridad de la Información (SGSI) en entidades públicas del estado peruano?

1.2.2. PROBLEMAS ESPECÍFICOS

¿Cómo influye el intercambio de conocimiento en seguridad de información con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye la colaboración en seguridad de información con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye la intervención en seguridad de información al personal con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye la experiencia en seguridad de la información adecuada con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye el apego organizacional con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye el compromiso organizacional con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye las normas personales (ética) con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye los lineamientos, normatividad y procedimientos de la organización en las normas subjetivas de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye el hábito en la evaluación de amenazas de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye el hábito en la evaluación de afrontamiento de la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye la actitud en la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye las normas subjetivas en la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye la evaluación de amenazas en la intención de cumplimiento de las políticas en un SGSI?

¿Cómo influye la evaluación de afrontamiento en la intención de cumplimiento de las políticas en un SGSI?

1.3. JUSTIFICACIÓN TEÓRICA

La presente investigación contribuye con la propuesta de un Modelo de comportamiento en un SGSI que influya positivamente en la intención de cumplimiento de las PSI, donde el factor humano representa el principal origen de incidentes de SI. Se realizó el estudio de diferentes factores que influyan en el comportamiento hacia la SI como el intercambio de conocimientos, la colaboración, la intervención y la experiencia en SI; el compromiso organizacional, el apego organizacional y las normas personales (Ética), lineamientos, normatividad y procedimientos de la organización y el hábito en las entidades públicas del estado peruano la cual será importante para la protección de su información.

La validación de las teorías más significativas y probadas que influiran en la intención del cumplimiento de las PSI, tal como la Teoría de Vinculo Social, Teoría de Comportamiento Planificado y la Teoría de Motivación de Protección, que son teorías con enfoque interdisciplinario que permiten mejorar la visión global en las diferentes disciplinas, así como también en investigaciones relacionadas al comportamiento humano en la intención de cumplimiento de las PSI, en base a los diferentes aspectos que influyen de acuerdo a las teorías desarrolladas.

1.4. JUSTIFICACIÓN PRÁCTICA

La propuesta de un modelo de comportamiento que sea aplicado a la organización permitirá mejorar la participación del factor humano en el cumplimiento de PSI (normas, lineamientos, directivas, instructivos y procedimientos de SI) en un SGSI, asimismo, permitirá reducir los riesgos generados por el factor humano frente a la información sensible e importante de las entidades públicas que gestionan información estratégica del estado peruano.

La investigación propone un modelo orientado a incrementar la intención de cumplimiento de las PSI por parte del factor humano, frente a un contexto donde los incidentes de seguridad continúan representando riesgos críticos para la continuidad operativa, la protección de datos personales, la confianza ciudadana y la integridad de los servicios públicos, optimizando la implantación de los SGSI en las entidades públicas del estado peruano mejorando la protección de la información, incrementando las capacidades y el nivel de conocimiento de la SI y mejorando la cultura en SI.

Finalmente, la propuesta aporta valor práctico porque puede integrarse en los sistemas de gestión actuales (como la normatividad digital actual como los lineamientos de la PCM, el Decreto Legislativo 1412, las medidas mínimas de seguridad TIC y la Política Nacional de Transformación Digital), permitiendo a las entidades públicas fortalecer su capacidad de prevención, respuesta y disuasión ante incidentes. Esto contribuye directamente a la protección de los activos de información, a la reducción de riesgos institucionales y al incremento de la calidad de los servicios ofrecidos a la ciudadanía, convirtiendo al modelo en una herramienta estratégica aplicable, útil y necesaria para la realidad del sector público peruano.

1.5. OBJETIVOS

1.5.1. OBJETIVOS GENERALES

Formular un modelo de comportamiento que influya en la intención de cumplimiento de las políticas en un Sistema de Gestión de la Seguridad de la Información en entidades públicas del estado peruano.

1.5.2. OBJETIVOS ESPECÍFICOS

Determinar cómo influye el intercambio de conocimiento de seguridad de la información con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye la colaboración en seguridad de la información con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye la intervención en seguridad de información al personal con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye la experiencia en seguridad de la información adecuada con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye el apego organizacional con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye el compromiso organizacional con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye las normas personales (ética) con la actitud positiva de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye los lineamientos, normatividad y procedimientos de la organización en las normas subjetivas de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye el hábito en la evaluación de amenazas de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye el hábito en la evaluación de afrontamiento de la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye la actitud en la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye las normas subjetivas en la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye la evaluación de amenazas en la intención de cumplimiento de las políticas en un SGSI.

Determinar cómo influye la evaluación de afrontamiento en la intención de cumplimiento de las políticas en un SGSI.

CAPÍTULO 2: MARCO TEÓRICO

2.1. MARCO FILOSÓFICO O EPISTEMOLÓGICO DE LA INVESTIGACIÓN

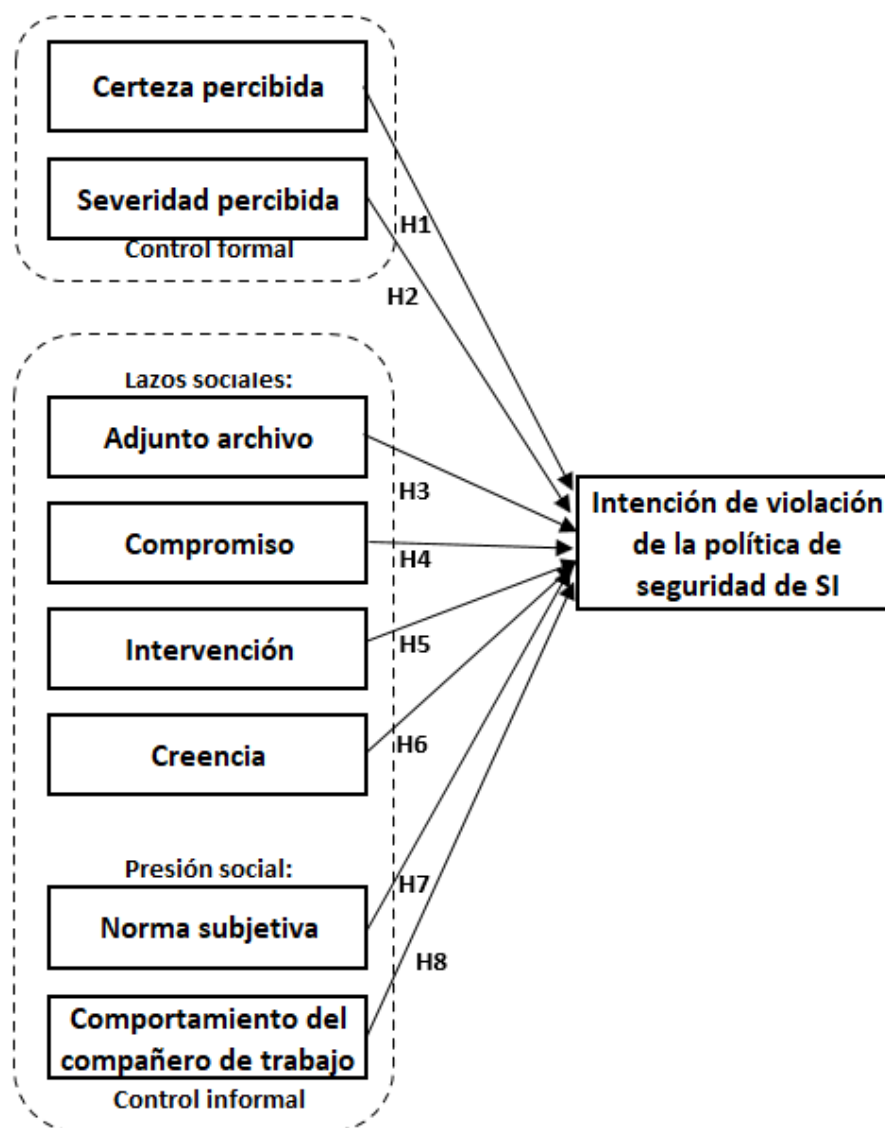
En esta investigación conceptualizamos un modelo conceptual que muestra el cumplimiento de las PSI en las organizaciones. Los conceptos de la teoría de la participación, teoría de vínculo social SBT, teoría del comportamiento planificado TPB y la teoría de la motivación de la protección PMT, compuesta por 3 partes principales. La primera parte analizaremos las dimensiones de la actitud que se compone por la participación que se presenta como (intercambio de conocimiento, la colaboración, la intervención y la experiencia en SI), apego, el compromiso y normas personales, la segunda parte analizaremos las dimensiones de la norma subjetiva como los lineamientos, normatividad y procedimientos de la organización y en la tercera parte analizaremos las dimensiones del control conductual percibido (Evaluación de Amenazas y Evaluación de Afrontamiento) como son los hábitos.

2.2. ANTECEDENTES DE INVESTIGACIÓN

En su investigación Cheng et al. (2013) desarrollo un modelo teórico en base a la integración de los modelos de disuasión y teorías de vínculo social, tal como se observa en la figura 9, que incorpore una nueva perspectiva para comprender mejor el comportamiento del factor humano en el cumplimiento de las PSI.

Figura 9

Modelo integrado por la Teoría de la disuasión y la Teoría de control social

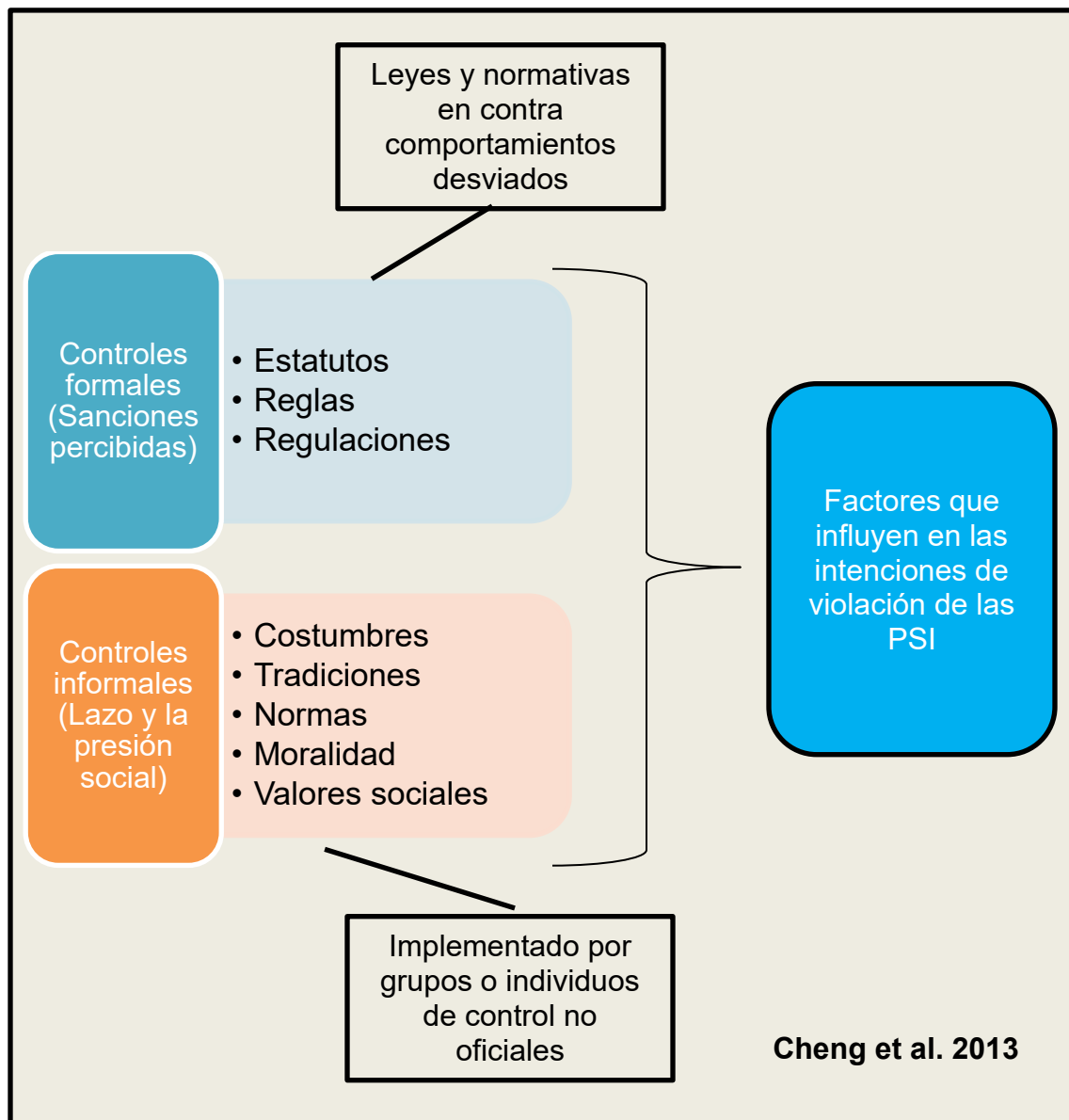


Buscaron los factores sobresalientes de los controles formales e informales que son fundamentales y críticos (ver figura 10), que influyen en el comportamiento de los empleados en las organizaciones. Que tuvo como objetivo un estudio sobre los factores que influyen en las intenciones de violación de las PSI a través de teorías de prueba vinculadas al comportamiento de los empleados en una

organización. Usaron dos formas básicas como el control social formal y el control social informal.

Figura 10

Factores sobresalientes de los controles formales e informales

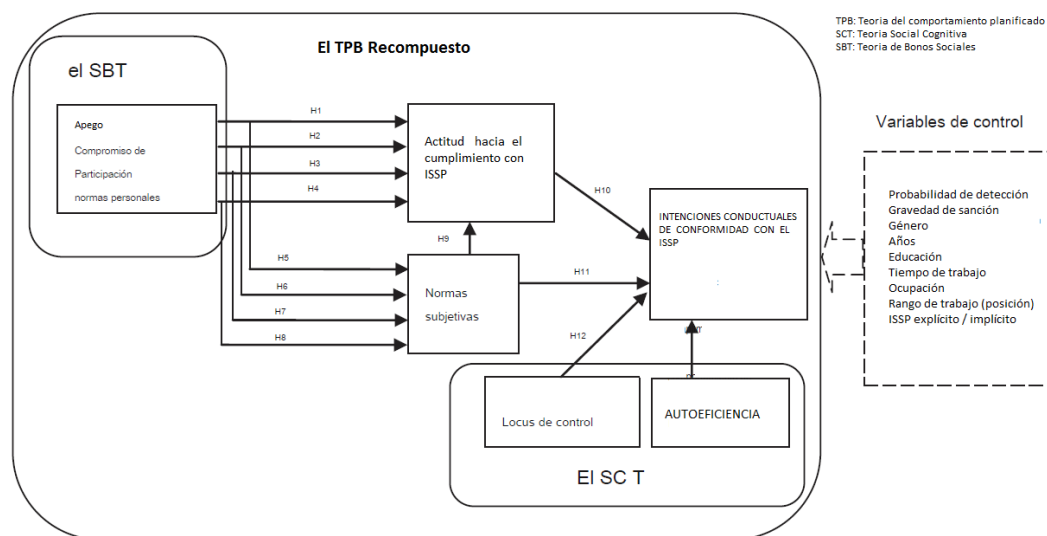


Ifinedo (2014), propone un modelo de investigación que fortalece la comprensión de los factores sociales, organizacionales y psicológicos que promueven el cumplimiento de las PSI por parte de los empleados (ver figura 11), explicando de manera más integral los factores organizacionales y psicosociales que pueden

incentivar o reforzar conductas alineadas con la SI en el lugar de trabajo. Adoptando los principales constructos de la Teoría del control Social, tales como el apego a la organización, el compromiso con las políticas y planes organizacionales, la participación en las prácticas de SI y la convicción personal de que el cumplimiento de las PSI es fundamental para la protección de los activos de información de la organización. El autor desarrolló una investigación orientada a complementar los estudios emergentes basados en la teoría de la socialización y la psicología social, con el propósito de comprender el cumplimiento de las PSI en el contexto organizacional, fundamentada en la Teoría del Comportamiento Planificado (TPB) y en la Teoría Cognitiva Social (SCT), la cual sostiene que los comportamientos humanos son el resultado de una interacción simultánea y dinámica entre factores personales, sociales y ambientales, lo que permite explicar una amplia gama de conductas, incluidos los comportamientos asociados al cumplimiento de las PSI. Donde integra una versión ampliada de la TPB con la Teoría del Control Social, dado que esta última resulta particularmente adecuada para adaptar el modelo conductual a entornos laborales en los que los vínculos sociales influyen significativamente en las percepciones, actitudes y comportamientos relacionados con el trabajo.

Figura 11

Modelo integrado por la teoría de comportamiento planificado, Teoría de motivación de protección y la Teoría de control social

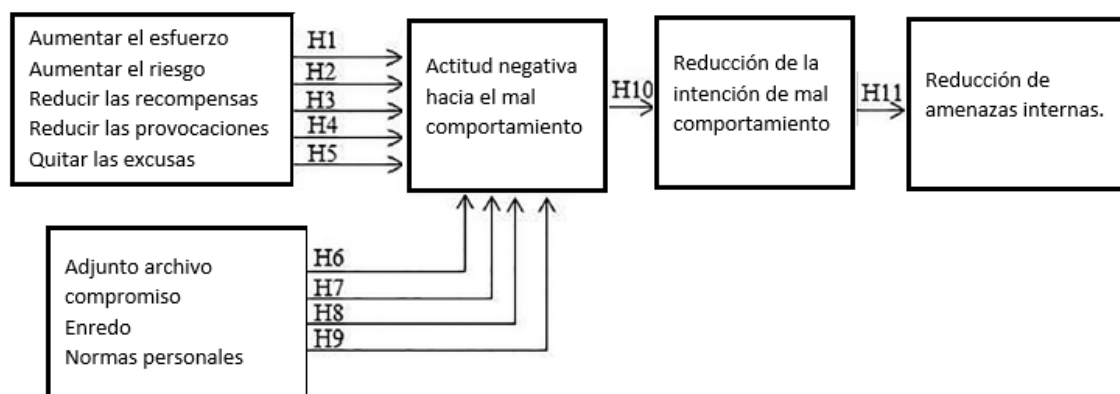


Por su parte, Sohrabi Safa et al. (2017) desarrollaron un modelo orientado a la reducción de las amenazas internas a la SI, fundamentado en los conceptos de motivación y oportunidad, donde integraron dos enfoques teóricos para explicar este fenómeno: la Teoría de control Social (SBT), utilizada para debilitar la motivación de los individuos a incurrir en conductas indebidas, y la Teoría de la Prevención del Delito Situacional (SCPT), orientada a limitar las oportunidades para la comisión de infracciones relacionadas con la SI (Ver figura 12). Asimismo, tuvo como objetivo analizar si el incremento del esfuerzo requerido y del riesgo percibido para ejecutar conductas inapropiadas, así como la reducción de las recompensas, la disminución de las provocaciones y la eliminación de excusas o racionalizaciones asociadas a la mala conducta factores derivados de la SCPT contribuyen efectivamente a la mitigación de las amenazas internas en las organizaciones. La investigación examinó el papel de variables propias de la SBT, tales como el apego del empleado a la organización, su compromiso con los objetivos institucionales, su participación en actividades de SI y sus normas

personales frente a las amenazas internas, como determinantes del comportamiento seguro.

Figura 12

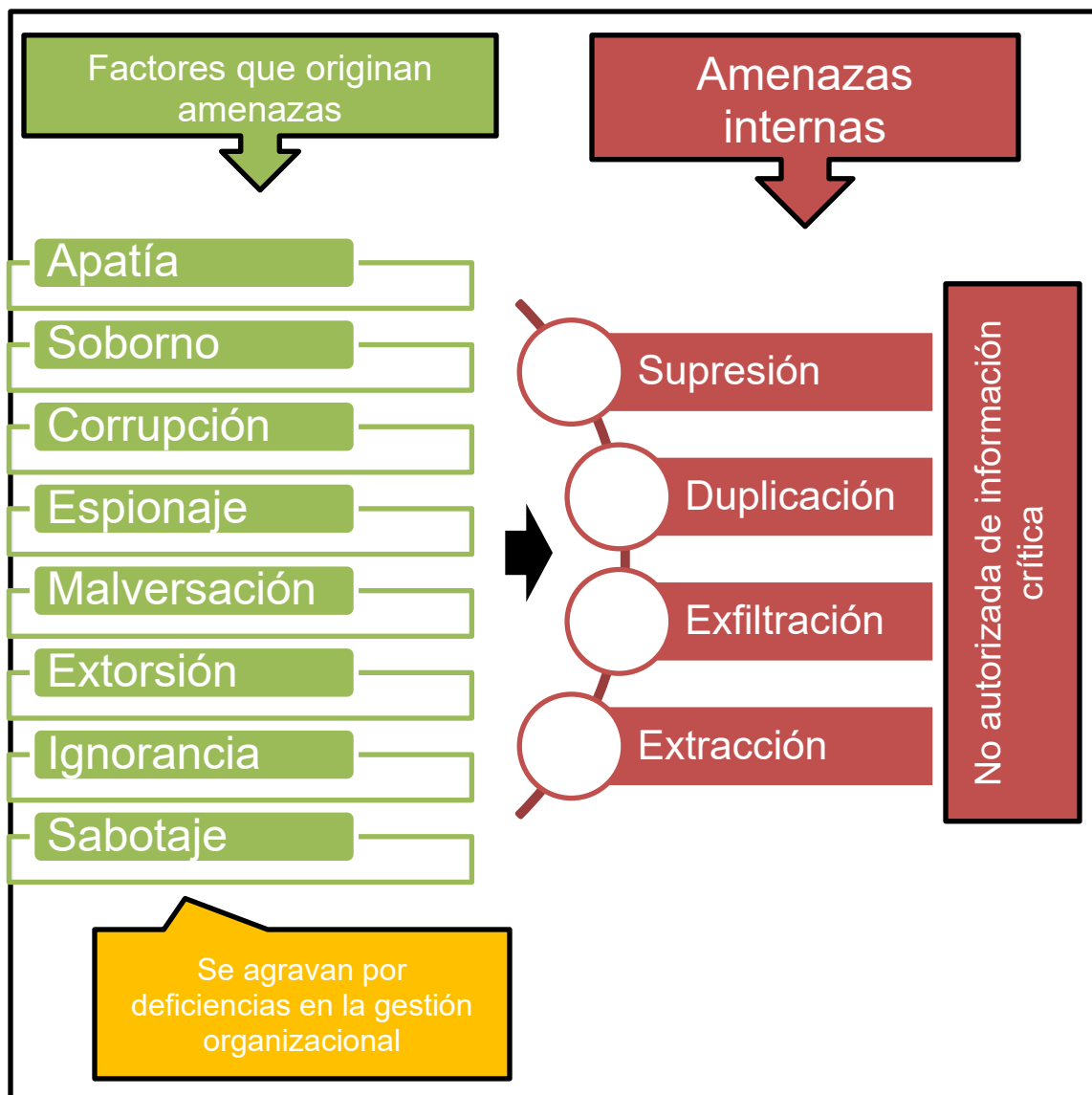
Modelo que integra la Teoría del vínculo social y la Teoría de la prevención del delito situacional



Los investigadores indican que las amenazas internas representan un riesgo significativo para los pilares de la SI como confidencialidad, la integridad y la disponibilidad de la información. Entre sus manifestaciones más comunes se encuentran la supresión, duplicación, exfiltración y extracción no autorizada de información crítica (Ver figura 13). Las causas de estas amenazas incluyen factores que pueden verse agravados por deficiencias en la gestión organizacional en la SI. Por lo que se concluye que tanto la motivación como la oportunidad desempeñan un papel determinante en la violación de normas y regulaciones de SI, por lo que su abordaje simultáneo resulta esencial para fortalecer la postura de seguridad organizacional y reducir la incidencia de amenazas internas.

Figura 13

Proceso de origen de amenazas internas de SI

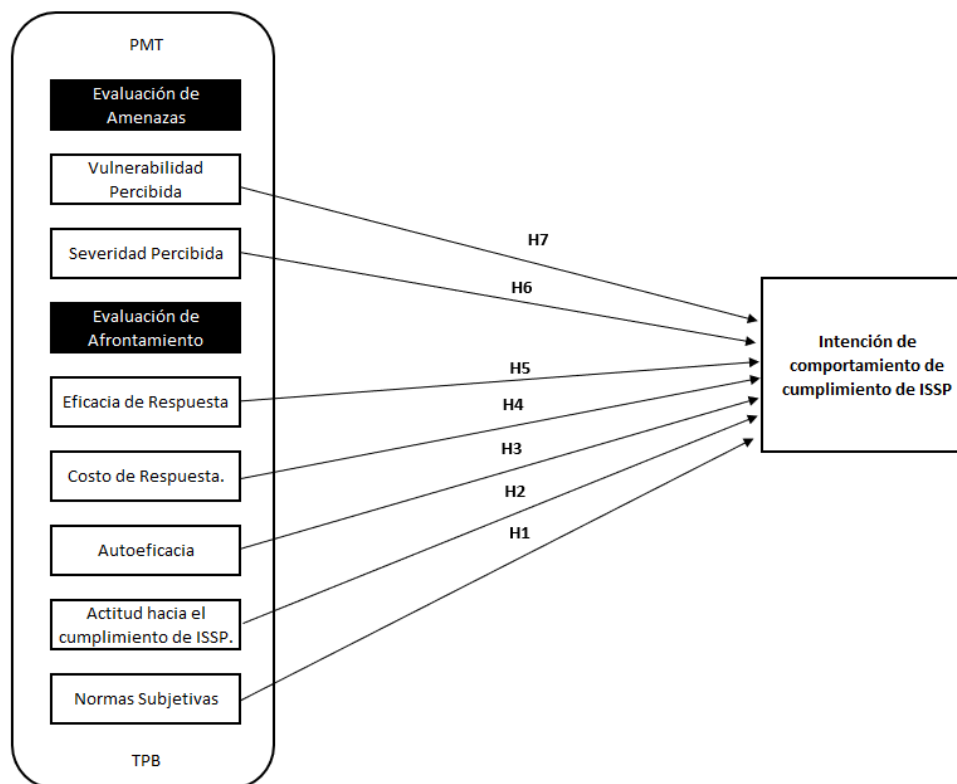


Por otro lado, Ifinedo (2012) investigó el cumplimiento de las PSI a partir de la integración de dos teorías ampliamente reconocidos: la Teoría del Comportamiento Planificado TPB y la Teoría de la Motivación de Protección PMT (ver figura 14). A través de un modelo de investigación que fusiona los principales constructos de ambas teorías, demostrando que la intención conductual de cumplimiento de las PSI es explicada de manera significativa por las variables

independientes. La articulación de ambos marcos teóricos permitió una comprensión más integral de los factores que influyen en el comportamiento de cumplimiento de los empleados relacionados a la SI. Resalta la relevancia de la TPB y la PMT al evidenciar que factores como la autoeficacia percibida, la eficacia de la respuesta, las normas sociales, la actitud hacia el cumplimiento y la vulnerabilidad percibida influyen positivamente en el comportamiento de cumplimiento de las PSI. En conformidad con los postulados de las teorías, los hallazgos indican que la intención conductual de cumplimiento se encuentra condicionada por imperativos sociales, actitudes individuales, la percepción de amenazas y las evaluaciones de afrontamiento realizadas por los empleados. El autor aporta evidencia empírica adicional a la literatura existente, al confirmar que variables como la autoeficacia, la eficacia de la respuesta, las normas sociales, la actitud hacia el cumplimiento y la vulnerabilidad percibida ejercen efectos significativos sobre el cumplimiento efectivo de las PSI en las organizaciones.

Figura 14

Modelo que integra la Teoría del comportamiento planificado y la teoría de la motivación de protección

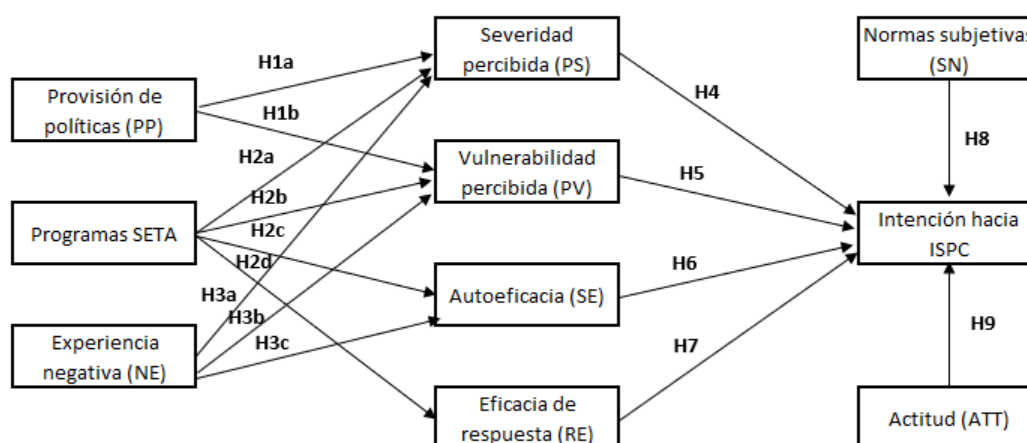


Según Hina et al. (2019), el cumplimiento de las PSI en las organizaciones puede explicarse mediante la integración de factores provenientes de dos teorías conductuales en el ámbito de la SI: la Teoría de la Motivación de Protección PMT y la Teoría del Comportamiento Planificado TPB, incorporando adicionalmente elementos propios de la gobernanza institucional. Con base en este enfoque, los autores diseñaron un modelo híbrido (PMT / TPB) orientado a explicar la intención conductual de cumplimiento de las PSI en contextos organizacionales (ver figura 15). Integraron constructos centrales de ambas teorías conductuales junto con tres factores críticos de gobernanza institucional: la provisión formal de políticas de seguridad de la información, los programas de educación, capacitación y

sensibilización en SI (SETA¹), y la experiencia negativa previa relacionada con incidentes de SI. Estos factores fueron incorporados con el propósito de evaluar de manera integral su influencia sobre la intención de los empleados de cumplir con las PSI. Los resultados de la investigación destacan que el comportamiento aceptable en SI no depende exclusivamente de la implementación de herramientas y controles tecnológicos, sino que constituye una combinación entre la adopción de medidas técnicas integrales y la intención consciente y deliberada de los empleados de cumplir con las PSI de la organización. Desde esta perspectiva, el cumplimiento normativo en materia de SI se configura como un fenómeno colaboración y pertenencia, en el que la regulación interna, la formación, la cultura institucional y la motivación individual desempeñan un papel determinante.

Figura 15

Modelo que integra la Teoría de la motivación de protección y la Teoría del comportamiento planificado



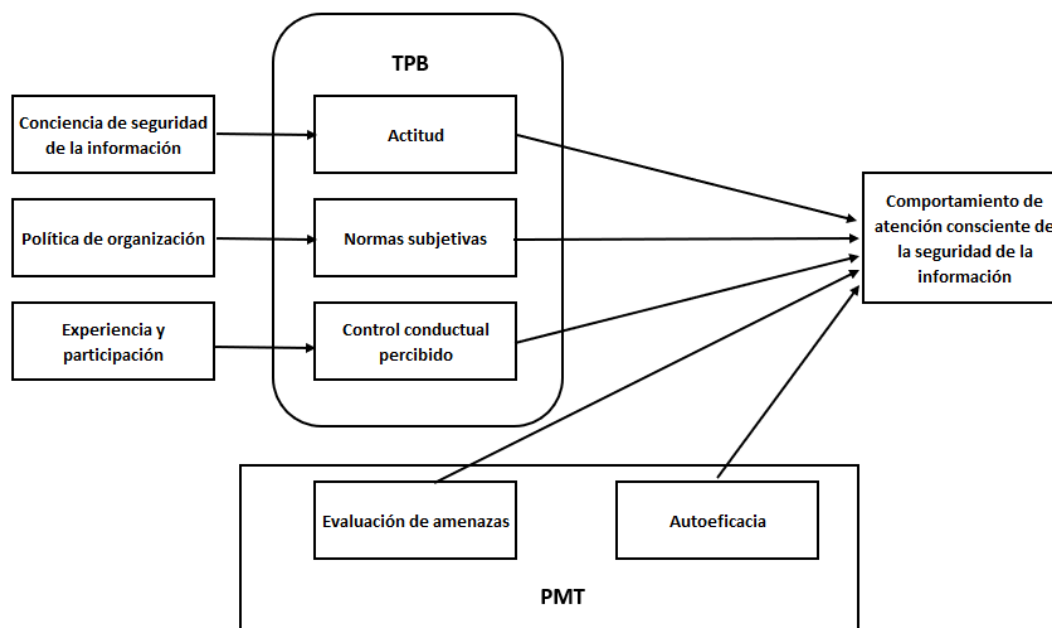
¹ SETA (Security education, training, and awareness / Educación, capacitación y concientización sobre seguridad)

Sohrabi Safa et al. (2015), propone un modelo innovador que explica la formación del comportamiento consciente de SI a partir de la interacción entre la conciencia de seguridad, las políticas organizacionales, la experiencia y el involucramiento del usuario, así como variables conductuales clave como la actitud, las normas subjetivas, la evaluación de amenazas y la autoeficacia. Sustentada en dos teorías fundamentales: la Teoría del Comportamiento Planificado TPB y la Teoría de la Motivación de Protección PMT, que constituyen el eje estructural del modelo propuesto (ver figura 16). A partir de estas teorías, los autores explican cómo el comportamiento de los usuarios puede evolucionar desde prácticas descuidadas hacia conductas conscientes y responsables en SI, evidencian que la conciencia de SI influye significativamente en la actitud del usuario hacia la adopción de comportamientos seguros. Por lo tanto, las políticas inciden directamente en la formación de normas subjetivas que orientan el comportamiento de cuidado consciente, la experiencia previa y el grado de participación de los usuarios influyen en su percepción de que adoptar conductas seguras no constituye una tarea compleja dentro del entorno organizacional.

El modelo incorpora los postulados de la PMT para comprender el papel de las apelaciones al miedo y los mecanismos mediante los cuales los individuos enfrentan las amenazas. Se distinguen dos procesos centrales la evaluación de amenazas y la evaluación de afrontamiento, donde la evaluación de amenazas se relaciona con la percepción del usuario respecto al nivel de riesgo asociado a comportamientos negligentes en SI y la evaluación de afrontamiento se vincula con la capacidad percibida para enfrentar dichas amenazas. En este proceso, la autoeficacia adquiere especial relevancia, al reflejar las habilidades y competencias del usuario para ejecutar el comportamiento en SI recomendado.

Figura 16

Modelo que integra la Teoría de la Conducta Planificada y la Teoría de la Motivación de Protección.

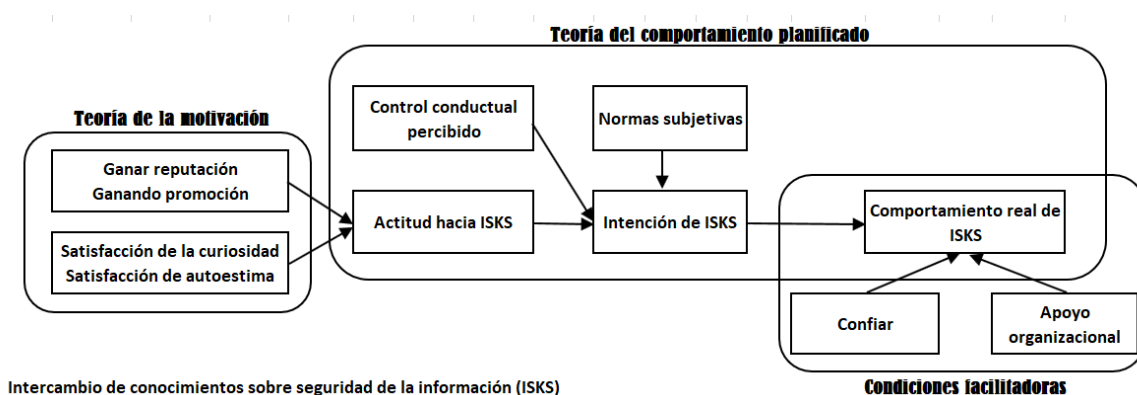


Según Sohrabi Safa y Von Solms (2016), el intercambio de conocimientos en SI constituye un enfoque eficaz no solo para elevar el nivel de conciencia en las organizaciones, sino también para reducir los costos asociados a la gestión de la SI, sustentado en la integración de las siguientes: Teoría de la Motivación, la Teoría del Comportamiento Planificado (TPB) y el modelo conductual de Triandis, con el propósito de explicar los factores que influyen en la disposición de los empleados a compartir conocimientos relacionados con la SI. La TPB se emplea para describir cómo los empleados participan en el intercambio de conocimientos de SI como un mecanismo para mitigar el riesgo de violaciones de SI. Analizando tanto las motivaciones intrínsecas, tales como la satisfacción de la curiosidad y el fortalecimiento de la autoestima, como las motivaciones extrínsecas, entre ellas la obtención de reconocimiento, reputación o promoción laboral, las cuales influyen significativamente en la actitud de los empleados hacia el intercambio de conocimientos en SI.

Desde esta perspectiva, la motivación se concibe como el conjunto de razones, necesidades y deseos que orientan la conducta humana, determinando la dirección y la intensidad de determinados patrones de comportamiento. En consecuencia, un motivo específico puede impulsar a un individuo a actuar de una manera determinada en contextos organizacionales relacionados con la SI, considerando que aun cuando existan fuertes intenciones conductuales, el comportamiento deseado puede no materializarse si se presentan obstáculos que lo inhiban. En este sentido, las condiciones facilitadoras desempeñan un papel crucial, al representar aquellos factores que permiten o favorecen la ejecución efectiva de una conducta. Para el intercambio de conocimientos en SI, incluyen principalmente el apoyo organizacional y la confianza entre los empleados, elementos que resultan fundamentales para promover un entorno propicio para la compartición del conocimiento en SI (ver figura 17).

Figura 17

Modelo que integra la Teoría de la Motivación de protección y la Teoría del Comportamiento Planificado y el modelo de Triandis



Vance et al. (2012) proponen un modelo conductual que amplía la Teoría de la Motivación de Protección (PMT) mediante la incorporación del hábito, entendido

como un patrón de comportamiento pasado, rutinario y automático, explicando cómo las prácticas previas de cumplimiento en SI influyen en la evaluación de amenazas y en los mecanismos de afrontamiento que sustentan la conducta de SI (ver figura 18). Los autores han considerado 2 etapas:

En la primera etapa, los factores de evaluación de amenazas, que incluyen:

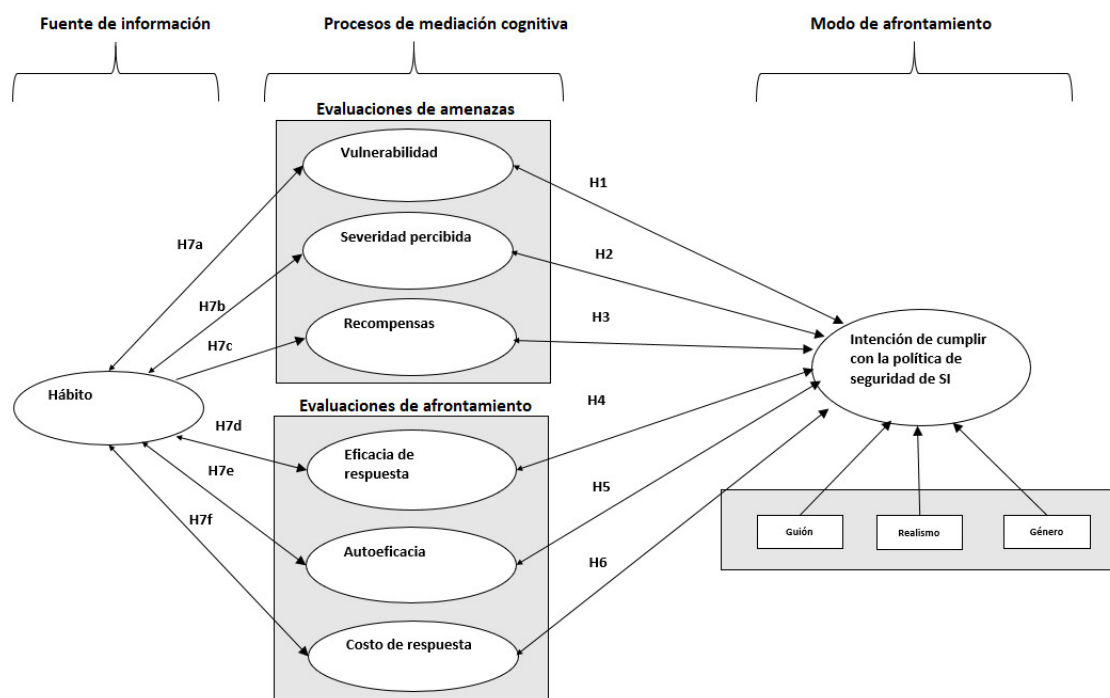
- (i) las recompensas asociadas a conductas inseguras, como beneficios psicológicos o aprobación social, que incrementan la probabilidad de respuestas desadaptativas.
- (ii) la vulnerabilidad percibida, entendida como la probabilidad de que ocurra un incidente de SI en ausencia de medidas preventivas.
- (iii) la severidad percibida, referida al nivel de impacto y gravedad de las consecuencias derivadas de una brecha de SI en la organización.

En la segunda etapa, la PMT incorpora los factores de evaluación de afrontamiento, entre los que destacan la eficacia de la respuesta, vinculada a la creencia de que el cumplimiento de las PSI constituye una protección efectiva; la autoeficacia, asociada a la confianza del empleado en su capacidad para cumplir adecuadamente con dichas políticas; y los costos de respuesta, que comprenden los esfuerzos, inconvenientes o cargas percibidas derivados del cumplimiento de los controles de SI.

El modelo propuesto por los investigadores permite comprender cómo la interacción entre hábitos, percepciones de amenaza y evaluaciones de afrontamiento configura la intención y el comportamiento real de cumplimiento de las PSI.

Figura 18

Modelo que integra Teoría del Comportamiento Planificado se integró con el hábito.



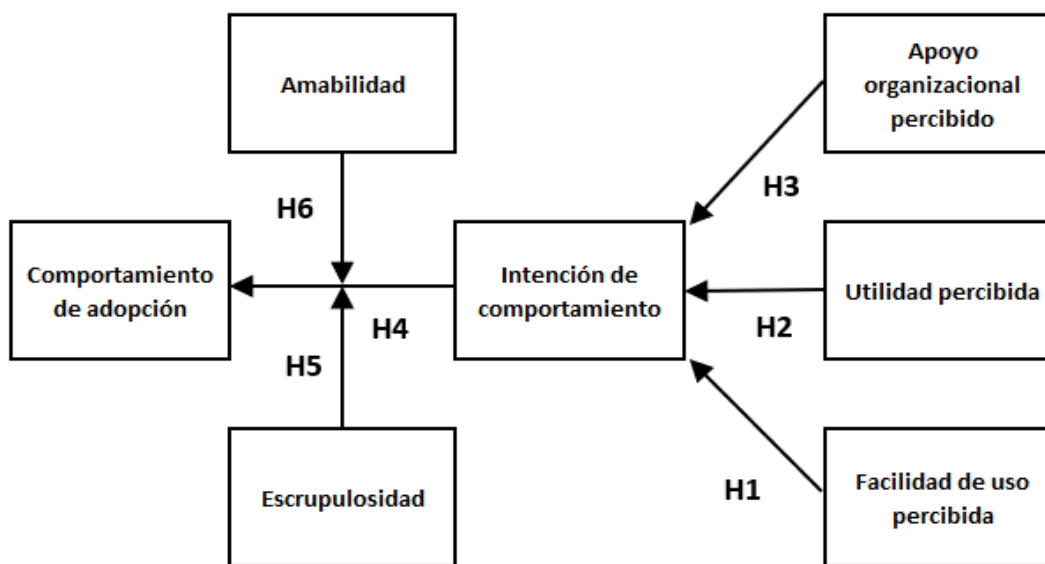
Shropshire et al. (2015) señalan que los estudios sobre adopción de tecnologías suelen explicar el comportamiento a partir de la relación entre actitudes e intenciones; no obstante, advierten que la intención no siempre constituye el mejor predictor de la conducta real. Incorporan los cinco grandes rasgos de personalidad apertura, escrupulosidad, extraversión, amabilidad y neuroticismo como variables explicativas adicionales del comportamiento, aportando una comprensión más profunda del comportamiento del usuario en el ámbito de la SI, un campo aún poco explorado desde esta perspectiva. Evidencian que la escrupulosidad y la amabilidad son rasgos particularmente relevantes, determinando que la escrupulosidad, asociada al autocontrol, la planificación y el cumplimiento de normas, se relaciona positivamente con conductas de SI y con el seguimiento de reglas organizacionales incluso en ausencia de supervisión. Por su parte, la amabilidad, vinculada a orientaciones prosociales como la

cooperación, la confianza y el altruismo, influye significativamente en la preocupación por la SI y la privacidad de la información, así como en la disposición a adoptar recomendaciones de SI (ver figura 19).

Asimismo, el estudio integra constructos del Modelo de Aceptación de la Tecnología (TAM), identificando la utilidad percibida, la facilidad de uso percibida y el apoyo organizacional percibido como factores que influyen en la intención conductual de adoptar prácticas de SI. En conjunto, los hallazgos sugieren que el comportamiento de SI no solo responde a evaluaciones racionales de utilidad o facilidad, sino que también está condicionado por características estables de la personalidad y por el contexto organizacional, reforzando la necesidad de enfoques integrales en la gestión de la SI.

Figura 19

Modelo en base a la amabilidad y la escrupulosidad

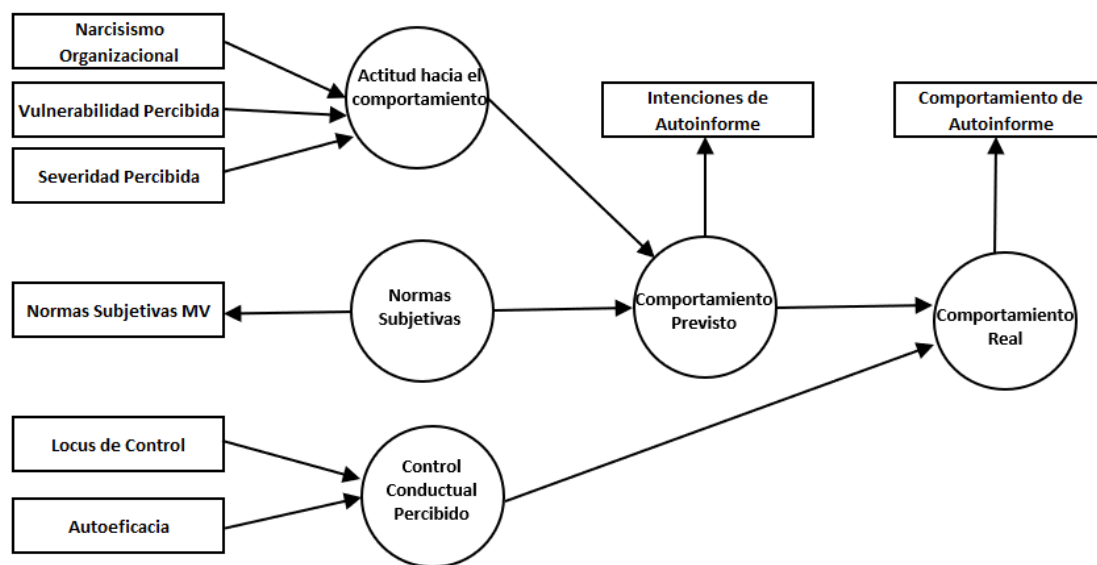


Cox (2012) desarrolla un modelo estructurado para explicar la brecha entre el conocimiento y la acción del usuario (*knowing–doing gap*) en el cumplimiento de

las PSI, sustentado principalmente en la Teoría del Comportamiento Planificado (TPB) tal como se observa en la figura 20. Su investigación se centra en el incumplimiento no malicioso de las PSI, atribuido a factores como la conveniencia, la negligencia o la falta de comprensión de las normas, más que a intenciones deliberadamente dañinas. Incorporando variables psicológicas y perceptuales que influyen en la actitud hacia el cumplimiento, las normas subjetivas y el control conductual percibido. Entre ellas destaca el narcisismo organizacional, entendido como la tendencia del individuo a sobrestimar sus capacidades y minimizar los riesgos, lo que lo lleva a percibir que los beneficios del incumplimiento superan sus posibles consecuencias. Asimismo, se considera la amenaza percibida, descompuesta en vulnerabilidad y gravedad percibidas, como un elemento central del proceso de evaluación del riesgo, en línea con la Teoría de la Motivación de Protección y los modelos de creencias en salud aplicados al contexto de la SI.

El autor resalta que las creencias normativas influyen en las normas subjetivas y, en consecuencia, en la intención de cumplimiento, al reflejar la presión social percibida y la motivación del individuo para ajustarse a las expectativas de su entorno organizacional. Concluyendo que el control conductual percibido, integrado por el locus de control y la autoeficacia, determina la percepción de capacidad del usuario para ejecutar la conducta esperada, influyendo de manera directa en la decisión de iniciar o no comportamientos alineados con las PSI.

Figura 20

Modelo elaborado en base a la Teoría del Comportamiento Planificado

Liu et al. (2020) definen al compromiso organizacional como el grado de identificación e involucramiento del empleado con la organización, separando en tres dimensiones: afectiva, de permanencia y normativa. El compromiso afectivo se manifiesta cuando el empleado permanece en la organización por afinidad con sus valores y objetivos; el compromiso de permanencia responde a los costos percibidos de abandonar la organización y el compromiso normativo se fundamenta en un sentido de obligación moral para continuar en ella. El compromiso afectivo se identifica como el determinante más sólido de los comportamientos favorables del empleado y como un factor clave frecuentemente subestimado en la investigación sobre SI. Recomendamos que la dimensión resulta especialmente relevante para explicar el cumplimiento de las PSI, al fortalecer la motivación interna del empleado para actuar en consonancia con los intereses organizacionales.

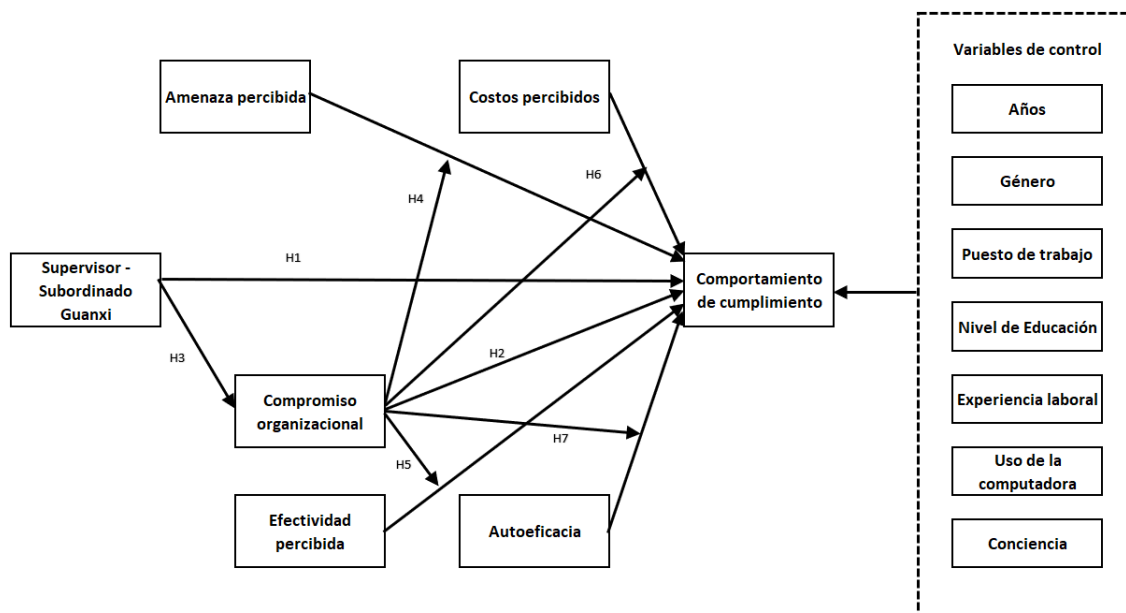
Desde la perspectiva del intercambio social, el comportamiento organizacional se ve influido por el principio de reciprocidad, según el cual las relaciones sostenidas en el tiempo generan obligaciones mutuas. El compromiso organizacional puede

entenderse como una actitud derivada de intercambios sociales positivos entre el empleado y la organización, lo que favorece relaciones de alta calidad entre supervisores y subordinados y refuerza conductas de cumplimiento normativo, incluidas las vinculadas a la SI (ver figura 21).

Asimismo, conceptos como el apego afectivo y la inclusión de la vida personal, asociados al *guanxi*, reflejan la existencia de vínculos emocionales y de confianza que fortalecen estas relaciones. El apego afectivo constituye el núcleo de dichos intercambios, mientras que la inclusión de la vida personal actúa como una manifestación de esa conexión emocional, contribuyendo indirectamente a la disposición del empleado para cumplir con las expectativas y normas organizacionales.

Figura 21

Modelo que integra la Teoría de la disuasión general, Teoría de la elección y la Teoría de la motivación de protección



2.3. BASES TEÓRICAS

2.3.1. MARCO TEÓRICO

2.3.1.1. TEORÍA DE VÍNCULO SOCIAL

Travis Hirschi (1969 - 1995) propuso La Teoría de Vínculo social o Teoría de Control Social argumentando que los hombres son intrínsecamente propensos a la desviación, describe cómo los individuos que tienen lazos sociales más fuertes se involucran menos en la conducta desviada. Esta teoría predice que una persona con mayor vínculo con la sociedad convencional tendrá menor probabilidad de incumplir con las normas y participar en un comportamiento criminal. Esta teoría adquirió mayor importancia durante la década de 1960 cuando los sociólogos buscaron diversas concepciones de la delincuencia, donde afirma que los vínculos con la familia, la escuela, la organización y otros aspectos de la sociedad sirven para minimizar la propia propensión a la conducta desviada. También propone una distinción entre el control ejercido desde fuentes externas al individuo y el control ejercido por el propio individuo. Sohrabi Safa et al. (2016) consideran este punto sobresaliente en esta teoría que nos anima a utilizarlo, con el fin de aumentar el nivel de cumplimiento de las PSI en un SGSI en las organizaciones, el apego, la participación, el compromiso y las normas personales son los cuatro elementos principales de esta teoría, las cuales están separados (Ver figura 22), pero relacionados entre sí. Su apego a otros significantes convencionales, su compromiso con las acciones de los objetivos convencionales, su participación en actividades convencionales y las normas personales en la validez de los sistemas de valores comunes afectan su comportamiento delictivo. Demostrando que el apego, el compromiso, la participación y las normas personales disminuyen significativamente el abuso informático del personal interno. Además, Sohrabi Safa et al. (2018) han llamado la atención de expertos de diferentes dominios, explica cómo se genera la delincuencia de los adolescentes, particularmente el apego de los adolescentes a los demás, el compromiso con el cumplimiento de sus metas, la participación

en sus actividades y las normas personales en la validez moral de los valores comunes. Todo esto afecta en el comportamiento delictivo de los adolescentes y el comportamiento indebido, conducir en estado de ebriedad, fumar cigarrillos y el abuso de drogas que la sociedad considera incorrectos o criminales.

La teoría de vínculos sociales o teoría de control social se ha ampliado para incluir el comportamiento inadecuado de los empleados en las organizaciones indicando que los que tienen un vínculo más fuerte con sus gerentes, compañeros de trabajo y organizaciones tienen menos probabilidades de participar en delitos contra las normas y políticas de la organización, en caso contrario aumentaría cuando el vínculo entre los empleados y la organización es débil. Esto implica que en ausencia de estos cuatro elementos una persona es propensa a participar en algún tipo de desviación.

Apego: (Adjunto) Se refiere al vínculo de carácter afectivo que se desarrolla mediante la interacción entre los padres y los hijos, los maestros, instituciones, áreas, etc.

Para Sohrabi Safa et al. (2016), es una relación de afecto y respeto que un individuo mantiene con una persona, una organización, un trabajo, un supervisor e incluso un compañero de trabajo. El factor humano con un fuerte apego tiene menos probabilidades de incurrir en comportamientos desviados.

Compromiso: Se refiere como un vínculo utilitario que podría ser definido como el grado según el cual, los propios intereses individuales han sido invertidos en un conjunto de actividades fijas o establecidas.

Implica esforzarse, prometer y manifestar apoyo para salvaguardar los activos de información de la organización. Considerando que los logros personales y la reputación son importantes para las personas comprometidas. Dedicar más tiempo y energía a lograr el éxito en su carrera que las personas no comprometidas. Es poco probable que las personas comprometidas se arriesguen a infringir normas que, por lo tanto, podrían poner en peligro o destruir sus aspiraciones profesionales. (Sohrabi Safa et al. 2016)

Participación: Es la inversión que el factor humano aplica a realizar actividades y evitar que los sujetos cometan delitos. Se considera que el hecho de poder participar en actividades comunitarias y obligar a los jóvenes a estar fuera de las calles es una buena forma de prevenir la delincuencia.

Consiste en la energía, el esfuerzo y el tiempo que alguien está dispuesto a dedicar a realizar una actividad o un tema en particular. La participación manifiesta la profundidad de la relación entre el individuo y el objeto de intervenir. Un alto nivel de participación tiene un mayor efecto sobre el comportamiento humano, como lo demuestra el modelo cognitivo, afectivo y conductual. (Sohrabi Safa et al. 2016).

Para el contexto de un sistema de SI, la participación se refiere a la energía, el tiempo y el esfuerzo que un empleado dedica a proteger la información o mejorar la SI en una organización. por lo que disuade de una mala conducta en el dominio.

Normas Personales: Consideradas también como las creencias desde el punto de vista de valores y normas que reciben una importante aprobación y respaldo social. Es decir, que las creencias están estrictamente sometidas al refuerzo social constante. Por ello implicaría que los entornos relacionados con la delincuencia consideraran los valores y normas relacionadas con la trasgresión de la ley como algo común.

Las normas personales son valores del sentido del deber de un individuo con respecto a un tema, evento o cosa en particular. Las normas personales influyen en la actitud, las intenciones de los individuos y, en consecuencia, en su comportamiento real. (Sohrabi Safa et al. 2016).

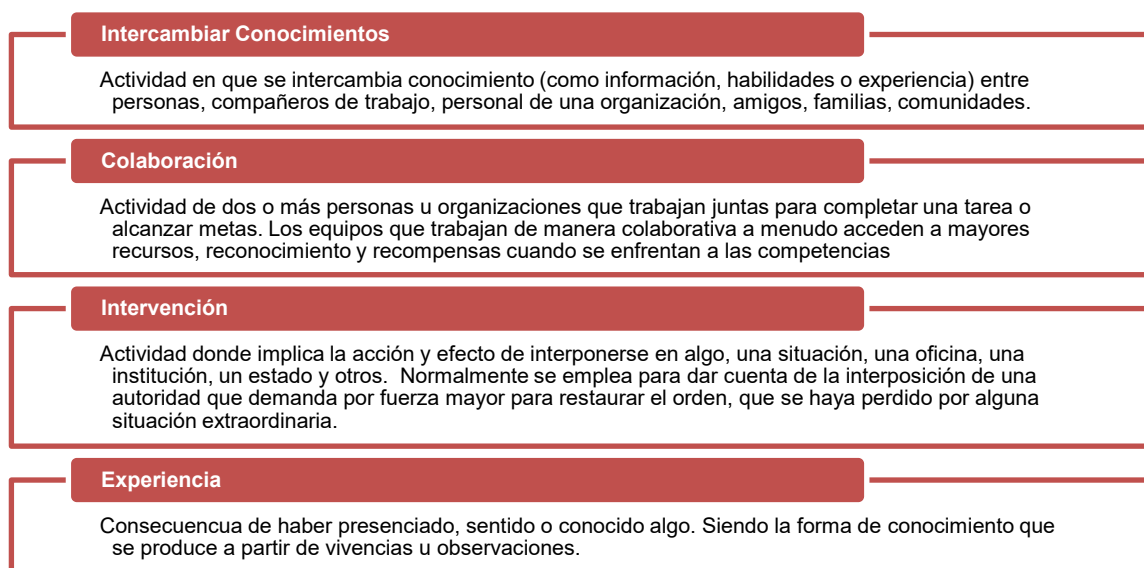
*Figura 22***Elementos de la teoría de control social****2.3.1.2. TEORÍA PARTICIPACIÓN**

Según Sohrabi Safa et al. (2016) La participación se refiere a la inversión que se destina a realizar actividades y evitar así que los sujetos cometan delitos. Considera por lo tanto que el hecho de poder participar en actividades realizadas en la entidad con el fin de mejorar la actitud de los empleados hacia el cumplimiento de las políticas de la organización analiza el nivel de energía y el tiempo en una actividad, la participación se ha aplicado en varios dominios, como la participación del cliente, la participación del producto, la participación del estudiante, etc.

La participación influye en la actitud y se manifiestan en diferentes formas (Ver figura 23) como el intercambio de conocimientos, la colaboración, la intervención y la experiencia.

Figura 23

Formas de participación



2.3.1.3. TEORÍA DEL COMPORTAMIENTO PLANIFICADO (TPB)

La Teoría del comportamiento planificado fue desarrollado por (Icek Ajzen, 1988, 1991) quien explica el entender cómo podemos cambiar el comportamiento del factor humano. Teoría que predice el comportamiento deliberado, porque el comportamiento puede ser planeado, se basa en la Teoría de la Acción Razonada (TCP) Esta teoría se compone por las siguientes variables como la actitud, la norma subjetiva y el control conductual percibido, dichas variables tienen una influencia en la intención de llevar a cabo un comportamiento.

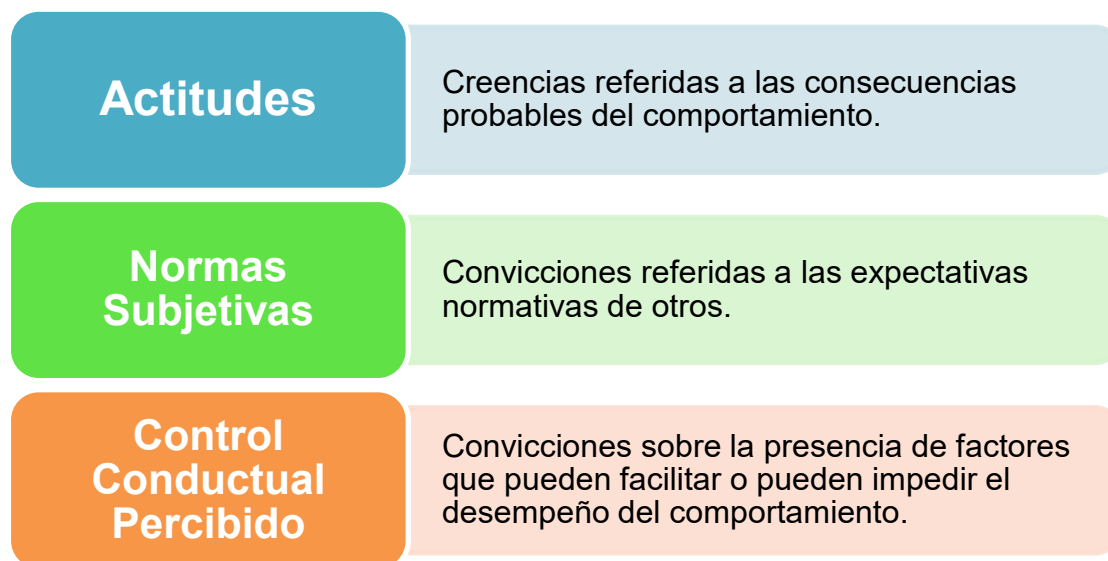
La “Teoría del comportamiento planeado (TPB)” se diferencia de la “Teoría de la acción razonada (TCP)”, por lo que se agrego el control del comportamiento percibido también conocido como locus de control (como un posible equivalente

de la auto-eficacia), el cual se vincula a las percepciones del factor humano sobre la presencia o ausencia de recursos y oportunidades requeridos, lo cual lleva al factor humano evaluar la situación que tan probable es que con sus recursos pueda realizar su conducta, esto además de los factores externos de los cuales se encuentra sometido no tiene el control absoluto. Asimismo, la teoría del comportamiento planeado sobresale en relación con la teoría de la acción razonada para la predicción del comportamiento, por lo que ha sido ampliamente utilizado en diferentes investigaciones, así también se ha tomado en investigación de sistema de gestión de información, en la decisión del individuo para cumplir con las PSI.

Mediante la revisión de las investigaciones que se ocupan de varios aspectos de la teoría del comportamiento planificado y se discuten algunos problemas no resueltos. En términos generales se encontró que la teoría está bien respaldada por evidencia empírica, además las intenciones de realizar comportamientos de diferentes tipos pueden predecirse con gran precisión a partir de 3 aspectos importantes como las actitudes hacia el comportamiento, las normas subjetivas y el control conductual percibido (ver figura 24).

Figura 24

Predictores de intención de comportamiento



Estos 3 aspectos importantes son cruciales en diferentes casos como circunstancias, proyectos y programas cuando se necesita cambiar el comportamiento de la gente a nivel individual, social y Información, tal como se observa en la figura 25.

Figura 25

Comportamiento del factor humano por niveles

Nivel Individual	Social	Información
• Personalidad • Estado • Anímico • Emoción • Inteligencia • Valores • Estereotipos • Experiencia	• Educación • Años • Género • Ingresos • Religión • Carrera • Etnía • Cultura • Leyes	• Conocimiento • Medios de comunicación • Intervención

Además, explica por qué las organizaciones de publicidad que brindan simplemente información no trabajan para aumentar solamente el conocimiento no ayuda mucho a cambiar el comportamiento. las campañas que están orientadas a actitudes, normas percibidas y el control conductual para realizar el cambio o comprar ciertos productos, tiene mejores resultados.

2.3.1.4. TEORÍA DE LA MOTIVACIÓN DE PROTECCIÓN (PMT)

La Teoría de la Motivación de Protección PMT fue desarrollado por Rogers (1975, 1983) para comprender cómo el factor humano decide adoptar comportamientos protectores, compuesta por dos conceptos claves evaluación de amenazas y evaluación de afrontamiento. Lo cual significa que cuando el factor humano se

encuentra frente a un riesgo, el comportamiento del factor humano en respuesta al riesgo está motivado por evaluaciones de amenaza y afrontamiento. Teniendo como efecto en la evaluación de la amenaza la gravedad percibida del impacto del riesgo, así como a la probabilidad de que ocurra. Mientras en la evaluación de afrontamiento se refiere a la eficacia percibida con la que el factor humano puede participar en el comportamiento protector de una manera rentable.

Al respecto conviene decir los principios de la evaluación de amenazas incluyen aspectos percibidos de la vulnerabilidad, la gravedad y las recompensas asociadas con los riesgos y los principios de la evaluación del afrontamiento incluyen la autoeficacia del afrontamiento, la eficacia de la respuesta y el costo percibido asociado con el comportamiento protector. En particular la teoría PMT se elaboró estudios en el dominio de la salud, su aplicabilidad ha abarcado en otros dominios como la SI.

Cabe destacar al investigador Verkijika (2019), quien es uno de los investigadores que ha utilizado la PMT para estudiar y comprender la motivación detrás de diferentes tipos de comportamientos de SI tanto en un contexto organizacional como a nivel personal, las organizaciones están expuestas a amenazas de SI, si no se toman medidas para prevenirlas, de acuerdo con el nivel del impacto potencial de la amenaza se verifica su severidad y la gravedad del daño que puede causar.

Evaluación de amenazas: Se define como el proceso cognitivo mediante el cual los individuos perciben, interpretan y valoran la existencia, probabilidad y severidad de una amenaza, así como su vulnerabilidad personal frente a ella. Para Sohrabi Safa et al. (2016), la evaluación de amenazas desempeña un rol clave en la explicación del comportamiento de cumplimiento de las PSI, al determinar el nivel de preocupación y alerta que experimentan los empleados frente a los riesgos de seguridad. Los autores sostienen que cuando los individuos perciben una amenaza como grave y consideran que son vulnerables a sus consecuencias, se incrementa su motivación para actuar de manera preventiva y cumplir con las PSI. Consta de factores de evaluación de amenazas,

que consta de factores como la vulnerabilidad, la gravedad percibida y las recompensas

Evaluación de afrontamiento: Define como el proceso cognitivo mediante el cual los individuos valoran su capacidad para enfrentar eficazmente una amenaza, considerando la efectividad de las respuestas disponibles, su propia competencia para ejecutarlas y los costos asociados a dichas acciones. Según Sohrabi Safa et al. (2016), la evaluación de afrontamiento desempeña un rol determinante en el comportamiento de cumplimiento de las PSI, al reflejar el grado en que los empleados perciben que las medidas de seguridad son efectivas, viables y aplicables en su entorno laboral. Los autores sostienen que incluso cuando los individuos perciben una amenaza como grave, el cumplimiento solo se materializa si consideran que cuentan con los recursos, conocimientos y capacidades necesarias para responder adecuadamente a dicha amenaza. La evaluación de afrontamiento, que dependen del aumento de la respuesta adaptativa como la eficacia, la autoeficacia y el costo de respuesta.

2.3.2. MARCO TECNOLÓGICO

A continuación, se define algunos conceptos claves en un Sistema de Gestión de Seguridad de Información:

2.3.2.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

Sistema de Gestión de Seguridad de Información (SGSI) o Information System Management System (ISMS) es un sistema de gestión para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la SI, de esta manera un SGSI busca poder mantener los principios fundamentales de la SI como la confidencialidad, integridad y disponibilidad mientras minimiza los riesgos de SI.

2.3.2.2. FUNDAMENTO NORMATIVO

El SGSI se rige principalmente por la norma internacional ISO/IEC 27001-2022, que proporciona un marco de referencia para establecer, implementar, mantener

y la aplicación de la mejora continua un sistema de gestión enfocado en la SI. Esta norma enfatiza la gestión del riesgo y el ciclo de Deming ciclo de mejora continua PDCA (Plan-Do-Check-Act).

2.3.2.3. POLÍTICA DE SEGURIDAD DE INFORMACIÓN

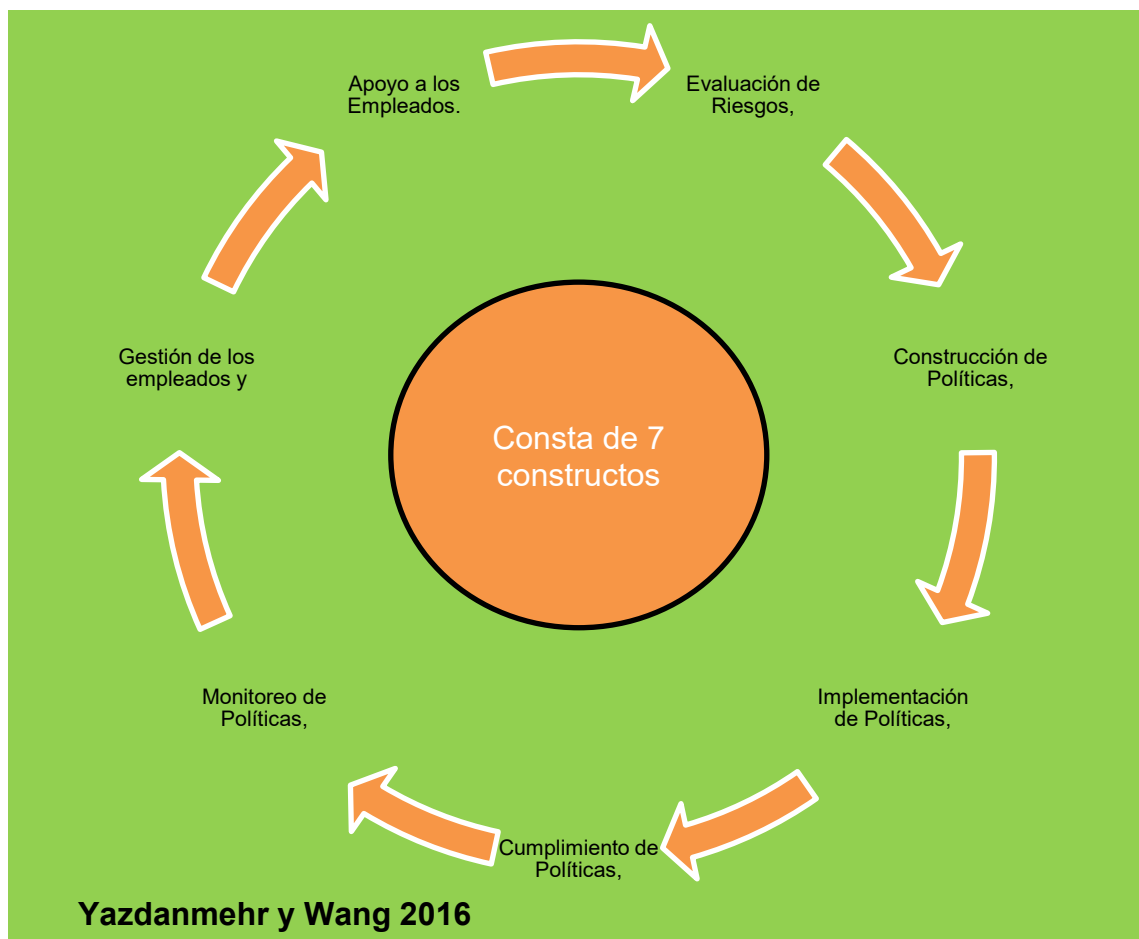
Las PSI son aquellas normas que se establecen para guiar a los miembros de la organización a resguardar correctamente la SI, siendo la base de una efectiva arquitectura de un SGSI, ya que de ella nacen otros documentos importantes tales como lineamientos, directivas, estándares, procedimientos y guías.

Según Liu et al. (2020) las PSI son conjuntos de regulaciones, normativas, lineamientos, directivas y procedimientos que restringen el acceso de los empleados y el uso adecuado de los recursos tecnológicos con responsabilidades de protección y sus consecuencias de las infracciones. Incluyen regulaciones formales que tienen como objetivo orientar los comportamientos de seguridad del factor humano y proporcionarles instrucciones para el uso adecuado de los recursos tecnológicos de la organización.

Asimismo, Yazdanmehr y Wang (2016), define a la PSI como un conjunto de reglas y lineamientos relacionadas con el acceso a la información y el uso adecuado de los activos de información en las organizaciones. Además de describir las responsabilidades del factor humano y las consecuencias de las violaciones de los lineamientos. Por otro lado, Flowerday y Tuyikeze (2016) proponen 4 componentes claves en el Ciclo de vida del desarrollo de la PSI, que se detallan a continuación:

Primer componente relacionado a las etapas de desarrollo, aplicación y gestión de las PSI. (ver figura 26)

Figura 26

Primer componente clave del ciclo de vida de la PSI

Segundo componente relacionado a la implementación de controles y mecanismos de SI en base a las amenazas identificadas. (ver figura 27)

Figura 27

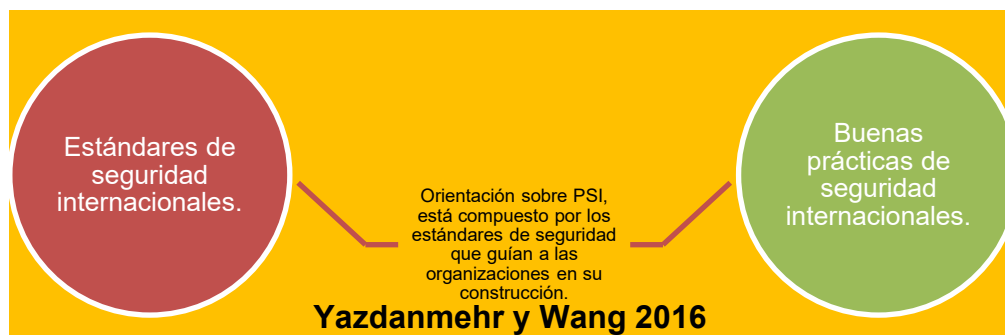
Segundo componente clave del ciclo de vida de la PSI



Tercer componente relacionado al uso de estándares y buenas prácticas para el desarrollo de la implementación de PSI. (ver figura 28)

Figura 28

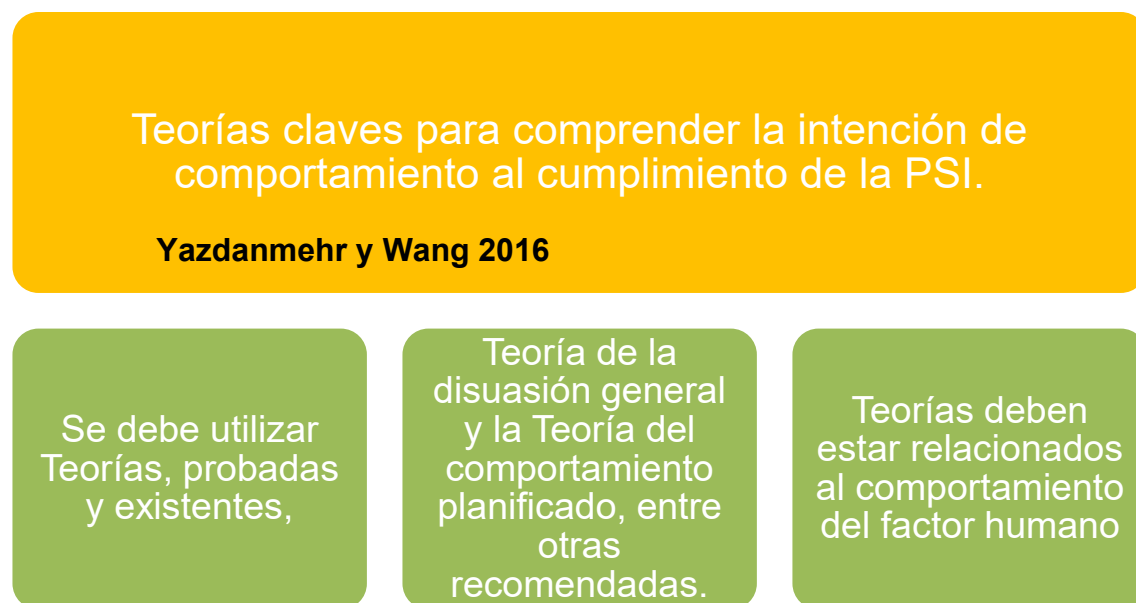
Tercer componente clave del ciclo de vida de la PSI



Cuarto componente relacionado al estudio del comportamiento del factor humano relacionado a la intención de cumplimiento de las PSI.

Figura 29

Cuarto componente clave del ciclo de vida de la PSI



2.3.2.4. OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL

El oficial de seguridad y confianza digital, también conocido por las siguientes siglas CISO (Chief Information Security Officer), es la persona encargada del SGSI quien planifica, presupuesta y verifica la implementación. Así como de realizar una correcta gestión de riesgo para la toma de decisiones.

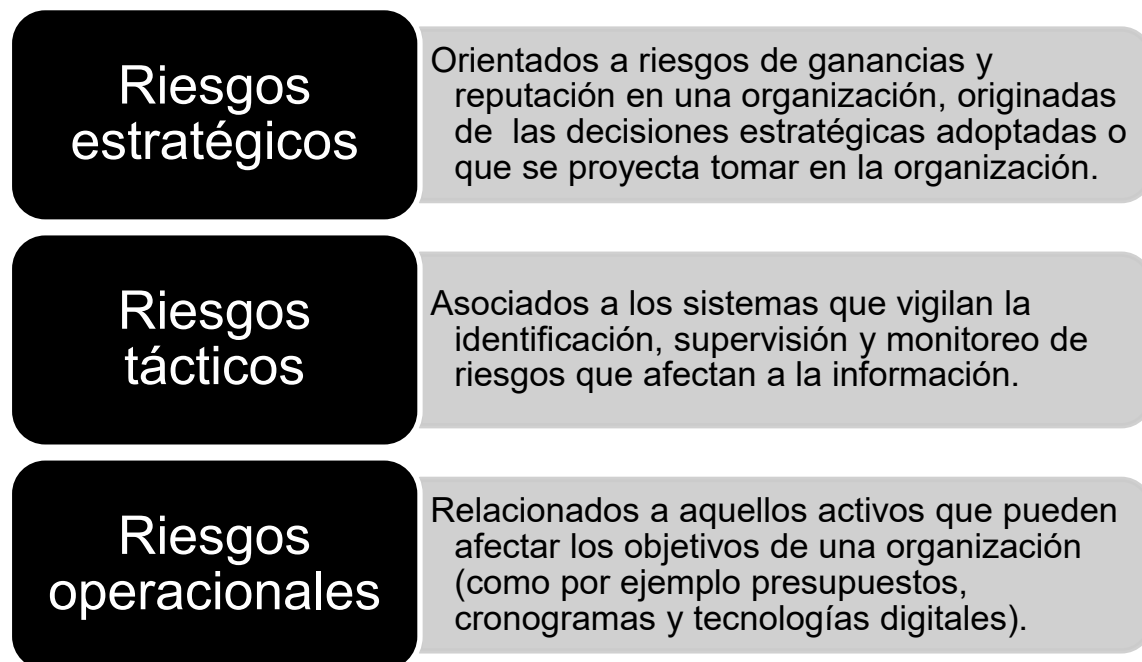
2.3.2.5. RIESGO

Riesgo es un evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia de la combinación del impacto negativo sobre los activos de información por la

probabilidad de que ocurra un evento. Se encuentra dividido en tres naturalezas (ver figura 30)

Figura 30

Tipos de riesgos



2.3.2.6. NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001-2022

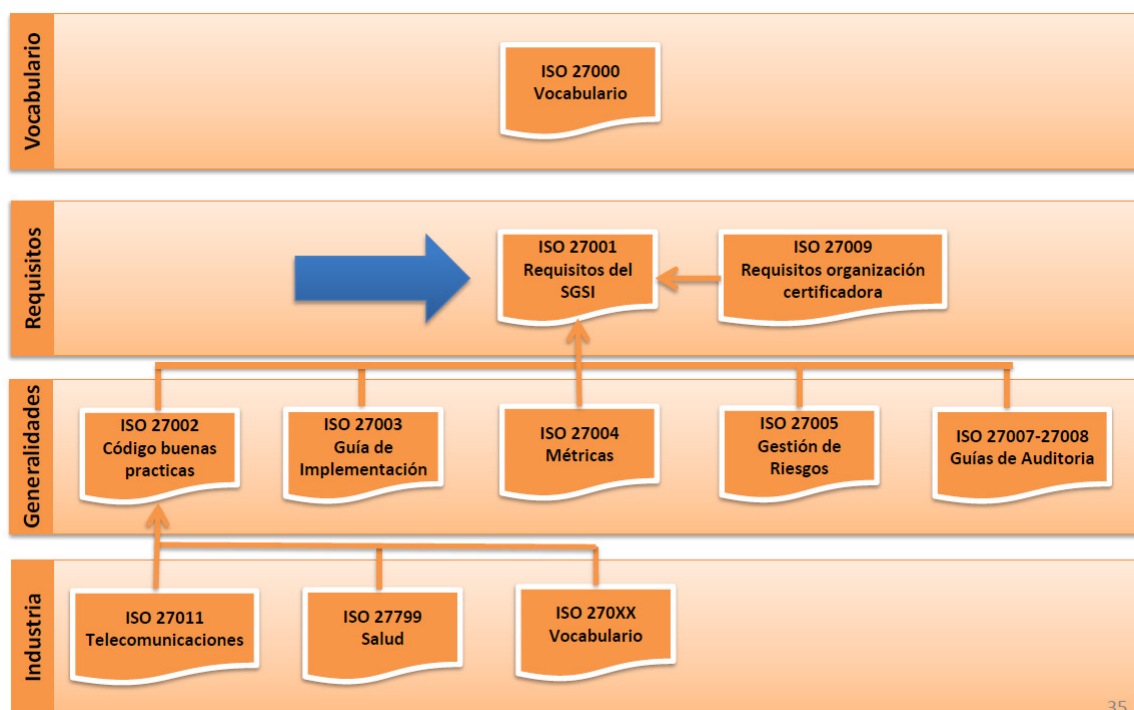
La Norma técnica Peruana NTP-ISO/IEC 27001-2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos, es una norma técnica peruana que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de Información, que reemplaza a la NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.

2.3.2.7. ISO/IEC 27000

La ISO/IEC² 27000 es una norma internacional que busca dar información general sobre los Sistemas de gestión de seguridad de la información (SGSI), que define términos relevantes que son usados por los diferentes estándares de la familia 27000. A diferencia de otras normas de esta familia, es de libre distribución y se caracteriza por brindar un listado de varias normas que serán mencionadas (ver figura 31) junto con una pequeña descripción [ISO/IEC 27000, 2012]:

Figura 31

Relación de estándares de la familia SGSI



Fuente: ISO/IEC 27000 – Tecnologías de información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Información general y vocabulario

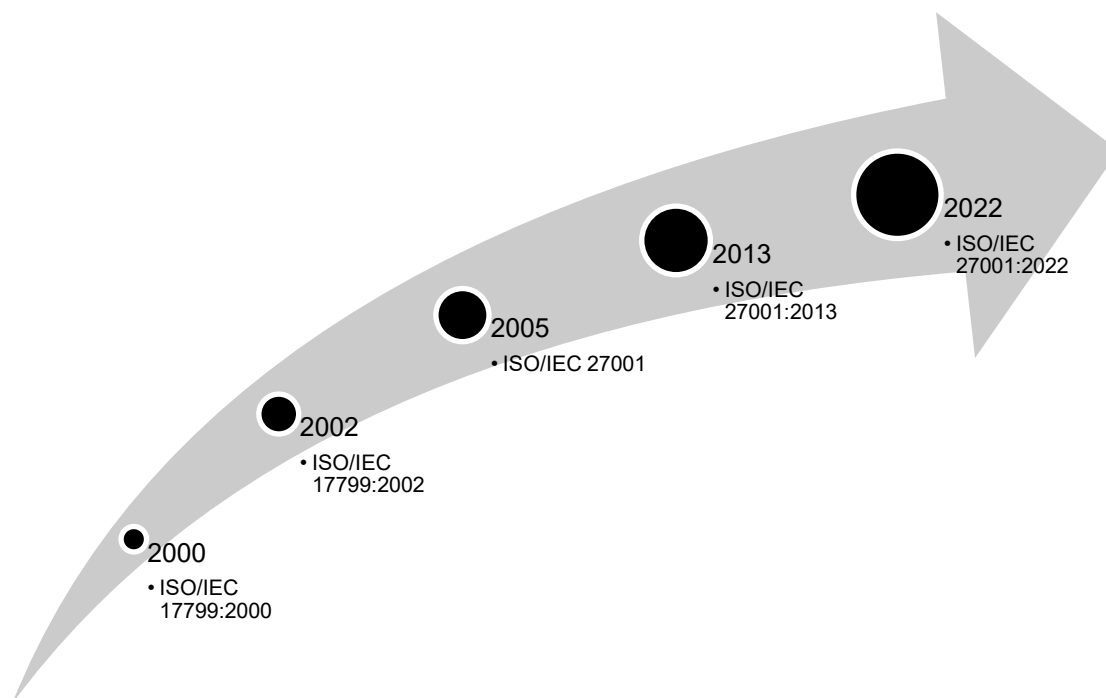
² ISO (International Organization for Standardization / Organización internacional de Normalización) IEC (International Electrotechnical Commission / Comisión Electrotécnica Internacional)

2.3.2.8. Evolución de la ISO/IEC 27001

La evolución de la ISO/IEC 27001:2022 se centra en la adaptación a la Estructura Armonizada y la mejora continua de los controles de SI (ver figura 32). La norma ha sido actualizada para reflejar las mejores prácticas actuales y para abordar los nuevos desafíos de SI. Los cambios incluyen la eliminación de controles duplicados y la adición de nuevos controles, así como la simplificación de la estructura de clasificación de los controles de SI. Estos cambios están diseñados para ayudar a las organizaciones a mantener su resiliencia y a mitigar riesgos de manera efectiva.

Figura 32

Evolución ISO/IEC 27001



2.3.2.9. NTP ISO 31000:2011

Norma técnica peruana basada en la ISO 31000:2009, la cual forma parte de la familia de estándares para gestionar riesgos. Esto debido a la existencia de factores internos o factores externos, que incrementan dudas en el logro de los objetivos en las organizaciones.

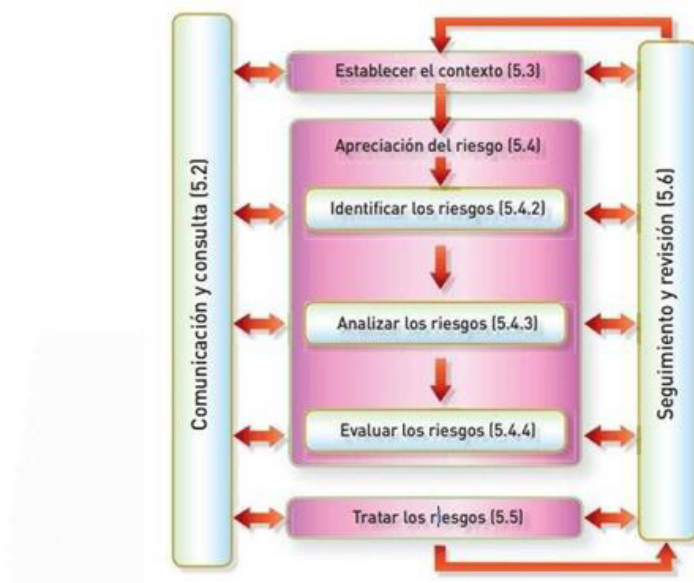
Norma que busca establecer principios para tener una gestión eficaz del riesgo mediante la implementación y la mejora continua de un marco de trabajo para la combinación del proceso de gestión de riesgos en la planificación, estrategia, gestión, procesos de información, políticas, valores y cultura de la organización.

La gestión de riesgo se debe basar en:

- Generar valor
- Tratamiento de la incertidumbre o dudas
- Ser parte de las decisiones
- Estar hecha a la medida
- Considerar al factor humano y los factores culturales
- Favorecer la mejora continua en la organización

El proceso de gestión del riesgo lo podemos observar en la figura 33.

Figura 33

Proceso de gestión de riesgos**2.3.3. MARCO REGULATORIO / LEGAL**

Las siguientes resoluciones ministeriales fueron autorizadas por la secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de ministros siendo el ente rector del sistema nacional de transformación digital, las cuales están relacionados a la investigación y la implementación del SGSI en las entidades publicas, estas son:

2.3.3.1. RM-246-2007-PCM

Esta resolución aprueba el uso obligatorio de la “NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información” en todas las organizaciones públicas que pertenecen al Sistema Nacional de Informática. La cual significo el reemplazo de la NTP-ISO/IEC 17799:2004 que en ese tiempo se encontraba de uso obligatorio.

2.3.3.2. RM-197-2011-PCM

Esta resolución establece como fecha límite del día 31 de diciembre del 2012, para la implementación de la “NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información” para todas las organizaciones que pertenecen al Sistema Nacional de Informática.

2.3.3.3. RM-129-2012-PCM

Esta resolución deja sin efecto la RM-197-2011-PCM, debido a que la norma “NTP-ISO/IEC 17799:2007” que debía ser implementada establece recomendaciones y buenas prácticas de seguridad de información, pero no definía una forma exacta de verificar la efectividad y eficiencia de los controles de SI que fueron implementados, por lo que la fecha límite dada por esta resolución quedaba sin efecto.

Asimismo, define que se debe implementar de manera obligatoria la “NTP ISO/IEC 27001:2008” dando nuevas fechas límites para el desarrollo de la implementación para todas las organizaciones públicas. La norma fue emitida el 23 de mayo del 2012, y da 45 días para el inicio de la primera fase por lo que a la primera semana de julio del 2012 debió haberse empezado con las actividades de la implementación.

2.3.3.4. RM-004-2016-PCM

Esta resolución aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de Información. Requisitos 2ª. Edición”, en todas las organizaciones integrantes del sistema nacional de Informática. La cual fue emitida el 8 de enero del 2016.

2.3.3.5. RSGTD-003-2023-PCM

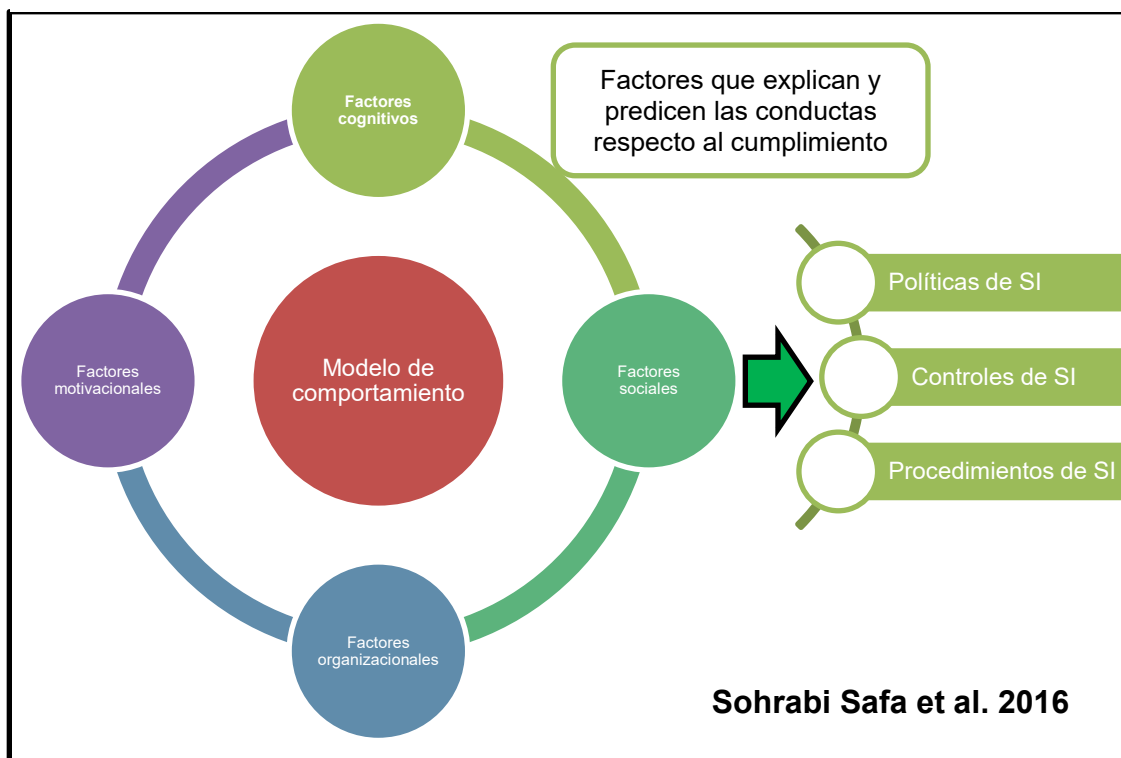
Esta resolución aprueba la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las organizaciones del estado, esta resolución aprueba el plan de implementación del Sistema de Gestión de Seguridad de la Información en las entidades públicas, asignación de un responsable de la implementación y la creación de un equipo técnico multidisciplinario.

2.3.4. MARCO CONCEPTUAL

2.3.4.1. MODELO DE COMPORTAMIENTO EN UN (SGSI)

Para Sohrabi Safa et al. (2016), el modelo de comportamiento en un Sistema de Gestión de Seguridad de la Información (SGSI) se refiere al conjunto de factores que explican y predicen las conductas de los empleados respecto al cumplimiento de la normatividad de SI. Tal como se observa en la figura 34. Además, otros autores definen un marco que explica como actitudes, normas sociales y percepciones de control determinan la ejecución de conductas seguras dentro de un SGSI, integrando factores cognitivos, sociales y motivacionales que predicen el cumplimiento de políticas y prácticas de protección de información (Schyff et al. 2020).

Figura 34

Factores del modelo de comportamiento en un SGSI

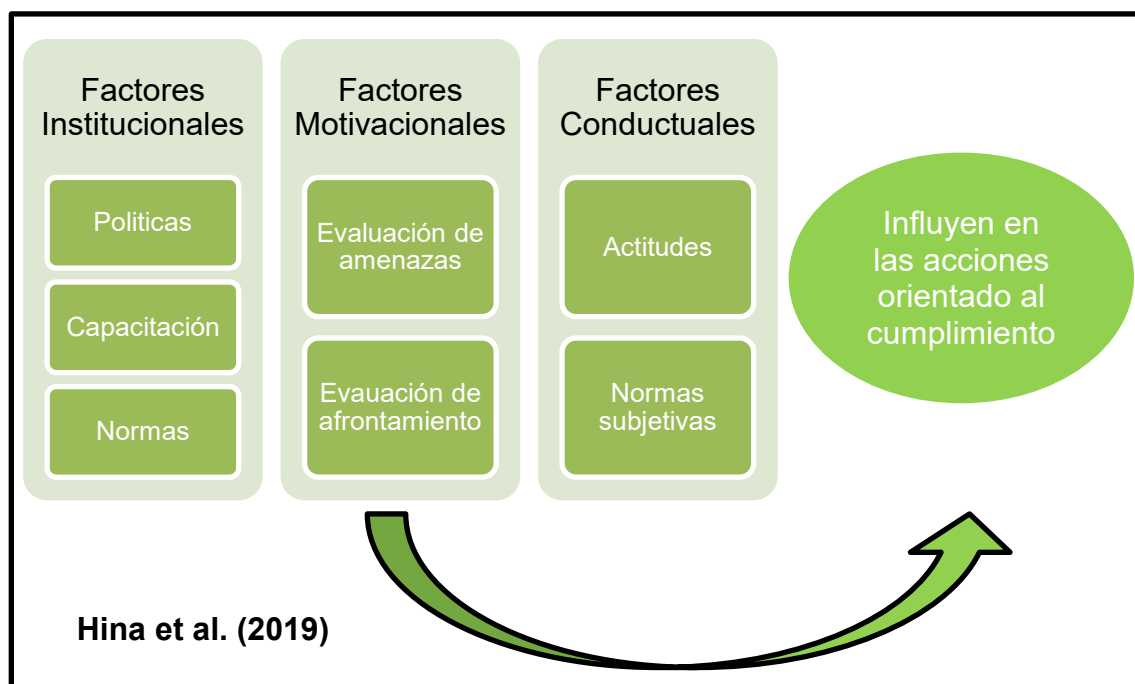
Del mismo modo Cheng et al. (2013), entiende como el conjunto de factores psicológicos, sociales y organizacionales que explican y regulan la conducta de los empleados frente al cumplimiento o violación de las PSI. Desde un enfoque de control social, este modelo articula mecanismos formales como la severidad y certeza de las sanciones; y los informales como el apego organizacional, la creencia en las normas, la presión social y la conducta de los compañeros que influyen en la decisión individual de adherirse o transgredir las PSI. En este sentido, el comportamiento no se explica únicamente por incentivos racionales, sino por la fuerza de los lazos sociales con la organización y por el clima normativo percibido.

Por otro lado, Verkijika (2018) concibe como una estructura teórica orientada a explicar la manera en que diversos factores cognitivos, emocionales y motivacionales influyen en las decisiones y conductas del factor humano frente a los riesgos de SI. En este enfoque, los comportamientos de seguridad no se

entienden como acciones aisladas, sino como el resultado de procesos psicológicos integrados que incluyen la evaluación de amenazas, la valoración de las capacidades de afrontamiento y la formación de intenciones de seguridad. Estos procesos incorporan, además, componentes afectivos relevantes, como el arrepentimiento anticipado, que influyen en la adopción de conductas protectoras. En consecuencia, sostiene que las acciones de seguridad se derivan de la percepción del riesgo expresada en términos de vulnerabilidad y severidad, de la creencia en la eficacia de las medidas de protección, de la autoeficacia del usuario y de mecanismos emocionales que regulan la toma de decisiones ante amenazas digitales. Asimismo, para Hina et al. (2019), se entiende como la estructura que explica cómo los factores configuran las acciones de los empleados orientadas al cumplimiento de la SI dentro de la organización (ver figura 35).

Figura 35

Descripción de factores de un modelo de comportamiento

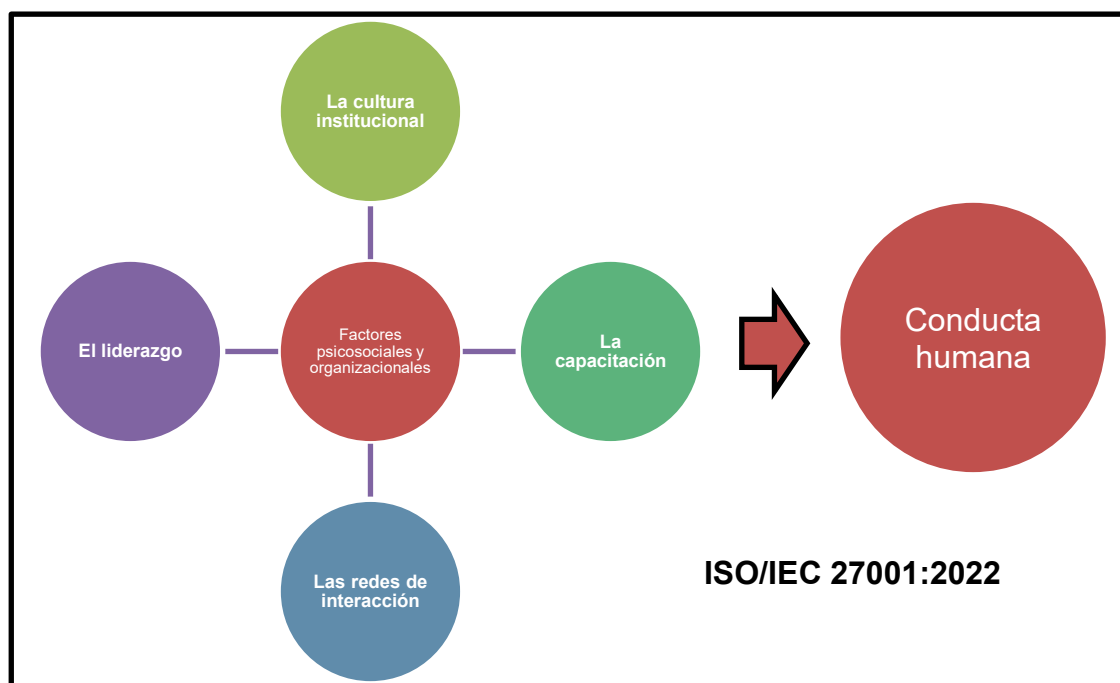


Por su parte Cox (2012) dispone como una estructura conceptual orientada a explicar los procesos mediante los cuales los usuarios adoptan, mantienen o incumplen las PSI. Este enfoque reconoce que la SI no depende exclusivamente

de controles tecnológicos, sino que está profundamente influida por factores humanos, cognitivos y organizacionales. Sosteniendo que el comportamiento de SI del factor humano está determinado por un conjunto de variables interrelacionadas, tales como las actitudes frente a las PSI, las normas subjetivas, el control conductual percibido, la percepción de vulnerabilidad y severidad ante las amenazas, la autoeficacia y las creencias sobre las consecuencias de la conducta individual, lo que explica la persistente brecha entre el conocimiento y la acción (*knowing-doing gap*). También para el contexto de un SGSI alineado a ISO/IEC 27001:2022 (ver figura 36), este modelo se fundamenta en la premisa de que la seguridad no depende únicamente de controles técnicos, sino también de la conducta humana como principal agente de riesgo o de protección.

Figura 36

Factores de modelo de acuerdo con el ISO/IEC 27001:2022



Finalmente, para Vance et al. (2012), concibe como un marco explicativo que integra mecanismos psicológicos, cognitivos y conductuales para comprender por qué y cómo los empleados deciden cumplir o incumplir las políticas y procedimientos de seguridad de la información en el contexto organizacional. Dicho comportamiento no responde exclusivamente a decisiones racionales y deliberadas, sino que también está influido por conductas automatizadas y hábitos adquiridos, los cuales se desarrollan y refuerzan dentro de un entorno organizacional específico. En este sentido, el modelo articula la evaluación de amenazas expresada en la percepción de severidad y vulnerabilidad con la evaluación de afrontamiento relacionada con la autoeficacia, la eficacia de la respuesta y los costos percibidos, así como con las conductas rutinarias de cumplimiento. Esta interacción permite explicar la adopción sostenida de prácticas de SI, destacando que el comportamiento del factor humano es el resultado tanto de procesos cognitivos conscientes como de patrones de acción habituales que influyen directamente en la efectividad del SGSI.

En conjunto, estos enfoques permiten afirmar que el modelo de comportamiento en un SGSI constituye un marco integrador que articula factores cognitivos, emocionales, normativos y organizacionales para explicar el cumplimiento o incumplimiento de las PSI. También, podemos definir como el conjunto de factores psicológicos, organizacionales y cognitivos que explican por qué y cómo los usuarios adoptan conductas seguras dentro de un entorno de SI.

2.3.4.2. INTENCIÓN DE CUMPLIMIENTO DE POLÍTICAS EN UN SGSI

Para Schyff et al. (2020), la intención de cumplimiento de PSI se conceptualiza como la predisposición consciente, voluntaria y deliberada del empleado para adherirse a las normas, procedimientos y controles establecidos por la organización en materia de SI tal como se observa en la figura 37. Además, Vance et al. (2012), demuestran que la intención se ve fortalecida por conductas habituales de cumplimiento y por la forma en que el trabajador procesa cognitivamente las amenazas y su capacidad de afrontamiento. Así, la intención no es solo una predisposición racional, sino un resultado del aprendizaje, la

experiencia previa y los hábitos consolidados. En consecuencia, la intención de cumplimiento de PSI, es la disposición motivacional del empleado para adherirse a las PSI, influida por la evaluación de amenazas, la autoeficacia, la eficacia percibida de las medidas de seguridad, los costos percibidos y los hábitos previos de cumplimiento, constituyendo el principal predictor del comportamiento seguro.

Figura 37

Conceptualización de la intención de cumplimiento de PSI



Según Cheng et al. (2013), la intención constituye un determinante crítico del comportamiento efectivo y se encuentra influida por múltiples variables (ver figura 38). Estos factores evidencian que el cumplimiento de las PSI no responde únicamente a un proceso racional e individual, sino que se configura como un fenómeno social y contextual, moldeado por normas compartidas y vínculos organizacionales. Por ello, la intención de cumplimiento de las PSI puede entenderse como una disposición conductual determinada por las percepciones de sanción, el apego y la identificación con la organización, así como por las presiones normativas del entorno laboral, consolidándose como un predictor clave del comportamiento real de SI dentro de las organizaciones. Asimismo, Cox

(2012) constituye el predictor inmediato del comportamiento efectivo y se configura a partir de la interacción entre la actitud hacia la conducta, las normas subjetivas y el control conductual percibido, en coherencia con los postulados de la TPB. En este marco, la intención de cumplimiento se fortalece cuando el usuario percibe que la amenaza es relevante y aplicable a su contexto, que sus acciones pueden mitigar eficazmente dichos riesgos (autoeficacia y eficacia de la respuesta), que existe una presión social favorable al cumplimiento (normas subjetivas) y que dispone del control necesario para ejecutar la conducta esperada. En este sentido, la intención de cumplimiento de las PSI puede entenderse como la motivación consciente y deliberada del usuario para seguir las prácticas establecidas, determinada por sus actitudes, las normas subjetivas percibidas y el control conductual percibido, y reconocida como el predictor más relevante del comportamiento real en SI.

Figura 38

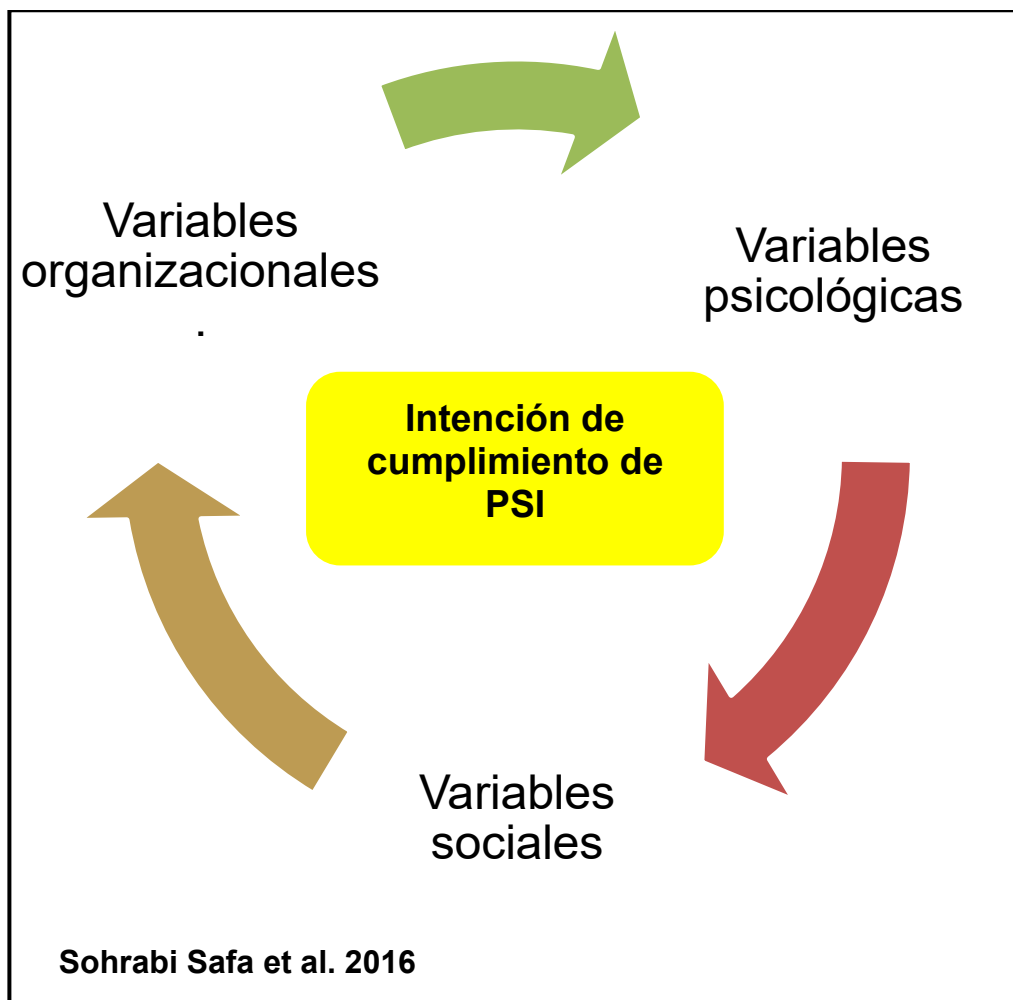
Variables que influyen en la intención de comportamiento efectivo



Desde la perspectiva de Verkijika (2018), la intención de cumplimiento de las PSI puede entenderse como la motivación deliberada de los usuarios para ejecutar comportamientos protectores, la cual está modulada por su percepción de autoeficacia, la confianza en la efectividad de las medidas de seguridad y la anticipación de consecuencias adversas asociadas a potenciales incidentes de SI. Del mismo modo Ifinedo (2012), determina que la intención de cumplimiento se configura a partir de dos procesos cognitivos fundamentales: la evaluación de amenazas, que comprende la percepción de severidad y vulnerabilidad ante los riesgos de seguridad, y la evaluación de afrontamiento, que incluye la autoeficacia, la eficacia percibida de la respuesta y los costos asociados a su implementación. La interacción de estos procesos determina el nivel de motivación del empleado para observar y cumplir las políticas de seguridad de la información.

Asimismo, Sohrabi Safa et al. (2016), sostienen que la intención de cumplimiento de PSI no es un acto puramente racional ni aislado, sino el resultado de un proceso integrado en el que intervienen variables psicológicas, sociales y organizacionales (ver figura 39). En este sentido, una intención de cumplimiento elevada incrementa significativamente la probabilidad de que el empleado adopte comportamientos de seguridad adecuados, mientras que una intención débil o ambigua favorece conductas negligentes, resistentes o desviadas que incrementan la exposición de la organización a incidentes de seguridad. Por lo que, la intención de cumplimiento de las PSI puede conceptualizarse como el mecanismo motivacional central que conecta la percepción del riesgo, la capacidad de afrontamiento y la influencia del entorno organizacional con el comportamiento real de SI, constituyéndose en un predictor clave del cumplimiento efectivo dentro de los SGSI.

Figura 39

Variables que influyen en la intención de cumplimiento de PSI

De acuerdo con Tsohou et al. (2015), representa el antecedente inmediato del comportamiento efectivo de seguridad y refleja el grado en que los usuarios están dispuestos a internalizar y aplicar las normas de SI en su quehacer cotidiano, la intención de cumplimiento se configura a partir de la comprensión de las expectativas organizacionales expresadas en las PSI, así como del reconocimiento de los riesgos asociados al incumplimiento y de la percepción de responsabilidad individual frente a la protección de los activos de información.

Asimismo, la intención de cumplimiento de PSI se encuentra condicionada por factores sociales y organizacionales, tales como la cultura de seguridad, el apoyo

de la alta dirección, la comunicación de las políticas y la percepción de consecuencias asociadas al incumplimiento. Cuando estos elementos son internalizados por los empleados, la intención de cumplir las PSI se fortalece, incrementando la probabilidad de que se adopten prácticas seguras de manera consistente. En contraste, una intención débil o ambigua favorece conductas negligentes o desviadas, aun cuando existan controles técnicos y normativos adecuados. Por lo que la intención de cumplimiento de las PSI puede conceptualizarse como el mecanismo motivacional clave que conecta las políticas formales de seguridad con el comportamiento real de los usuarios, constituyéndose en un predictor fundamental del cumplimiento efectivo dentro de los sistemas de gestión de seguridad de la información

Finalmente, Karjalainen et al. (2020) la intención se manifiesta de forma implícita, al estar incorporada en hábitos organizacionales estables; no obstante, los autores advierten que dicha intención sigue siendo susceptible a condiciones situacionales que pueden generar retrocesos temporales hacia comportamientos de no cumplimiento. Esto refuerza la idea de que la intención de cumplimiento no solo antecede al comportamiento de seguridad, sino que también debe ser comprendida como un proceso evolutivo influido por el aprendizaje, la experiencia y el contexto organizacional. En conclusión, la intención de cumplimiento de las PSI puede definirse como un constructo dinámico y evolutivo, que refleja el grado en que los empleados están motivados de manera autónoma a alinear su comportamiento con las PSI, y cuya consolidación depende del desarrollo progresivo de cogniciones de seguridad más reflexivas, internalizadas y rutinarias dentro del entorno organizacional.

CAPÍTULO 3: METODOLOGÍA

3.1. TIPO DE INVESTIGACIÓN

3.1.1. TIPO DE INVESTIGACIÓN

La investigación tiene un enfoque de tipo cuantitativo, dado que utiliza procedimientos sistemáticos, empíricos y críticos, que permita medir objetivamente las variables de estudio, establecer relaciones entre las variables y realizar inferencias estadísticas que permitan entender el comportamiento positivo en el cumplimiento de las PSI.

3.1.2. DISEÑO DE INVESTIGACIÓN

El estudio adopta un diseño de investigación no experimental, de corte transversal y correlacional explicativo porque no manipula las variables de estudio y solo busca encontrar las relaciones de las dimensiones del modelo de comportamiento en un SGSI con la intención de cumplimiento de PSI.

3.2. UNIDAD DE ANALISIS

La unidad de análisis estuvo conformada por los profesionales especializados involucrados en la gestión, operación y implementación del Sistema de Gestión de Seguridad de la Información (SGSI), implantado en los procesos estratégicos, misionales y de apoyo, de las diferentes unidades funcionales dentro de las entidades públicas ubicadas en la ciudad de Lima. Esta unidad de análisis fue seleccionada debido a su participación en la toma de decisiones, supervisión y cumplimiento de PSI, lo que los convierte en actores clave para comprender los factores que influyen en el comportamiento organizacional respecto al SGSI.

3.3. POBLACION DE ESTUDIO

Para la población de estudio se consideró a los profesionales que desempeñan roles vinculados a la SI en entidades públicas de la ciudad de Lima, incluyendo oficiales de seguridad y confianza digital, miembros de los comités de gobierno y

transformación digital, coordinadores de la unidades funcionales de TI y el personal de áreas estratégicas involucradas en la gestión del SGSI, con experiencia mínima de 3 años en funciones relacionados con la SI y se encuentren dentro de un rango de edad aproximado de 25 a 60 años.

3.4. TAMAÑO DE MUESTRA

El tamaño de muestra estuvo constituido por 50 profesionales especializados que cumplieran los criterios de experiencia relevante en SGSI y disponibilidad para participar en el estudio.

3.5. SELECCIÓN DE MUESTRA

La selección de este número se justificó en función de la accesibilidad al personal especializado en entidades públicas y la naturaleza del estudio cuantitativo, que requiere la participación de individuos con roles específicos y conocimiento técnico en la materia. Donde se utilizó una técnica de muestreo no probabilístico por conveniencia, debido a que la población objetivo está conformada por profesionales con funciones altamente especifica dentro del SGSI y cuya disponibilidad es limitada.

3.6. TECNICAS DE RECOLECCION DE DATOS

La recolección de datos tradicional (mediante un cuestionario), se utilizó la versión electrónica del cuestionario y envió el enlace del cuestionario para el correo electrónico de algunos participantes, con el fin de acelerar la recopilación de datos. Sus respuestas fueron recogidas automáticamente en el conjunto de datos. El uso de este tipo de instalaciones, los encuestados podían responder a los cuestionarios en cualquier momento y lugar; y la recogida de datos es más fácil de usar para los investigadores.

CAPÍTULO 4: MODELO DE COMPORTAMIENTO

4.1. DISEÑO DEL MODELO

En nuestra investigación, elaboramos un “Modelo de comportamiento que influya en la intención del cumplimiento de las políticas en un SGSI en las entidades públicas del estado peruano” (ver figura 40), donde haremos uso de las teorías más relevantes y utilizadas en estudios del comportamiento del Factor Humano como: La Teoría de Bonos Sociales (SBT), Teoría de Comportamiento Planificado, la Teoría de Motivación de Protección y La Teoría de la Participación.

La investigación se encuentra en un marco que tiene 3 secciones principales:

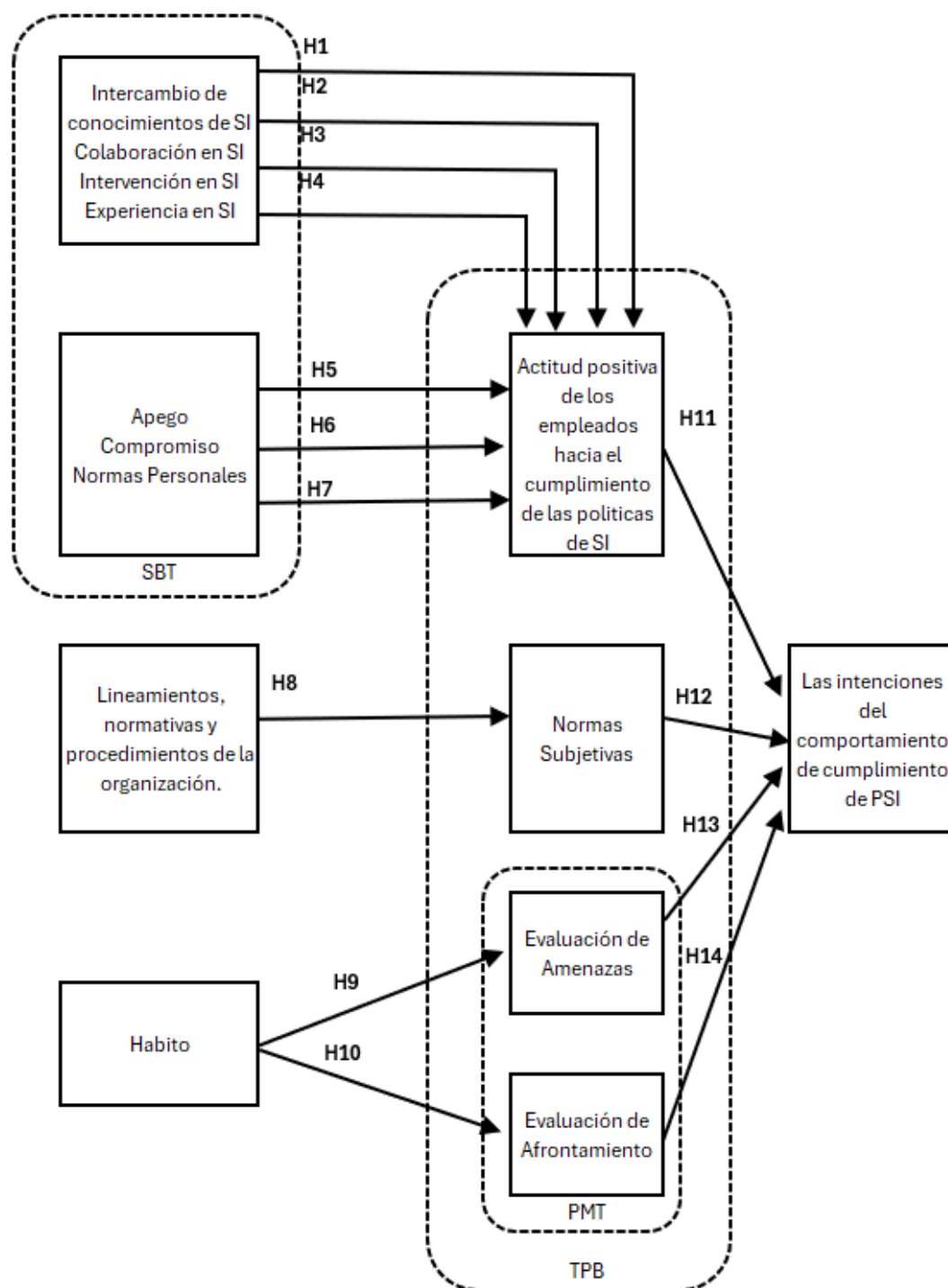
Primera sección analizaremos la actitud compuesta por el apego, el compromiso, normas personales y la participación que se presenta mediante el intercambio de conocimiento de SI, la colaboración, la intervención y la experiencia en SI.

Segunda sección, analizaremos las normas subjetivas como las Políticas de la organización, que está conformada por normativas internas como lineamientos, directivas y procedimientos institucionales.

Tercera sección, analizaremos el control conductual percibido como son los hábitos.

Figura 40

Propuesta de Modelo de comportamiento en base a teorías probadas.



4.2. DIMENSIONES DEL MODELO FORMULADO

Para la propuesta del modelo de comportamiento que influya en la intención de cumplimiento de políticas en un SGSI, se identificaron las siguientes dimensiones:

Figura 41

Dimensiones del modelo de comportamiento



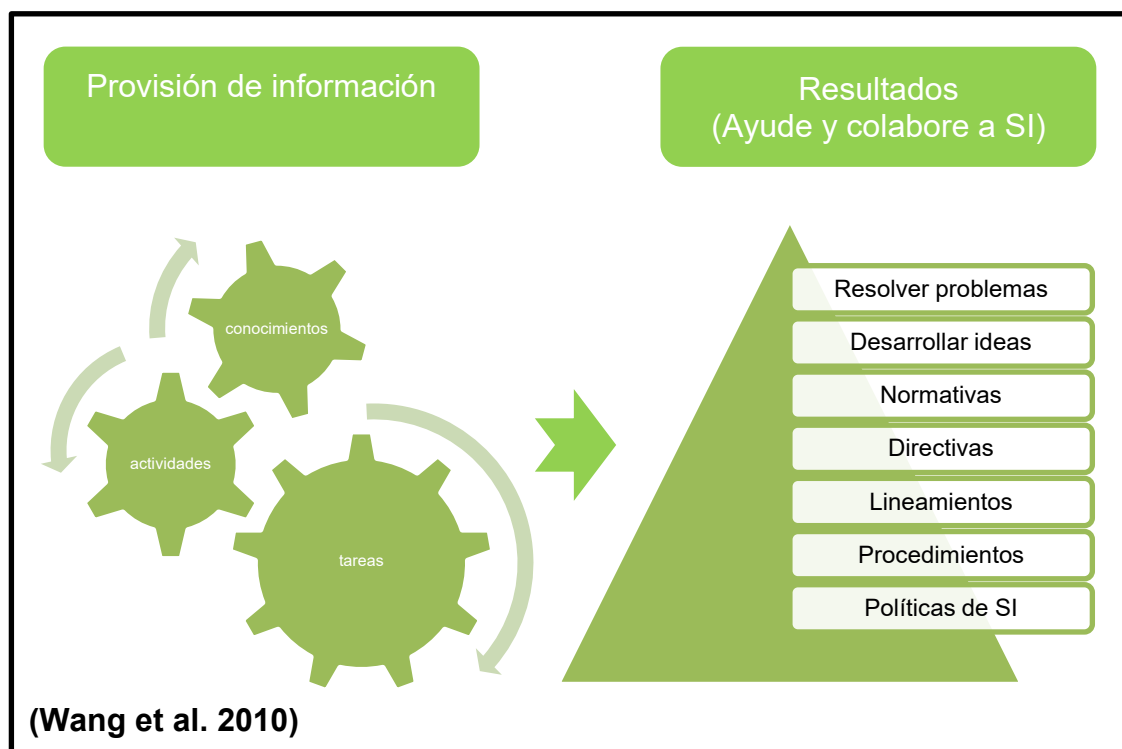
4.2.1. INTERCAMBIO DE CONOCIMIENTO DE SEGURIDAD DE INFORMACIÓN

Según Wang et al. (2010), el compartir conocimientos se refiere a la provisión de información (ver figura 42) que ayude y colabore con otros para resolver problemas, desarrollar ideas, normativas, directivas, lineamientos, procedimientos y políticas de SI. las cuales se dan a través de correspondencia escrita o reuniones presenciales con otros expertos, las cuales se estarán

documentando, organizando y capturando conocimiento para otros. Para los investigadores es importante compartir conocimientos a través del cual los empleados pueden contribuir con la aplicación del conocimiento, la innovación y en última instancia, la ventaja competitiva de la organización. El intercambio de conocimientos entre los empleados y dentro de los equipos permite a las organizaciones explotar y capitalizar los recursos basados en el conocimiento. La investigación ha demostrado que el intercambio y la combinación de conocimientos se relacionan positivamente con las reducciones en los costos de producción, la finalización rápida de proyectos de elaboración de productos, el desempeño del equipo, mejora de las capacidades de innovación y el buen desempeño de la empresa, incluido el crecimiento de las ventas y la generación de nuevos productos y servicios.

Figura 42

Intercambio de conocimiento



En estudios relacionados a la SI Sohrabi Safa et al. (2016) indica que el compartir conocimientos sobre SI no solo aumenta el nivel de conciencia como un enfoque

eficaz, sino que también reduce el costo de la SI en las organizaciones. Intercambiando conocimientos sobre SI, como compartir experiencias, ideas y conocimientos con el fin de salvaguardar la información en las organizaciones. Los expertos se enfrentan a problemas similares en este ámbito ofreciendo soluciones adecuadas, en lugar de reinventar la rueda de la SI. Evitar el desarrollo de las mismas soluciones para problemas similares mediante el intercambio de conocimientos conduce a evitar pérdidas de tiempo y costos adicionales.

Según Dang-Pham et al. (2017), el intercambio de conocimiento de seguridad de información es un tema emergente, en su estudio indica que los consejos de SI, juega un papel crucial en ayudar a las organizaciones a desarrollar lugares de trabajo de SI centrados en las personas, mediante los cuales se fomenta la conciencia y sensibilización de SI del factor humano y la responsabilidad personal por la SI. Definiendo que mientras haya actitud favorable hacia la seguridad y la participación en las actividades diarias como asesoramiento, intercambio de trabajo y dar soluciones a problemas de seguridad, se obtendrá un impacto positivo en el intercambio de consejos de seguridad.

Al respecto conviene decir que descubrieron que las comunicaciones informales de SI que tienen lugar dentro de las áreas de trabajo tienen un gran impacto y por lo tanto merecen mayor atención. Al mismo tiempo argumentaron que fomentar el intercambio de conocimientos sobre SI en el lugar de trabajo, trae muchos beneficios a la gestión de la SI en la organización que incluyen la propagación efectiva de experiencias, conocimientos e ideas de SI entre los empleados, además de prevenir reprocesos y permitir más tiempo para dedicarlo al desarrollo de mejores soluciones de SI.

4.2.2. COLABORACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Según Ahmad et al. (2012) destacaron la comunicación y la colaboración para responder a los incidentes de SI, tal como se observa en la figura 43, donde un incidente de SI ocurre cuando hay un ataque directo o indirecto a la

confidencialidad, integridad y disponibilidad de la información. Además, definen el objetivo principal de un equipo de respuesta a incidentes de SI es mitigar el impacto de un posible incidente importante, así mismo se tiene diferentes respuestas. En primer lugar las respuestas a incidentes pueden ser puramente reaccionarios, formándose equipos de respuesta para solucionar específicamente cada incidente una vez detectado. En segundo lugar, tenemos los equipos de respuesta a incidentes de seguridad informática más avanzados que adoptan un papel proactivo, buscando las vulnerabilidades antes de que se conviertan en incidentes brindan asesoramiento y concienticen a los empleados sobre cuestiones de SI.

Es decir, la colaboración en SI se refiere al trabajo en equipo para realizar diferentes actividades de SI o lograr metas propuestas de SI. Por lo que es sinónimo de participación, asociación y el trabajo en equipo; siendo un proceso recursivo, en el que dos o más personas, equipos y organizaciones, trabajan juntas para alcanzar metas compartidas. La colaboración en SI ayuda a los expertos a recopilar, integrar, clasificar, distribuir y compartir conocimientos sobre SI con otros expertos y empleados.

Figura 43

Colaboración en SI

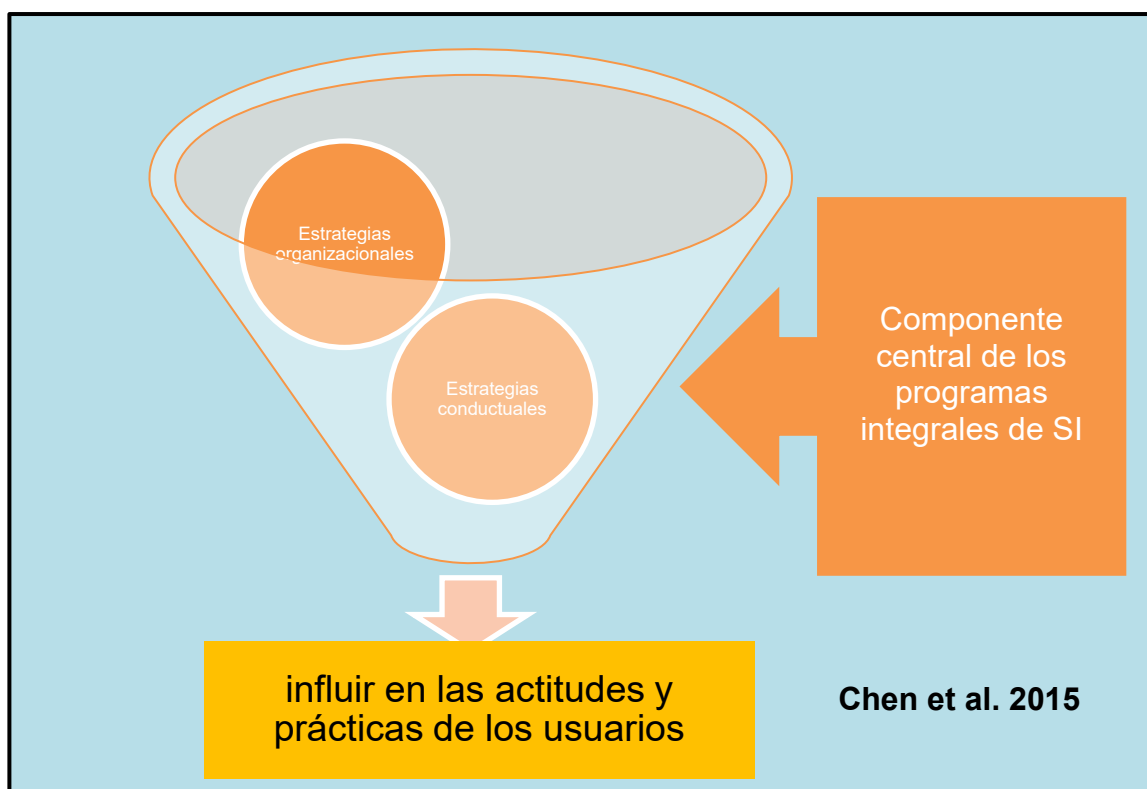


4.2.3. INTERVENCIÓN EN SEGURIDAD DE INFORMACIÓN.

Se entiende como las acciones organizacionales orientadas a influir en el comportamiento de los empleados, tales como programas de capacitación, campañas de sensibilización y concienciación, simulacros, comunicaciones formales y retroalimentación continua. Para Chen et al. (2015) sostienen como un componente central de los programas integrales de SI (figura 44), los cuales no se limitan a controles técnicos, sino que incorporan estrategias organizacionales y conductuales para influir de manera directa en las actitudes y prácticas de los usuarios, argumentando que las intervenciones bien diseñadas permiten alinear los valores individuales de los empleados con los objetivos de SI de la organización, favoreciendo la adopción de comportamientos seguros de forma continua.

Figura 44

Componente central de intervenciones

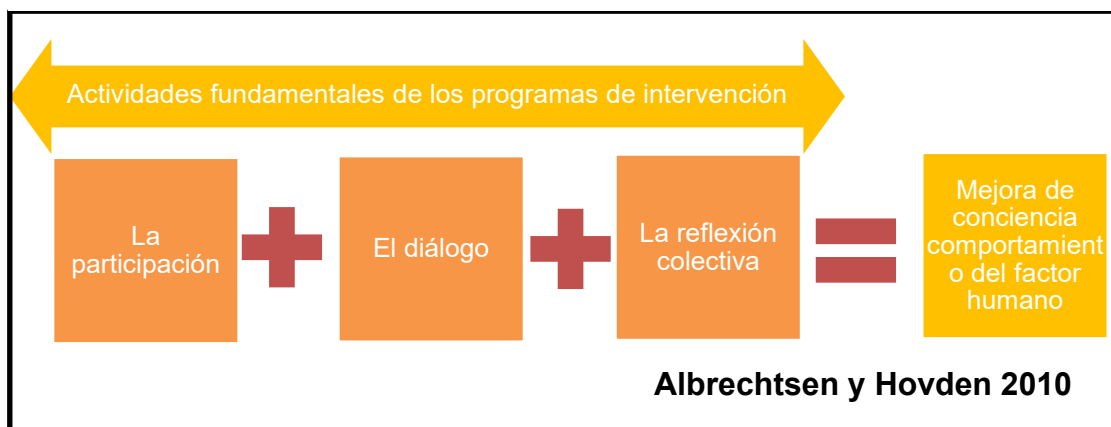


Para Albrechtsen y Hovden (2010), su estudio aplicó la intervención mediante pequeños talleres destinados a mejorar la conciencia y el comportamiento del factor humano de la SI, mediante los programas de concientización sobre seguridad de la información. Estos programas destacaron la participación de los empleados, el diálogo y la reflexión colectiva en grupos. Del mismo modo difiere de los principales métodos de concientización y sensibilización sobre SI, que típicamente tienen como objetivo tener un impacto a nivel individual a través de un enfoque basado en expertos dirigido a una gran población, mediante diferentes medios de comunicación como presentaciones formales, correos electrónicos, folletos y carteles. Por lo que demuestran que la participación local de los empleados, la reflexión colectiva, los procesos grupales y la creación de conocimiento a nivel organizacional sí generan cambios en la conciencia y el comportamiento de SI a nivel individual.

Albrechtsen y Hovden (2010) analizaron los efectos de los programas de capacitación de mejora de conciencia y el comportamiento del factor humano en SI (figura 45). Indicando que el objetivo de los programas de capacitación era mejorar las actitudes de SI entre los empleados y mejorar el comportamiento laboral relevante para la SI. Además, demostraron que la intervención en SI de los empleados locales, la reflexión colectiva y los procesos grupales generan cambios a corto plazo en la concientización y el comportamiento en SI.

Figura 45

Actividades fundamentales en la intervención



Chen et al. (2015), investigo los componentes claves de los programas integrales de SI que tengan influencia sobre la cultura de SI, que incluyen principalmente las PSI, programas de Educación, Capacitación y Concienciación de SI y monitoreo de seguridad que se han establecido ampliamente en muchas organizaciones para salvaguardar la información para la estabilidad y éxito de los negocios, resaltan la importancia que son los programas de Educación, capacitación y concientización de SI, bien diseñados e implementados pueden cambiar percepciones, actitudes y creencias en el factor humano en relación a la SI, realizar actividades de SI, incluso a costa de su esfuerzo y carga de trabajo, creando una cultura de SI. Confirma la importancia de los programas educación para incluir a los empleados en la participación de la formulación, diseño y desarrollo de PSI si la intención es construir una cultura de seguridad de información sólida y sostenible. También es importante la relación entre el conocimiento de los programas de educación y la PSI. Resaltaron a un hallazgo importante que simplemente tener PSI implementadas sin asegurarse de que los empleados las comprendan plenamente y las perciban favorablemente, no pueden inculcar el propósito de tales políticas entre los empleados y en consecuencia, el efecto de las políticas quedaría marginado. Por lo que las organizaciones deben involucrar a los empleados en el desarrollo e implementación de esquemas de monitoreo para que los comentarios sobre el cumplimiento de las PSI puedan ayudar a fomentar una cultura de SI. Por otro lado, Tsohou et al. (2015) define que los esquemas de los programas enfocados al comportamiento del factor humano involucran una estructura piramidal de comunicación de SI, que incluye niveles de concientización, capacitación y educación, tal como se observa en la figura 46.

Figura 46

Niveles de programas de intervención



Según Dang-Pham et al. (2017), indica que los empleados puedan adquirir su concientización sobre la SI y la responsabilidad de sus acciones a través de la participación en las redes sociales de la organización. Además, decidió seleccionar, capacitar y luego colocar campeones de SI en todos los departamentos. Ayudando a descentralizar el modelo de gestión de seguridad y difundir la conciencia de seguridad de manera más eficaz y eficiente. Tomando criterios para seleccionar campeones de seguridad como los empleados que trabajan en el mismo departamento y tener antigüedad.

Bauer et al. (2017), diseñaron programas de concientización de SI para superar el incumplimiento de los usuarios con las PSI en los bancos. Utilizando programas estructurados de capacitación de seguridad de información para educar a los empleados sobre los riesgos de seguridad de información y cómo comportarse para cumplir con las PSI. En consecuencia, tales programas de capacitación de SI comprenden intervenciones planificadas sistemáticamente, que tienen como objetivo transportar continuamente información de SI. Estas intervenciones de capacitación de SI pueden incluir mensajes de intranet,

carteles, vasos impresos o tutoriales de aprendizaje electrónico para aumentar la capacitación de SI de los usuarios y reducir el comportamiento de riesgo voluntario y no voluntario. Por otro lado, Hyeun-Suk et al. (2009) el mayor desafío para los profesionales de la SI es saber cómo transformar a los usuarios de la mayor vulnerabilidad a la primera línea de defensa. Identificando condiciones más específicas que influyen en la formación de la autoeficacia en la SI, podemos desarrollar un programa de SI más eficaz que las organizaciones deberían poder utilizar para promover el comportamiento de mejora en los usuarios. Recomendaron que los gerentes de SI presten más atención al ciclo PDCA para incorporar en particular la evaluación y las adaptaciones del programa de capacitación de SI. Este estudio demostró que su enfoque interactivo parece ser más beneficioso para aumentar la percepción del riesgo de SI. Además, al diseñar los programas de capacitación de SI, los gerentes de SI deben considerar un concepto más diferenciado para llegar efectivamente a todos los usuarios. Los bancos, así como otras organizaciones centradas en la información, deben personalizar sus programas de capacitación de SI distinguiendo entre las necesidades de SI de los grupos de usuarios, en términos de usuarios de la sede y de la sucursal.

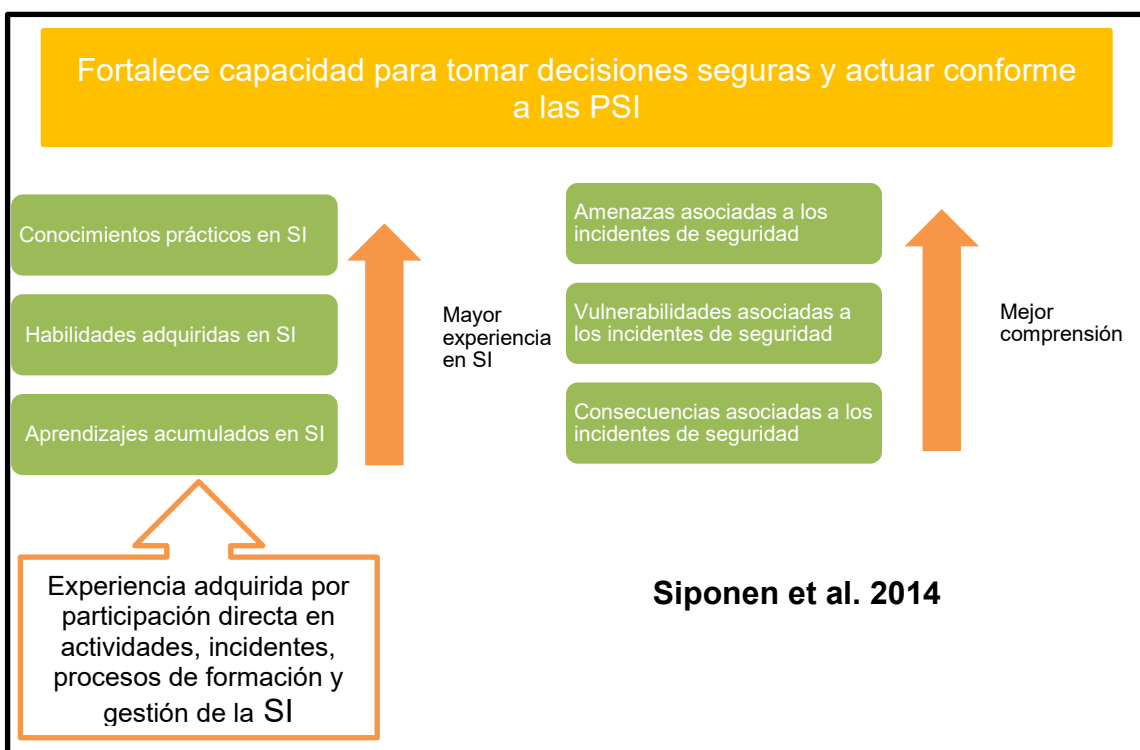
4.2.4. EXPERIENCIA EN SEGURIDAD DE INFORMACIÓN.

La experiencia en SI constituye un factor determinante en la configuración del comportamiento seguro de los empleados y en su disposición a cumplir con las PSI. Desde una perspectiva conductual y cognitiva, la experiencia se define como el conjunto de conocimientos prácticos, habilidades adquiridas y aprendizajes acumulados a partir de la participación directa en actividades, incidentes, procesos de formación y gestión de la seguridad de la información dentro de la organización. Estudios sostienen que los empleados con mayor experiencia en SI presentan una mejor comprensión de las amenazas, vulnerabilidades y consecuencias asociadas a los incidentes de SI (ver figura 47), lo que fortalece su capacidad para tomar decisiones seguras y actuar conforme a las PSI establecidas (Siponen et al. 2014). Por lo tanto, la experiencia no solo incrementa

el conocimiento técnico, sino que también influye en la internalización de normas y en la percepción de responsabilidad individual frente a la protección de los activos de información. Además, Weishäupl et al. (2018), en su estudio resalta la necesidad de proteger la información en las organizaciones, mediante la toma de decisiones, la evaluación y el aprendizaje de las organizaciones a partir de decisiones de inversión anteriores. Ampliamos las investigaciones donde ofrecen una visión exhaustiva y teórica de cómo se realizan las inversiones en SI en su contexto. En presencia de limitaciones presupuestarias y activos de información que proteger, las organizaciones deben decidir en qué medidas de seguridad de tecnologías de información invertir, cómo evaluar esas decisiones de inversión y cómo aprender de decisiones pasadas para optimizar las acciones de inversión en seguridad futuras.

Figura 47

Importancia de la experiencia para el cumplimiento del PSI

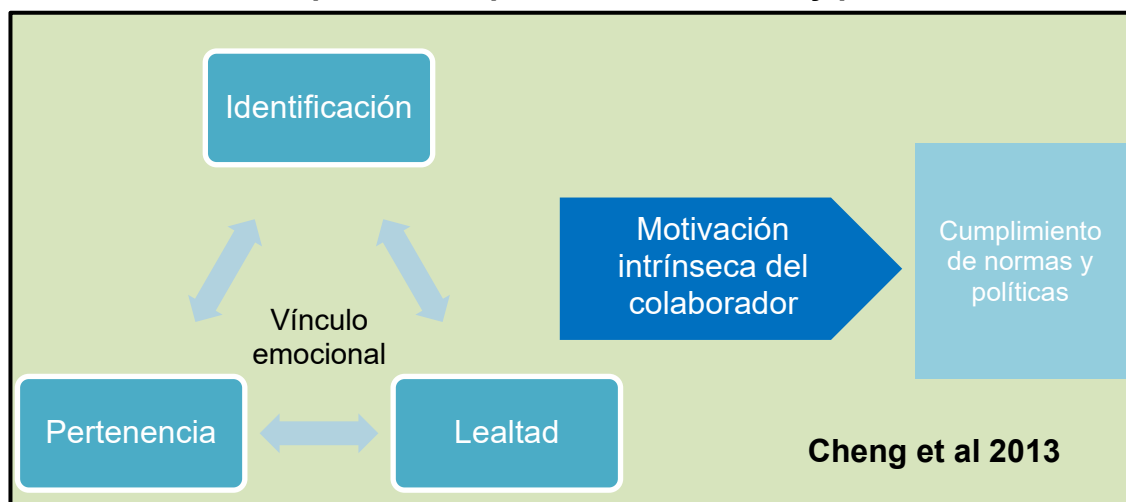


Por otro lado, Moon et al. (2018), sostienen un rol relevante en la formación de comportamientos de SI, al influir en la manera en que los empleados interpretan, evalúan y responden a las PSI, así como una mayor capacidad para reconocer amenazas y aplicar prácticas seguras de manera consistente en sus actividades laborales. Asimismo, investigaciones empíricas evidencian que la experiencia en SI contribuye al desarrollo de hábitos seguros y a una mayor adherencia a las políticas organizacionales, especialmente cuando dicha experiencia es reforzada mediante programas de formación continua, simulaciones de incidentes y participación en procesos del SGSI (Tsohou et al. 2015).

4.2.5. APEGO

Describe el vínculo emocional que los empleados desarrollan con la organización, caracterizado por sentimientos de identificación, lealtad y pertenencia. Para Cheng et al (2013), constituye un determinante clave del comportamiento individual dentro de las organizaciones, especialmente en contextos donde el cumplimiento de normas y políticas depende en gran medida de la motivación intrínseca del colaborador (ver figura 48). Asimismo, sostiene que, cuando los empleados desarrollan un alto nivel de apego organizacional, tienden a comportarse de manera coherente con los objetivos institucionales, ya que perciben el bienestar de la organización como estrechamente vinculado a su propio bienestar, lo que refuerza su disposición a actuar conforme a los intereses organizacionales.

Figura 48

Determinante clave para el cumplimiento de normas y políticas

Por otro lado, D'Arcy y Teh (2019) se basaron en los factores afectivos como impulsores de las incertidumbres en el cumplimiento de las (PSI), aplicando la Teoría de eventos afectivos que es un marco general que se ocupa de los estados afectivos en el trabajo y su relación con el comportamiento del empleado. Indicando que el afecto se refiere al estado de sentimiento de uno o cómo se siente en un momento dado, como por ejemplo en el contexto organizacional, el sentimiento hacia el trabajo o algún aspecto del trabajo.

Asimismo, Cheng et al. (2013) destacan que tanto los controles formales como los controles informales tienen efectos significativos en el incumplimiento de las PSI por el factor humano; argumentando los lazos sociales actúan como controles formales y las presiones sociales actúan como controles informales. Determinaron que los controles formales son importantes para formar el comportamiento de los empleados a través de las normas regularizadas y las correspondientes sanciones establecidas por la organización; expresada a través de leyes, estatutos, reglas y regulaciones contra comportamientos desviados, además, que los lazos de la persona con la organización, jefes, supervisores, compañeros de trabajo y la presión de otros pueden influir en su acción; se basan en costumbres, tradiciones, normas, moralidad y otros valores sociales; es implementado por grupos o individuos controladores no oficiales.

Yazdanmehr y Wang (2016), realizaron un estudio de los empleados que trabajan en un grupo o equipos de trabajo dentro de una organización, es probable que otros influyan en su comportamiento u opiniones, así mismo definen que las normas sociales de un empleado en una organización son basadas en interacciones sociales entre individuos, definen ampliamente las reglas de comportamiento basadas en creencias comunes cómo las personas deben actuar en una situación particular. Indirectamente promueven el bienestar de un grupo a través de recompensas y sanciones informales basadas en las expectativas del grupo.

Tsohou et al. (2015) en su estudio determinan que las personas pueden emitir juicios y tomar decisiones rápidamente en función de sus impresiones afectivas. Al mismo tiempo el afecto es que los individuos tienden a subestimar los riesgos y costos asociados con las cosas que les gustan y los sobreestiman cuando están asociados a cosas que no les gustan. Para Liu et al. (2020) estudiaron la medida en que un subordinado y su supervisor están involucrados y afectados por los asuntos personales y familiares; por lo que resultados de la investigación indican que la dimensión afectiva del subordinado y su supervisor desempeña un papel crucial en la promoción del cumplimiento de las normas de los empleados, tanto directa como indirectamente.

4.2.6. COMPROMISO

Es el grado en el que el empleador está dispuesto a invertir esfuerzo, tiempo y lealtad para contribuir al logro de los objetivos institucionales. Este compromiso se asocia con una mayor responsabilidad y disposición a cumplir normas y políticas. Liu et al. (2020), determinaron que el compromiso organizacional desempeña un rol fundamental en la explicación del comportamiento de cumplimiento de las políticas organizacionales, particularmente en contextos donde el factor humano representa un componente crítico del riesgo, como en la SI. Considerando que los empleados con altos niveles de compromiso organizacional tienden a mostrar una mayor predisposición a cumplir las políticas internas (ver figura 49), ya que perciben el cumplimiento como una expresión de

responsabilidad y lealtad hacia la organización, consideraron que el compromiso organizacional tiene tres dimensiones principales.

Figura 49

Dimensiones de compromiso organizacional



Dado que el compromiso afectivo ha sido visto como el determinante más fuerte de los comportamientos favorables de los empleados y ha sido considerado como el "eslabón perdido" en la investigación de SI, sostenemos que la dimensión afectiva del compromiso organizacional es más adecuada para nuestro contexto de investigación. Por lo tanto, evidencia suficiente sugiere que el compromiso organizacional juega un papel fundamental en motivar el cumplimiento del PSI.

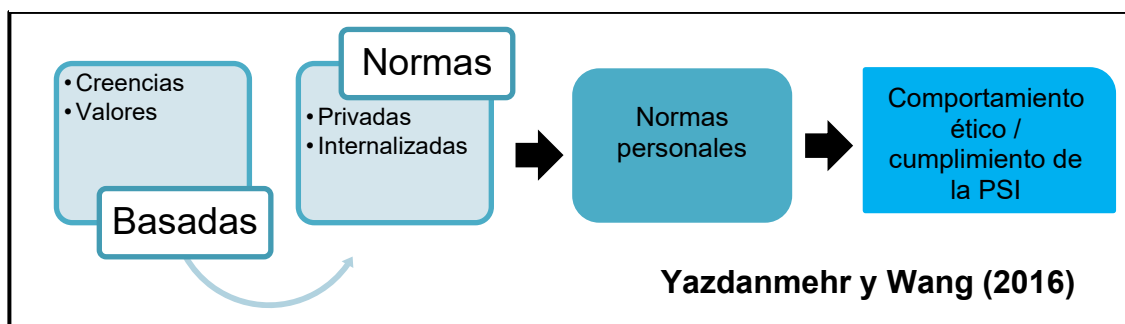
De manera similar, el compromiso organizacional también puede considerarse como una actitud o percepción hacia los intercambios sociales entre un empleado y su organización. Proporcionando una base teórica para relaciones de alta calidad entre empleados y gerentes, así mismo entre empleados y sus organizaciones, que también son adecuados para explicar los comportamientos de cumplimiento de PSI de información en el lugar de trabajo. Por lo tanto, proponemos la siguiente hipótesis

4.2.7. NORMAS PERSONALES

Las normas personales asociadas a la ética individual representan los valores morales internos que guían el comportamiento del factor humano, que influyen en la decisión de cumplir con las PSI, incluso en ausencia de supervisión o sanciones. Según Yazdanmehr y Wang (2016), constituyen un determinante fundamental del comportamiento ético y de cumplimiento de la PSI, determinando que los empleados con normas personales sólidas tienden a evaluar el incumplimiento de las PSI no solo desde una perspectiva de convivencia, sino también desde una dimensión moral, considerando las posibles consecuencias negativas para la organización, los usuarios y otros grupos de interés. Además, definen que las normas personales son normas privadas e internalizadas basadas en las creencias y valores (ver figura 50), que influyen en el comportamiento cuando un individuo siente que sus valores más importantes están en peligro. Sus recompensas y sanciones son autoimpuestas.

Figura 50

Influencia de las normas personales en el comportamiento ético.



Por otro lado, Tsohou et al. (2015), determinaron en su estudio que la actitud hacia el cumplimiento de las PSI está influenciada por un conjunto de creencias que constituyen la evaluación general de las consecuencias de cumplimiento o incumplimiento y que esta evaluación de consecuencias está conformada por un conjunto de creencias sobre los resultados de comportamiento conforme o no conforme. Otras investigaciones empíricas en SI confirman que las normas personales tienen un impacto directo y significativo sobre la actitud y la intención de cumplimiento de las PSI, superando en algunos casos la influencia de factores

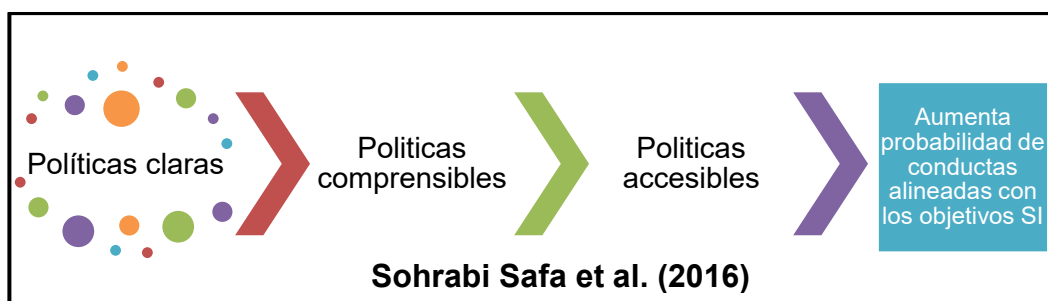
como la amenaza percibida o las sanciones (Hina et al. 2020). Ello se debe a que la ética internalizada genera una motivación intrínseca que promueve conductas consistentes y sostenidas en el tiempo.

4.2.8. LINEAMIENTOS, NORMATIVIDAD Y PROCEDIMIENTOS DE LA ORGANIZACIÓN

Se definen como el conjunto de lineamientos, normas formales y directrices institucionales establecidas para orientar el comportamiento de los colaboradores y regular el uso adecuado de los recursos organizacionales. Para Sohrabi Safa et al. (2016), las políticas de la organización desempeñan un rol central como mecanismo formal de control, influyendo directamente en la actitud, la intención y el comportamiento de cumplimiento de los empleados. Sostienen los pilares en la normatividad y políticas en las organizaciones (ver figura 51), que incrementa la probabilidad de que los colaboradores adopten conductas alineadas con los objetivos de SI.

Figura 51

Pilares de las políticas en las organizaciones.



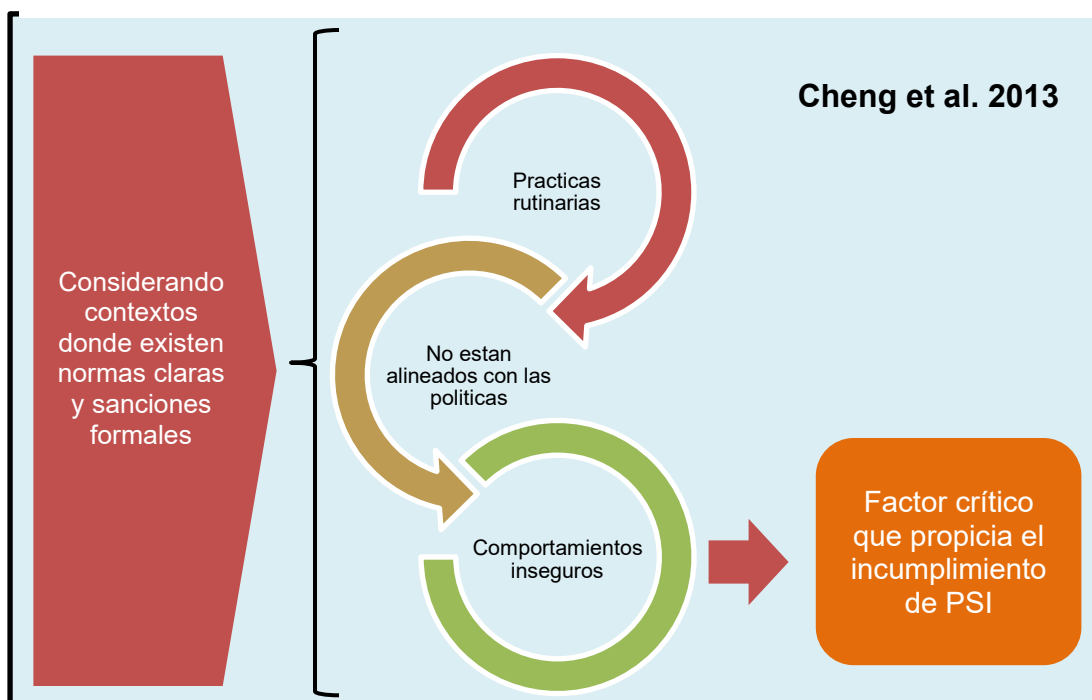
Asimismo, diversos estudios empíricos evidencian que la efectividad de las políticas depende en gran medida de su adecuada comunicación, accesibilidad y coherencia con la cultura organizacional. Tsohou et al. (2015) sostienen que la legitimidad ética de las políticas refuerza las normas subjetivas y reduce la percepción de las políticas como simples imposiciones burocráticas.

Por tanto, las políticas de la organización no deben entenderse únicamente como documentos normativos, sino como instrumentos estratégicos de gestión del comportamiento ético y seguro. Su correcta formulación, difusión y aplicación contribuyen de manera decisiva a consolidar una cultura de seguridad basada tanto en el control formal como en la convicción moral de los empleados, incrementando así la intención de cumplimiento de las PSI.

4.2.9. HÁBITOS.

Son comportamientos repetidos que se ejecutan de forma automática y con bajo esfuerzo cognitivo. Según Cheng et al. (2013), los hábitos desempeñan un papel central en la explicación de las violaciones de las PSI, tal como se observa en la figura 52, ya que muchos comportamientos inseguros no responden a decisiones racionales deliberadas, sino a prácticas rutinarias adaptadas en la conducta diaria de los empleados. Los autores indicaron que los hábitos mejoraron fuertemente los procesos cognitivos de la teoría del comportamiento planificado (TPB). Además, casi todos los componentes de la teoría de Motivación de Protección (PMT) se constituyen en factores relevantes de la intención de cumplimiento de las PSI por el factor humano.

Figura 52

Hábitos papel central en las violaciones de PSI

Vance et al. (2012) Estudiaron el hábito asumiendo que el comportamiento pasado afecta considerablemente la toma de decisiones, donde integramos el hábito (una forma rutinaria de comportamiento pasado) con la Teoría de la Motivación de Protección (TMP) para explicar el cumplimiento PSI, demostrando que el cumplimiento habitual de la SI reforzaba considerablemente los procesos cognitivos teorizados por la TMP, así como la intención de los empleados de cumplimiento de las PSI. También descubrimos que casi todos los componentes de la TMP impactaban significativamente en la intención de los empleados de cumplir con las PSI, por lo que destacaron la importancia de abordar el comportamiento pasado y automático de los empleados para mejorar el cumplimiento.

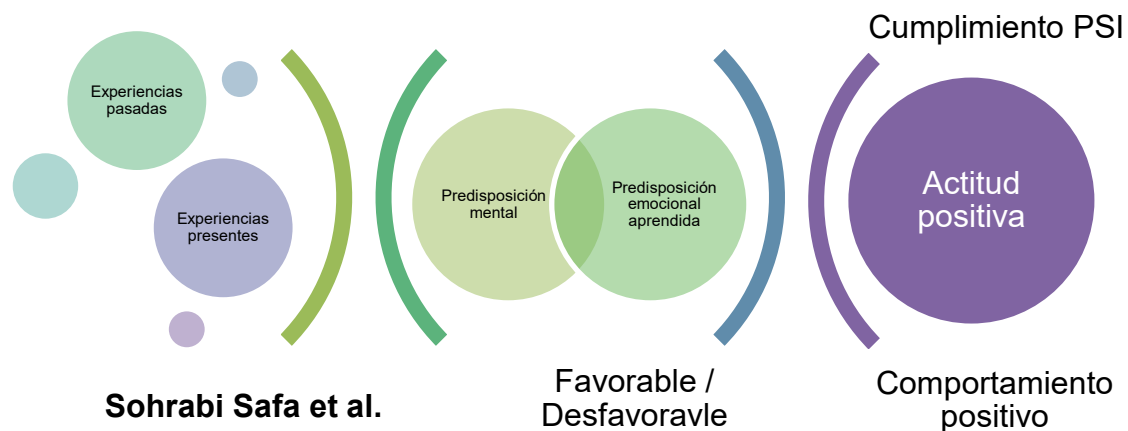
Chen et al. (2015) Proponen que los programas integrales de SI es ayudar a construir una cultura de SI donde se establecen valores, normas y conocimientos de SI, se convierte en un aspecto natural e inherente en los trabajos diarios relacionados con la información de los empleados. Por lo que definen a la cultura

de SI una colección de valores, creencias y supuestos de SI compartidos de alto nivel en la organización y puede conducir a comportamientos inconscientes, continuos y habituales en la SI.

4.2.10. ACTITUD

Es la evaluación psicológica general, favorable o desfavorable, que un individuo realiza respecto a un comportamiento específico, incluyendo directamente en su disposición a ejecutarlo, constituye un determinante en el comportamiento del factor humano al reflejar sus creencias, percepciones y valoraciones sobre la importancia y utilidad de dichas políticas. Para Sohrabi Safa et al. (2016), la actitud del factor humano se forma sobre la base de las experiencias pasadas y presentes, se refiere a la predisposición mental y emocional aprendida para responder de forma consistente, ya sea favorable o desfavorable, hacia un objeto, persona, grupo o situación en particular. En particular si las personas evalúan un comportamiento como positivo (actitud positiva) tal como se observa en la figura 53. Esto nos lleva al grado de efectos positivos sobre el comportamiento frente a la SI, en las que mitiga el riesgo de violaciones de SI en las organizaciones. Inducimos que una actitud positiva hacia las PSI organizacional tiene un efecto positivo en el cumplimiento del PSI.

Figura 53

Formación de la actitud para cumplimiento de PSI**4.2.11. NORMAS SUBJETIVAS**

Definido como la percepción que tiene un individuo sobre la presión social ejercida por personas o grupos significativos tales como superiores, compañeros de trabajo o la organización en su conjunto para que adopte o evite un determinado comportamiento. Del mismo modo Sorhabi Safa et al. (2016), señalan que las normas subjetivas constituyen un determinante clave de la intención de cumplimiento de las PSI (ver figura 54), al influir directamente en la motivación del individuo para actuar conforme a las expectativas sociales y organizacionales. Los investigadores mantienen que cuando los empleados perciben que sus superiores y colegas consideran importante el cumplimiento de las PSI, aumenta significativamente su disposición a adoptar comportamientos seguros, incluso en ausencia de mecanismos coercitivos formales. Asimismo, las normas subjetivas muestran la presión social sobre los empleados para realizar un comportamiento específico y las opiniones de los demás sobre el intercambio de conocimientos sobre SI.

Figura 54

Formación de las normas subjetivas para el cumplimiento de PSI

Van Slyke y Belanger (2020), explican que la práctica de seguridad ha reconocido desde hace mucho tiempo que los activos de información eficaces necesitan una combinación de controles administrativos, técnicos y físicos destinados a restringir el comportamiento del factor humano. Por otro lado, Ali et al. (2019) señala que los requisitos legales y contractuales son componentes esenciales de la SI ya que las organizaciones deben comprender la importancia del cumplimiento legal y las obligaciones que se derivan en las diferentes acciones de salvaguardar la información de la organización. Los aspectos legales de los requisitos de SI a menudo son exigidos por estándares y normatividad relacionado a la privacidad y datos sensibles.

Según Barton et al. (2016) en su investigación verificaron que la motivación de la alta dirección a comprometerse con la SI, es fundamental para el éxito de la implementación de un Sistema de SI. Abordando cómo las presiones externas motivan la participación de la alta dirección. Hou et al. (2018). proponen estrategias de respuesta organizacional a presiones regulatorias que están determinadas conjuntamente por los incentivos internos organizacionales y la supervisión del gobierno, promoviendo Sistemas de SI eficientes, el gobierno debe garantizar que los documentos legales pertinentes y la orientación política asociada son útiles para las organizaciones que buscan proteger su seguridad de la información proporcionando un incentivo para cumplir. Al mismo tiempo, el

gobierno también debe considerar la importancia de aplicar medidas más estrictas de aplicación en la supervisión y las inspecciones, para asegurar que las leyes relativas a la organización del Sistema de Seguridad de Información se respetan en la práctica.

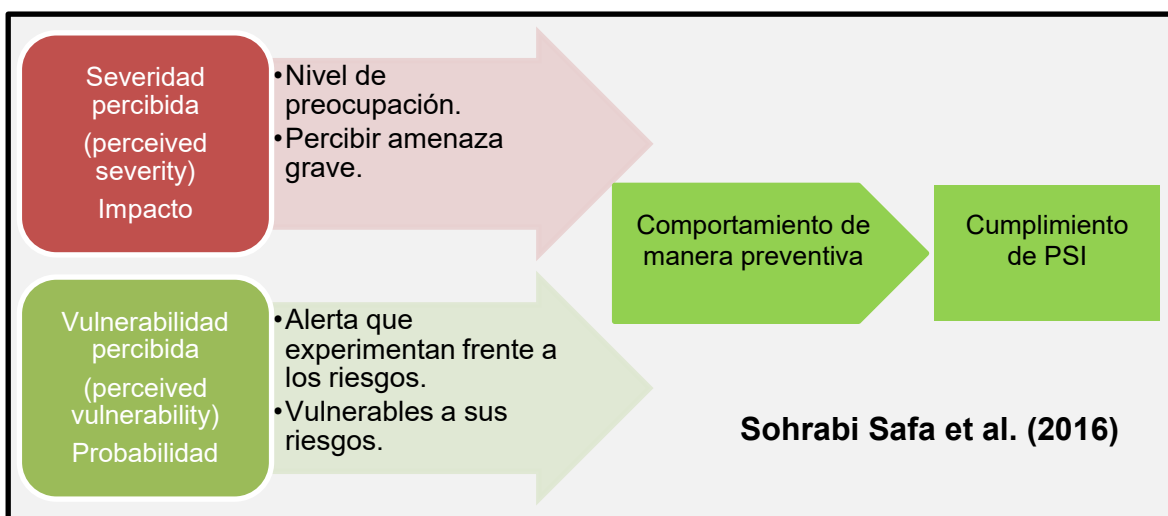
Por otro lado, Chua et al. (2018) estudiaron que las regulaciones contienen cláusulas que dictan cómo las organizaciones deben recopilar, almacenar y utilizar los datos de los consumidores para que cumplan con las regulaciones, cuyo incumplimiento resultaría en considerables sanciones. La SI se ha convertido en una de las principales prioridades de muchas organizaciones, porque el aseguramiento institucional y el cumplimiento de las regulaciones son factores importantes que afectan el proceso de toma de decisiones de los consumidores.

4.2.12. EVALUACIÓN DE AMENAZAS

Se define como el proceso cognitivo mediante el cual los individuos perciben, interpretan y valoran la existencia, probabilidad y severidad de una amenaza, así como su vulnerabilidad personal frente a ella. Para Sohrabi Safa et al. (2016), la evaluación de amenazas desempeña un rol clave en la explicación del comportamiento de cumplimiento de las PSI (ver figura 55), al determinar el nivel de preocupación y alerta que experimentan los empleados frente a los riesgos de SI. Los autores sostienen que cuando los individuos perciben una amenaza como grave y consideran que son vulnerables a sus consecuencias, se incrementa su motivación para actuar de manera preventiva y cumplir con las PSI. Asimismo, el control conductual percibido³ se refiere a la percepción de una persona de si pudiera completar con éxito una tarea o comportamiento. Se calcula la dificultad de la tarea frente a las capacidades percibidas.

³ Percepción que tiene un individuo de la facilidad o dificultad para realizar un comportamiento específico, que está influenciada por la disponibilidad de los recursos necesarios para llevar a cabo ese comportamiento

Figura 55

Organización de evaluación de amenazas para el cumplimiento de PSI.

Para Tsohou et al. (2015) para influir en el comportamiento de SI de los usuarios en el cumplimiento de las PSI, debemos afectar la forma en que los usuarios perciben los riesgos (evaluación de amenazas) y toman decisiones (Evaluación de afrontamiento) relacionadas con la SI. Los programas de sensibilización deben ir más allá de la simple comunicación de información relacionada con la SI y alinearse con el proceso de toma de decisiones individual. Asimismo, Gratian et al. (2018), la evaluación de amenazas en el marco de la Teoría de Motivación de Protección se refiere al proceso cognitivo mediante el cual un individuo valora el impacto y la probabilidad de un riesgo en la SI. Compuesta por dos dimensiones:

- **Severidad percibida** (*perceived severity*): la valoración del daño o impacto potencial de una violación de seguridad de información (por ejemplo, pérdida de datos, sanciones económicas, daño reputacional).
- **Vulnerabilidad percibida** (*perceived vulnerability*): la percepción de la probabilidad personal de ser víctima de dicho riesgo o ataque.

Además, demostró que la disposición a asumir riesgos de salud y seguridad estaba inversamente correlacionada con la conciencia proactiva y los

comportamientos de actualización. descubrió que los usuarios reacios al riesgo eran menos propensos a caer en el phishing, demostrando nuevamente que las preferencias de tomar riesgos pueden influir en los comportamientos de seguridad.

Fischer-Preßler et al. (2021) mostraron que la percepción de amenazas (severidad percibida y la vulnerabilidad percibida) explican la intención de cumplir con PSI en las organizaciones, también Alrawhani et al. (2024), hallaron que la percepción de amenazas (severidad percibida y vulnerabilidad percibida) tiene un efecto directo en la motivación a cumplir las PSI, pero su fuerza depende de la confianza en las medidas de afrontamiento y Sulaiman et al. (2022) demostraron en el factor humano que una baja percepción de vulnerabilidad reducía la intención de seguir las políticas, pese a recibir formación. También, Ali et al. (2019) señala que las evaluaciones de riesgos para la SI también han considerado la conciencia del usuario como una parte esencial de la seguridad general de la información.

4.2.13. EVALUACIÓN DE AFRONTAMIENTO

Define como el proceso cognitivo mediante el cual los individuos valoran su capacidad para enfrentar eficazmente una amenaza, considerando la efectividad de las respuestas disponibles, su propia competencia para ejecutarlas y los costos asociados a dichas acciones. Según Sohrabi Safa et al. (2016), la evaluación de afrontamiento desempeña un rol determinante en el comportamiento de cumplimiento de las PSI (ver figura 56), al reflejar el grado en que los empleados perciben que las medidas de seguridad son efectivas, viables y aplicables en su entorno laboral. Los autores sostienen que incluso cuando los individuos perciben una amenaza como grave, el cumplimiento solo se materializa si consideran que cuentan con los recursos, conocimientos y capacidades necesarias para responder adecuadamente a dicha amenaza.

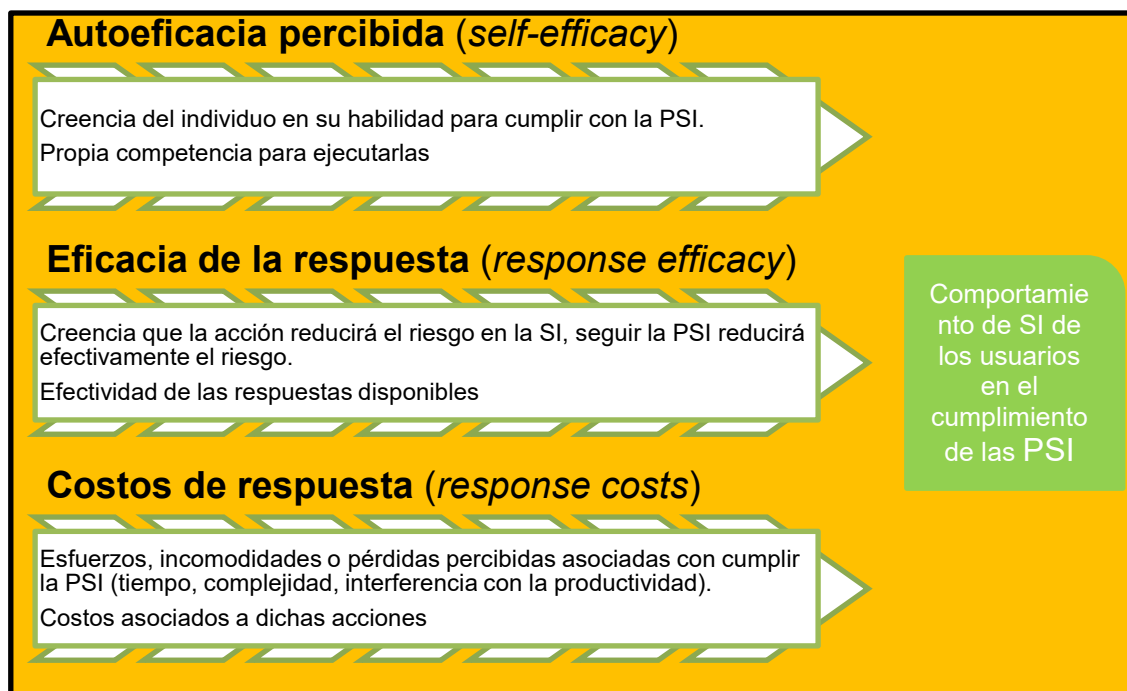
Para los investigadores, el control conductual percibido⁴ se refiere a la percepción de una persona de si pudiera completar con éxito una tarea o comportamiento. Se calcula la dificultad de la tarea frente a las capacidades percibidas.

Tsohou et al. (2015) para influir en el comportamiento de SI de los usuarios en el cumplimiento de las PSI, debemos afectar la forma en que los usuarios perciben los riesgos (evaluación de amenazas) y toman decisiones (Evaluación de afrontamiento) relacionadas con la SI.

La **evaluación de afrontamiento** es el proceso mediante el cual los individuos valoran su capacidad y los recursos disponibles para ejecutar una conducta protectora frente a la amenaza. Formado por tres componentes:

Figura 56

Componentes de la evaluación de afrontamiento



D'Arcy y Teh (2019) en su estudio plantearon que las reacciones emocionales dan lugar a ciertas respuestas de afrontamiento. Considerando dos categorías principales de afrontamiento: afrontamiento centrado en el problema que implica

⁴ Percepción que tiene un individuo de la facilidad o dificultad para realizar un comportamiento específico, que está influenciada por la disponibilidad de los recursos necesarios para llevar a cabo ese comportamiento

esfuerzos directos para manejar o alterar la situación y afrontamiento centrado en la emoción que es el afrontamiento centrado en las emociones de los empleados.

4.3. HIPÓTESIS

4.3.1. HIPÓTESIS GENERAL

La hipótesis general planteada fue “La formulación de un modelo de comportamiento influye en la intención de cumplimiento de las políticas en un Sistema de Gestión de la Seguridad de la información (SGSI) en entidades públicas del estado peruano”.

Las hipótesis específicas se detallan a continuación:

4.3.2. HIPÓTESIS ESPECÍFICA

El intercambio de conocimiento de seguridad de información influye en la actitud positiva de la intención de cumplimiento de las políticas de seguridad de la información.

La colaboración en seguridad de información influye en la actitud positiva de la intención de cumplimiento de las políticas de seguridad de la información.

La intervención en seguridad de información al personal influye en la actitud positiva de la intención de cumplimiento de las políticas de la seguridad de la información.

La experiencia en seguridad de información adecuada influye en la actitud positiva de la intención cumplimiento de las políticas de seguridad de la información.

El apego organizacional influye en la actitud positiva de la intención de cumplimiento de las políticas de seguridad de la información.

El compromiso organizacional influye en la actitud positiva de la intención de cumplimiento de las políticas de seguridad de la información.

Las normas personales (ética) influye en la actitud positiva de la intención cumplimiento de las políticas de seguridad de la información.

Los lineamientos, normatividad y procedimientos de la organización influyen en las normas subjetivas de la intención cumplimiento de las políticas de seguridad de la información.

El hábito influye en la evaluación de amenazas de la intención cumplimiento de las políticas de seguridad de la información.

El hábito influye en la evaluación de afrontamiento de la intención cumplimiento de las políticas de seguridad de la información.

La actitud positiva influye en la intención cumplimiento de las políticas de seguridad de la información.

Las normas subjetivas influyen en la intención cumplimiento de las políticas de seguridad de la información.

La evaluación de amenazas influye en la intención cumplimiento de las políticas de seguridad de la información.

La evaluación de afrontamiento influye en la intención cumplimiento de las políticas.

4.4. IDENTIFICACIÓN DE VARIABLES

4.4.1. VARIABLE INDEPENDIENTE

VARIABLE DE EVALUACIÓN (X)

Modelo de comportamiento en un SGSI (Variable Independiente, causa)

Dimensiones:

Intercambio de conocimiento de SI

Colaboración de SI

Intervención de SI
Experiencia de SI
Apego
Compromiso
Normas Personales (Ética)
Lineamientos, normatividad y procedimientos de la organización
Habito

4.4.2. VARIABLE DEPENDIENTE

VARIABLE DE EVALUACIÓN (Y)

Intención de cumplimiento de políticas en un SGSI (Variable Dependiente, consecuencia)

Dimensión

Actitud
Normas subjetivas
Evaluación de amenazas
Evaluación de afrontamiento

4.5. MATRIZ DE CONSISTENCIA

4.5.1. OPERALIZACIÓN DE LA VARIABLE DEPENDIENTE

Cuadro 1

Intención de cumplimiento de políticas de un SGSI

Variables	Definición conceptual	Definición Operacional	Dimensiones	Indicador	Unidades	Valor Final
VD Intención de cumplimiento de políticas de un SGSI	Se define como la voluntad consciente y deliberada del factor humano para adherirse o aceptar a las políticas, normas y procedimientos de seguridad de información establecidos por la organización. Para Siponen et al. (2014) es un predictor directo del comportamiento de seguridad, determinado por tres dimensiones: actitud hacia las políticas, normas subjetivas y control conductual percibido. Por otro lado, Ifinedo	La Intención de cumplimiento de políticas de un SGSI, está vinculada a la Actitud, Normas subjetivas, Evaluación de amenazas y Evaluación de Afrontamiento que determinan el comportamiento o de cumplimiento efectivo dentro del SGSI.	Actitud	-Considera que las políticas de seguridad mejoran el conocimiento. -Cumplir políticas mitiga riesgos. -Cree que las políticas mejoran la cultura en SI	Escala de Likert: 1,2,3,4,5 1.Totalmente desacuerdo 2. En desacuerdo 3. Neutral 4. De acuerdo 5. Totalmente de acuerdo.	Categórica Ordinal. 1.- cumpliment o deficiente 2.- cumpliment o regular 3.- cumpliment o excelente
			Normas subjetivas	-El comportamiento del Jefe de SI influye en los compañeros. -La cultura de SI influye en los compañeros. - Las costumbres de SI influye en los compañeros.		
			Evaluación de amenazas	-Probabilidad de violaciones de seguridad aumenta si no se considera las políticas. -Reconoce vulnerabilidad ante ataques o		

	(2014), determina la intención de cumplimiento de las Políticas de Seguridad de Información (PSI) refleja la determinación interna del colaborador para comportarse de manera segura.			sanciones. -La pérdida o filtración de información puede ocasionar sanciones legales o económicas importantes.		
			Evaluación de Afrontamiento	-Confía en su capacidad personal para cumplir las políticas. - Percibe que los controles y herramientas institucionales facilitan el cumplimiento. - Considera que las políticas son viables y aplicables.		

4.5.2. OPERALIZACIÓN DE LA VARIABLE INDEPENDIENTE

Cuadro 2

Modelo de Comportamiento

Variables	Definición conceptual	Definición Operacional	Dimensiones	Indicador	Unidades	Valor Final
VI Modelo de Comportamiento	El modelo de comportamiento en un Sistema de gestión de seguridad de la información (SGSI) se basa en el análisis del comportamiento humano y organizacional frente a las políticas y prácticas de seguridad. Según Safa et al. (2015) plantean el modelo de Information Security Conscious Care Behaviour Formation, que integra la TPB y la PMT, y demuestra que la conciencia, las políticas de seguridad y la autoeficacia son determinantes del comportamiento	Modelo evolucionado a partir de marcos conceptuales como la Teoría del Comportamiento Planificado (TPB), la Teoría de la Motivación de Protección (PMT) y la Teoría del Control Social (SBT), compuestas por Intercambio de conocimiento de SI, Colaboración	Intercambio de conocimiento de SI	-Variables identificadas -Índices estadísticos	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Colaboración de SI	-Variables identificadas -Índices estadísticos	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Intervención de SI	-Variables identificadas -Índices estadísticos	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Experiencia en SI	-Variables identificadas -Índices estadísticos	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Apego en SI	-Variables identificadas -Índices estadísticos	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Compromiso en SI	-Índices estadísticos	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Normas Personales	-Variables identificadas	Escala de Likert: 1,2,3,4,5	Categórica Ordinal

	consciente y cuidadoso. Siponen et al. (2014) desarrollan un modelo de adherencia a las políticas de seguridad, centrado en las creencias conductuales, normas subjetivas y control percibido como predictores del cumplimiento. Modelo de cumplimiento PSI Ifinido (2014) amplía el enfoque incorporando el compromiso organizacional y las normas personales, subrayando que la motivación intrínseca y la cultura institucional fortalecen la intención de cumplir las Políticas.	de SI, Intervención de SI, Experiencia en SI, Apego en SI, Compromiso en SI, Normas Personales de SGSI (Etica), Lineamientos, normativas y procedimientos de la organización y Habito	de SGSI (Etica)			
			Lineamientos, normativas y procedimientos de la organización.	-Variables identificadas	Escala de Likert: 1,2,3,4,5	Categórica Ordinal
			Habito	-Variables identificadas	Escala de Likert: 1,2,3,4,5	Categórica Ordinal

CAPÍTULO 5: RESULTADOS Y DISCUSIÓN

5.1. ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

De acuerdo con el desarrollo de la encuesta dirigida a 50 profesionales especializados involucrados en la implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información (SGSI), implantado en los procesos estratégicos, misionales y de apoyo, de las diferentes unidades funcionales dentro de las entidades públicas del estado peruano.

5.1.1. DIMENSIONES PARA EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

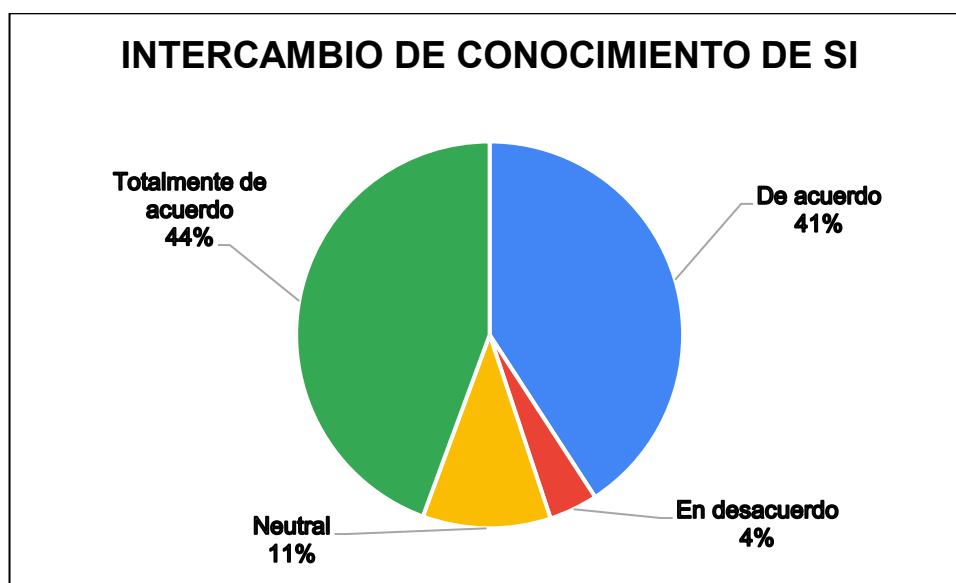
A continuación, se presentan los resultados para cada dimensión:

5.1.1.1. INTERCAMBIO DE CONOCIMIENTO DE SEGURIDAD DE INFORMACIÓN

La figura 57 presenta los resultados del promedio de las respuestas para la dimensión intercambio de conocimiento de SI.

Figura 57

Resultados correspondientes a la dimensión intercambio de conocimiento de SI

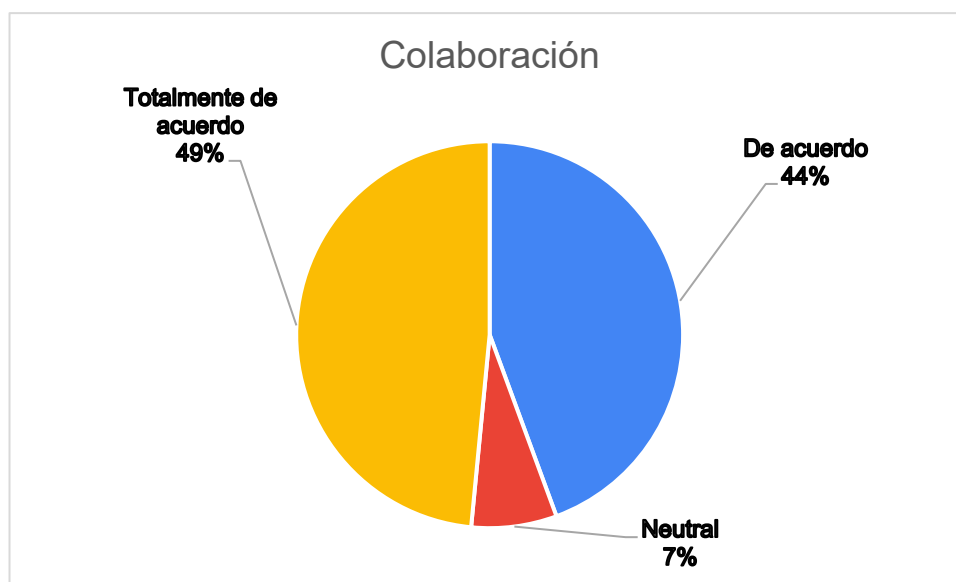


5.1.1.2. COLABORACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La figura 58 presenta los resultados del promedio de las respuestas para la dimensión colaboración en SI.

Figura 58

Resultados correspondientes a la dimensión colaboración en SI

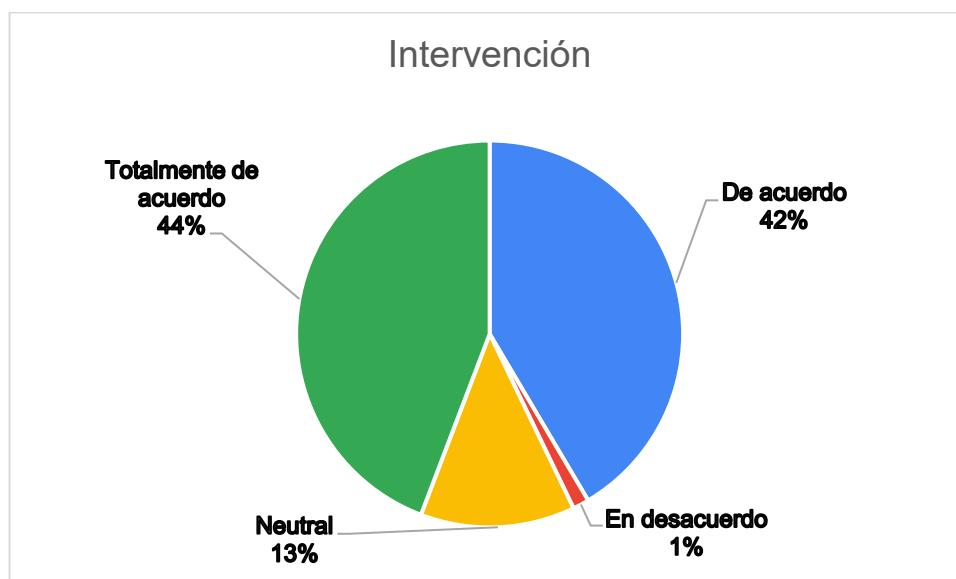


5.1.1.3. INTERVENCIÓN EN SEGURIDAD DE INFORMACIÓN.

La figura 59 presenta los resultados del promedio de las respuestas para la dimensión intervención en SI.

Figura 59

Resultados correspondientes a la dimensión Intervención en SI

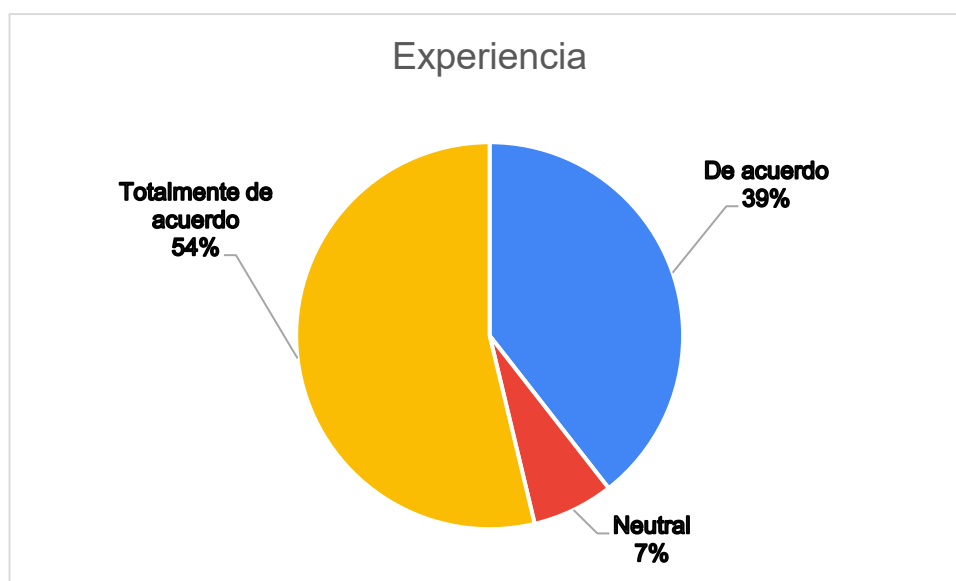


5.1.1.4. EXPERIENCIA EN SEGURIDAD DE INFORMACIÓN.

La figura 60 presenta los resultados del promedio de las respuestas para la dimensión experiencia en SI.

Figura 60

Resultados correspondientes a la dimensión Experiencia en SI

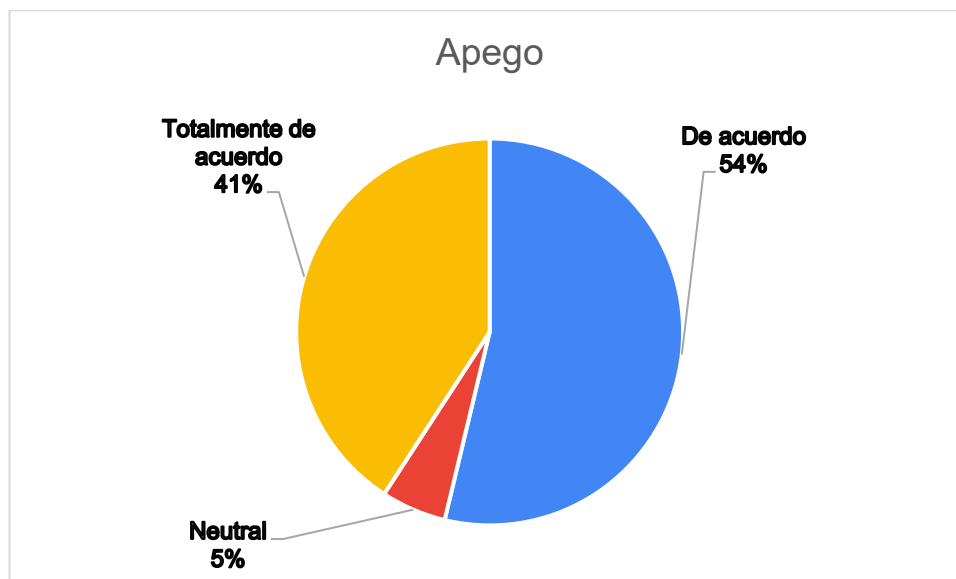


5.1.1.5. AFECTO ORGANIZACIONAL

La figura 61 presenta los resultados del promedio de las respuestas para la dimensión afecto organizacional que influya en la intención de cumplimiento de PSI.

Figura 61

Resultados correspondientes a la dimensión afecto organizacional

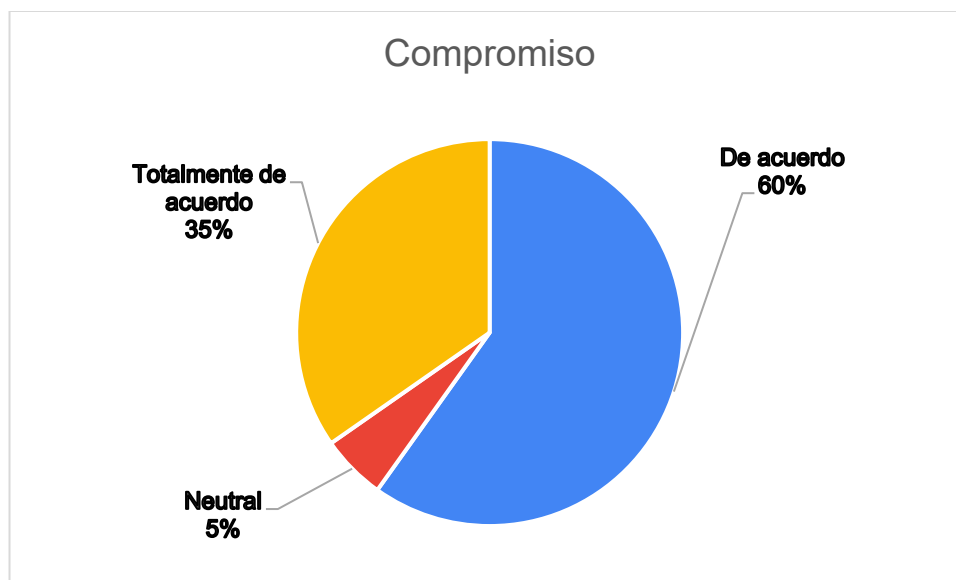


5.1.1.6. COMPROMISO ORGANIZACIONAL.

La figura 62 presenta los resultados del promedio de las respuestas para la dimensión compromiso organizacional que influya en la intención de cumplimiento de PSI.

Figura 62

Resultados correspondientes a la dimensión compromiso organizacional

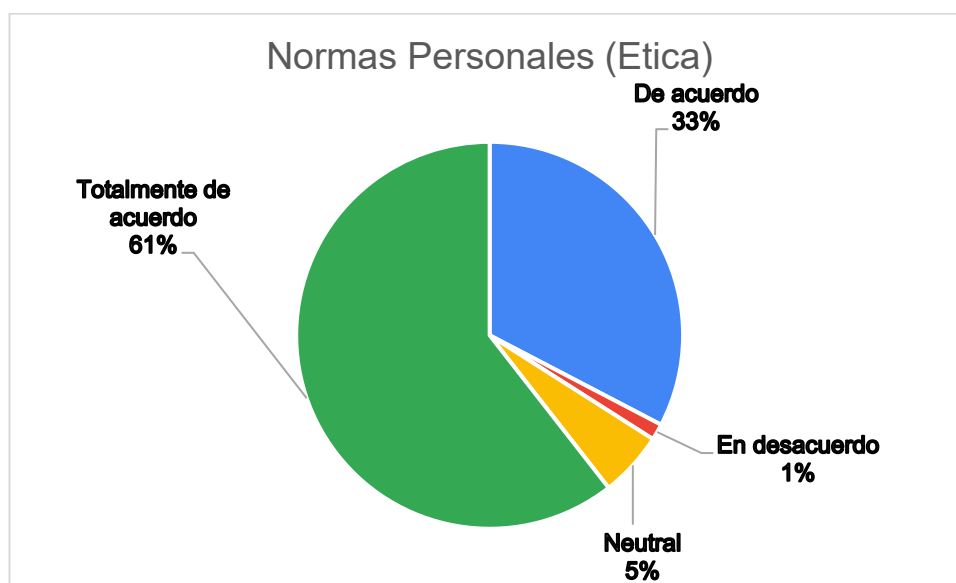


5.1.1.7. NORMAS PERSONALES (ÉTICA).

La figura 63 presenta los resultados del promedio de las respuestas para la dimensión Normas Personales (Ética).

Figura 63

Resultados correspondientes a la dimensión Normas Personales (Ética)



5.1.1.8. LINEAMIENTOS, NORMATIVIDAD Y PROCEDIMIENTOS DE LA ORGANIZACIÓN

La figura 64 presenta los resultados del promedio de las respuestas para la dimensión Lineamientos, Normatividad y procedimientos de la organización.

Figura 64

Resultados correspondientes a la normatividad de la organización.

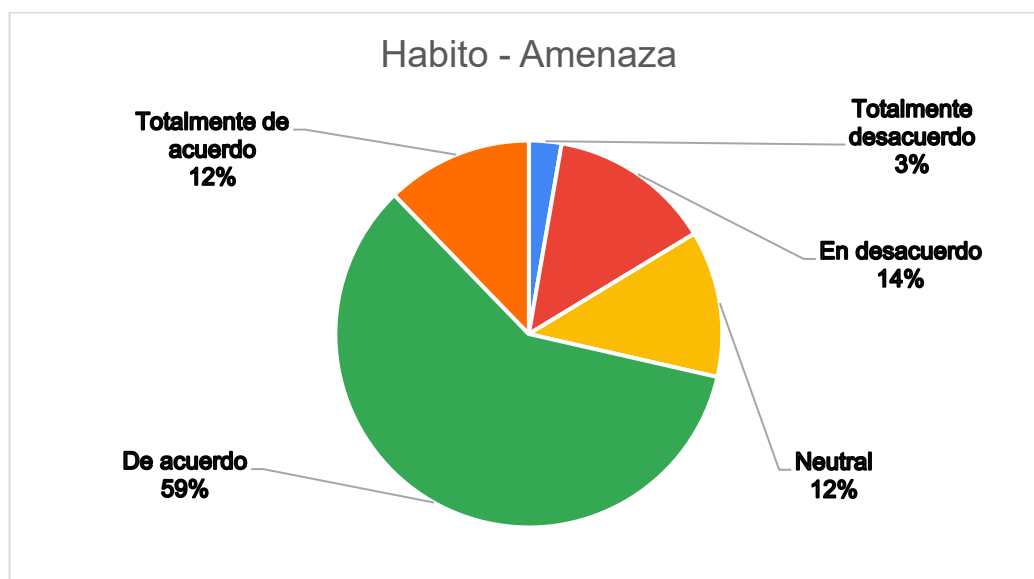


5.1.1.9. HÁBITO EN LA EVALUACIÓN DE AMENAZAS

La figura 65 presenta los resultados del promedio de las respuestas para la dimensión hábito en la evaluación de amenazas.

Figura 65

Resultados correspondientes al hábito en la evaluación de amenazas

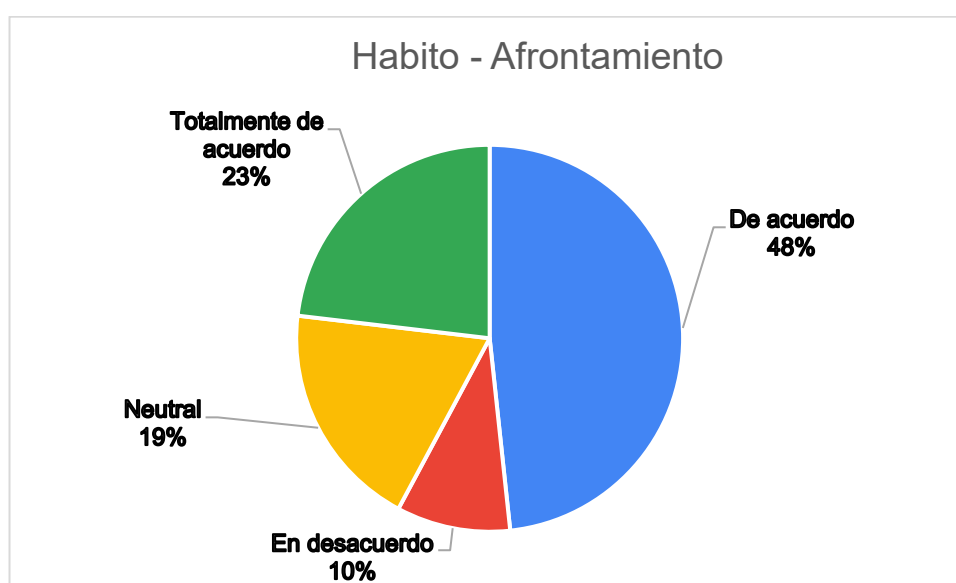


5.1.1.10. HÁBITO EN LA EVALUACIÓN DE AFRONTAMIENTO.

La figura 66 presenta los resultados del promedio de las respuestas para la dimensión hábito en la evaluación de afrontamiento.

Figura 66

Resultados correspondientes al hábito en la evaluación de afrontamiento

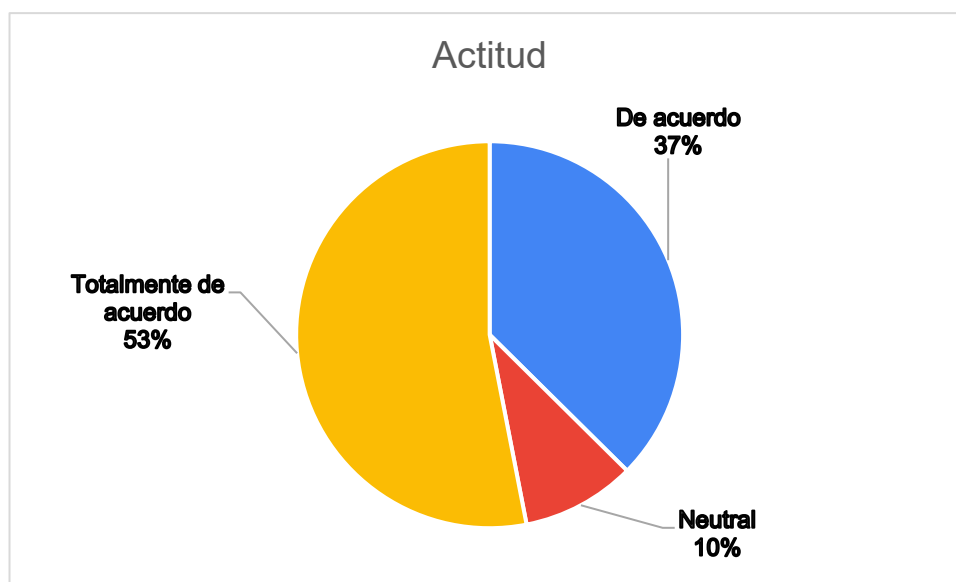


5.1.1.11. ACTITUD.

La figura 67 presenta los resultados del promedio de las respuestas para la dimensión actitud.

Figura 67

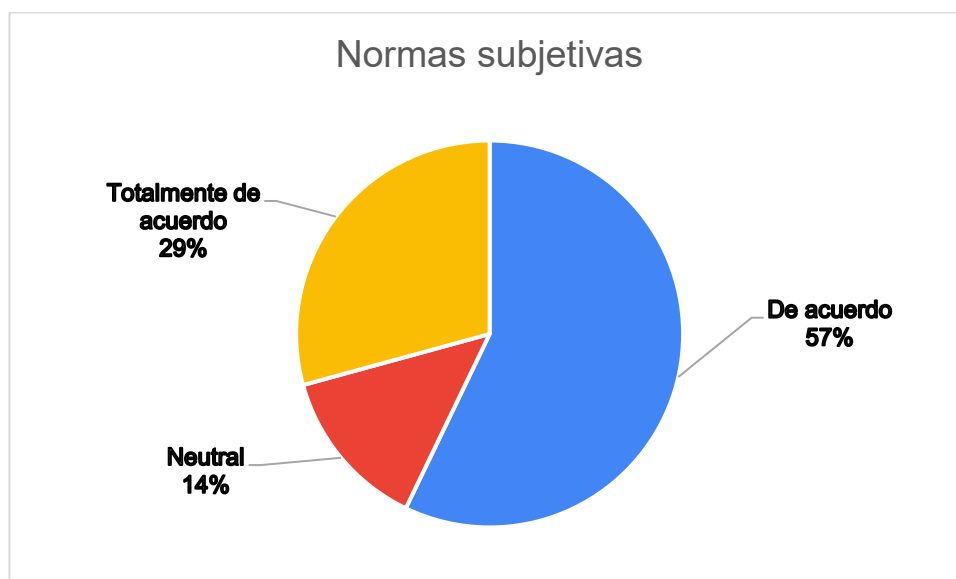
Resultados correspondientes a la actitud



5.1.1.12. NORMAS SUBJETIVAS

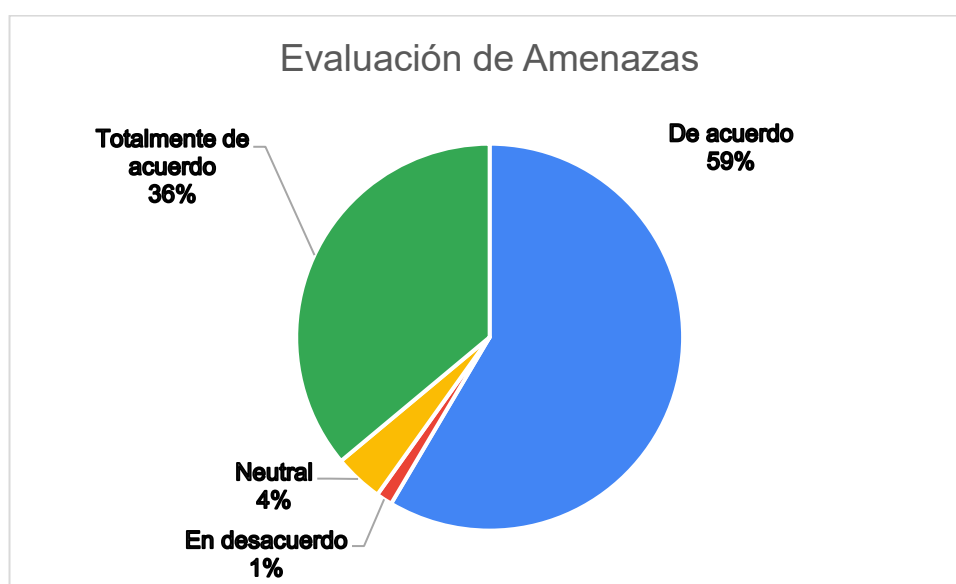
La figura 68 presenta los resultados del promedio de las respuestas para la dimensión normas subjetivas.

Figura 68

Resultados correspondientes a las normas subjetivas**5.1.1.13. EVALUACIÓN DE AMENAZAS**

La figura 69 presenta los resultados del promedio de las respuestas para la dimensión normas evaluación de amenazas.

Figura 69

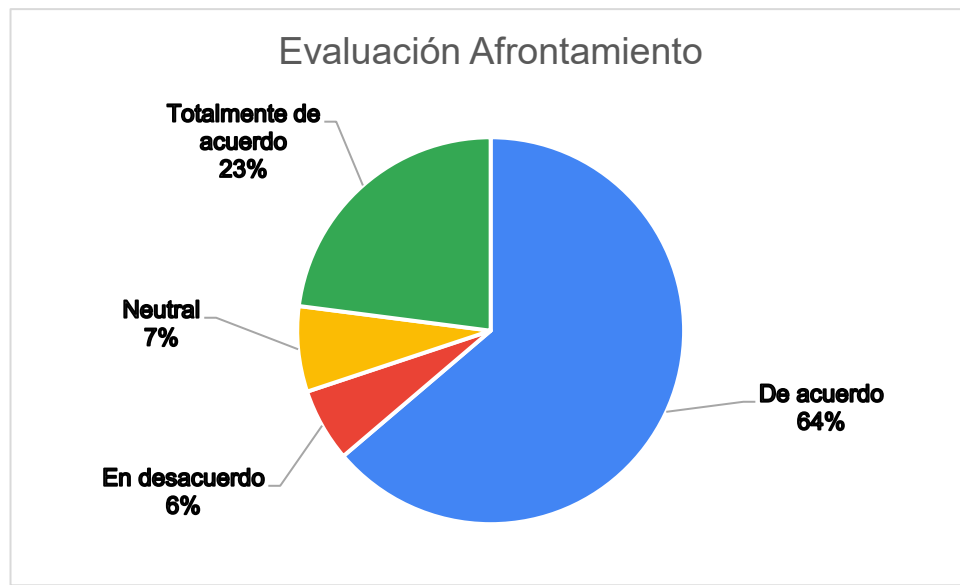
Resultados correspondientes a la evaluación de amenazas

5.1.1.14. EVALUACIÓN DE AFRONTAMIENTO

La figura 70 presenta los resultados del promedio de las respuestas para la dimensión normas evaluación de afrontamiento.

Figura 70

Resultados correspondientes a la evaluación de afrontamiento

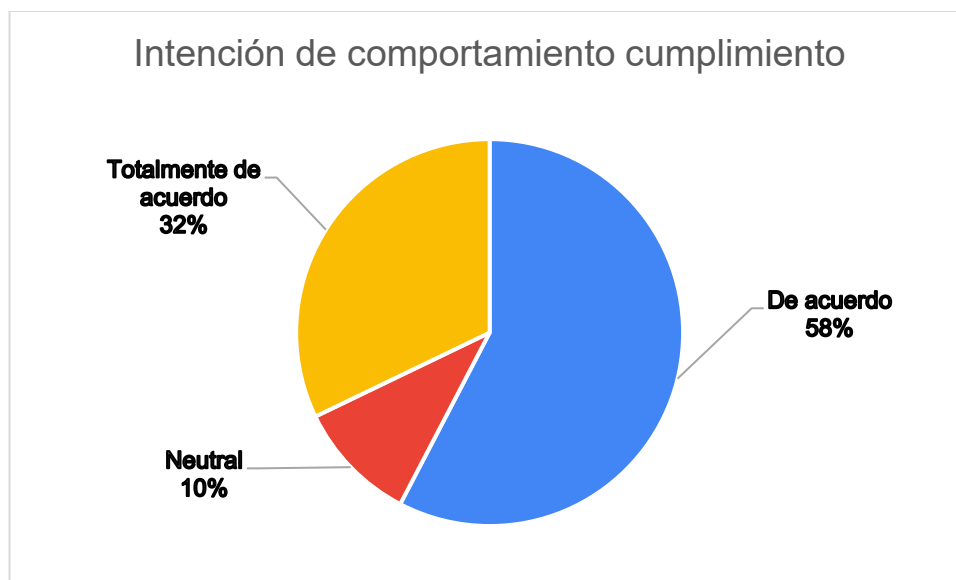


5.1.1.15. INTENCIÓN DE COMPORTAMIENTO DE CUMPLIMIENTO

La figura 71 presenta los resultados del promedio de las respuestas relacionados a la intención de comportamiento para el cumplimiento.

Figura 71

Resultados correspondientes a la intención de comportamiento para el cumplimiento.



5.2. CONTRASTACIÓN DE HIPÓTESIS

Los resultados del cuadro 03, muestran que la variable Modelo de comportamiento, asociada a los factores que influyen en el cumplimiento de las PSI, presenta valores comprendidos entre 97 y 157, con una media de 136.29 y una mediana de 133, lo que evidencia una tendencia hacia niveles altos de percepción positiva respecto a los elementos que estructuran el modelo. La dispersión observada ($DE = 16.38$) y un rango intercuartílico ($RIC = 27$) sugieren una moderada variabilidad entre los participantes, lo que refleja diferencias en la forma en que los empleados interiorizan los elementos del comportamiento organizacional en seguridad de la información. Por su parte, la variable Intención de cumplimiento presenta valores mínimos y máximos entre 42 y 70, con una media de 59.16 y una mediana de 58, lo que sugiere que, en promedio, los participantes manifiestan una elevada disposición a cumplir las políticas de seguridad del SGSI. La baja dispersión ($DE = 6.498$) y el reducido rango intercuartílico ($RIC = 10$) indican mayor homogeneidad en las respuestas, lo cual sugiere que la mayoría de los participantes comparten una actitud consistente y favorable hacia el cumplimiento de las políticas del SGSI. En conjunto, estos resultados permiten inferir que la percepción del

modelo de comportamiento es relativamente amplia y diversa, mientras que la intención de cumplimiento se mantiene más estable y consolidada entre los colaboradores, constituyendo un indicio preliminar de que los factores conductuales pueden contribuir a fortalecer dicha intención dentro de las entidades públicas.

Cuadro 3

Resultados descriptivos

Variables	Mínimo	Máximo	Media	Mediana	Rango	RIC	D.E
Modelo de comportamiento	97	157	136.29	133	63	27	16.38
Intención de Cumplimiento	42	70	59.16	58	28	10	6.498

Los resultados del cuadro 4, muestran que existe una correlación altamente positiva y significativa entre la variable Modelo de comportamiento y la Intención de cumplimiento ($r = 0.917$, $p = 0.001$, $n = 49$), lo cual evidencia que ambas variables mantienen una relación directa muy fuerte dentro de las entidades públicas del estado peruano evaluadas. Este coeficiente $r = 0.917$ indica que a medida que los trabajadores perciben con mayor intensidad los elementos del modelo, también aumenta de manera notable su predisposición y convicción para cumplir las PSI. El nivel de significancia ($p = 0.001$) confirma que esta relación no es producto del azar y posee un respaldo estadístico sólido. En conjunto, el hallazgo sugiere que fortalecer los componentes conductuales dentro de la organización impacta directamente en la intención de cumplir las PSI, consolidando un entorno institucional más seguro y orientado a la protección de la información.

Cuadro 4

Correlación entre variables independiente y dependiente

Variable I	Variable D	r	p	n
Modelo de comportamiento	Intención de cumplimiento	0.917	0.001	49

Resultados por hipótesis

Los resultados del cuadro 5 evidencian una relación altamente significativa entre el modelo de comportamiento en la gestión de la seguridad de la información y la intención de cumplimiento ($r = 0.917$). Los factores vinculados al aprendizaje, la colaboración y la experiencia en seguridad muestran correlaciones fuertes con la actitud de cumplimiento, mientras que las normas subjetivas y la evaluación de afrontamiento destacan como los predictores más influyentes de la intención de comportamiento. En conjunto, los hallazgos confirman que los aspectos conductuales y organizacionales son determinantes para promover el cumplimiento de políticas de seguridad en el sector público

Cuadro 5

Correlación entre dimensiones

Hipótesis	Relación	r	p	Resultado
H1	Intercambio de conocimientos → actitud	0.676	0.000	Significativa
H2	Colaboración → actitud	0.629	0.000	Significativa
H3	Intervención → actitud	0.694	0.000	Significativa
H4	Experiencia → actitud	0.730	0.000	Significativa
H5	Apego organizacional → actitud	0.622	0.000	Significativa
H6	Compromiso organizacional → actitud	0.457	0.001	Significativa
H7	Normas personales (Ética) → actitud	0.751	0.000	Significativa
H8	Lineamientos, normatividad y procedimientos de la organización → normas subjetivas	0.692	0.000	Significativa
H9	Hábito → evaluación de amenazas	0.172	0.238	No significativa
H10	Habito → evaluación de afrontamiento	0.543	0.000	Significativa
H11	Actitud → intención	0.528	0.000	Significativa
H12	Normas subjetivas → intención	0.821	0.000	Significativa
H13	Evaluación de amenazas → Intensión	0.449	0.001	Significativa
H14	Evaluación de afrontamiento → Intensión	0.774	0.000	Significativa

En base a los resultados obtenido en el cuadro 4, donde se evidencia una relación altamente significativa entre el modelo de comportamiento y la intención de cumplimiento ($r = 0.917$). Asimismo, podemos indicar que se puede generalizar los hallazgos del modelo de comportamiento en todas las instituciones públicas del Estado Peruano, porque se sustenta en una base metodológica y conceptual; robusta y contextualizada. Esta solidez radica en la transversalidad de los constructos psicosociales factor humano, derivados de la Teoría del Vínculo Social, Teoría de la Participación, Teoría Del Comportamiento Planificado y la Teoría de la Motivación De Protección, cuya eficacia para predecir la Intención de Comportamiento de Cumplimiento de las PSI es universal, independientemente del tamaño o tipo organizacional. La

fortaleza de la generalización reside en que el modelo se centra en el factor humano y conductual, que es transversal a cualquier organización, más que en la tecnología o la infraestructura específica.

5.3. DISCUSIÓN

En primer lugar, la evidencia empírica del estudio muestra que la actitud, normas subjetivas y la evaluación de afrontamiento son predictores significativamente asociados a la intención de cumplimiento, debido a que la mayoría de los especialistas consideran que la actitud incrementa la convicción del personal de seguir las políticas, las normas subjetivas promueven comportamiento alineados a la SI y la evaluación de afrontamiento que el personal se siente capaz de cumplir. Estos resultados coinciden con los modelos basados en la Teoría de comportamiento planificado (TPB) y la Teoría de motivación de protección (PMT), ampliamente utilizados en investigaciones previas, coincide con lo indicado por Ifinedo (2012), que indica que la actitud, la autoeficacia, la eficacia de la respuesta y las normas sociales explican de forma sustancial la disposición del empleado a cumplir las PSI.

Asimismo, los resultados de este estudio evidencian correlaciones fuertes entre dimensiones como el intercambio de conocimiento de SI, la colaboración en SI, la intervención en SI y la experiencia en SI, con la actitud hacia la intención de cumplimiento, debido a que gran parte de los especialistas consideran que el intercambio de conocimiento es importante en la actitud para seguir y cumplir con las PSI; la colaboración con expertos y los grupos de trabajo necesarios para la actitud para el cumplimiento de PSI; la intervención es fundamental en la actitud mediante los métodos de formación que estén alineados a las PSI; y la experiencia con gran importancia en la actitud creando conocimiento y mejora en las respuestas a los incidentes de SI en el cumplimiento de las PSI. Este patrón coincide plenamente con lo reportado por Safa et al. (2015), quienes demostraron que todas estas dimensiones vinculadas a la participación del empleado en actividades formativas y colaborativas fortalecen la actitud hacia la intención de cumplimiento de PSI y mejoran la disposición conductual de los usuarios frente a la SI.

Por otra parte, se evidencia la importancia del marco normativo interno, considerando los lineamientos, normativas y procedimientos de la organización mostraron un efecto significativo en las normas subjetivas, debido a que los especialistas consideran que la normativa interna claras, difundidas y de cumplimiento obligatorio son importantes para la cultura organizacional, e incrementa el cumplimiento de PSI. Podemos comparar con la investigación de Flores et al. 2014, quien destaca que las estructuras de gobernanza y los procesos de coordinación influye directamente en la disposición de los empleados para adoptar conductas seguras; en otras palabras, cuando las normas son claras, difundidas y respaldadas por la dirección, aumentan las presiones sociales positivas y se refuerza la cultura del cumplimiento. Esto respalda la correlación significativa encontrada entre normatividad interna y normas subjetivas en el presente estudio.

Asimismo, habiendo obtenido un hallazgo donde las normas personales (Ética) presentan una de las correlaciones más elevadas del estudio ($r = 0.751$), debido a que los especialistas consideraron de gran importancia los valores y la ética en la actitud para el cumplimiento de las PSI, teniendo la convicción de hacer lo correcto y la rigurosidad de cumplir cualquier norma. Coincide con (Cheng et al. 2013), sosteniendo que los valores, creencias y vínculos sociales son más determinantes que severidad percibida de las sanciones, señalando que factores como lazos organizacionales, la unión laboral y la presión grupal influyen sustancialmente en la detención de violaciones de SI.

Finalmente, estudios desarrollados en instituciones educativas, como los de Hina et al. 2019, subrayan que la PMT es especialmente eficaz para explicar el comportamiento de cumplimiento en contextos donde los riesgos percibidos son altos y donde la eficacia de las respuestas institucionales se convierte en un determinante crítico. Esto es plenamente coincidente con la correlación considerable entre la evaluación de afrontamiento y la intención de cumplimiento ($r = 0.774$) encontrada en los resultados del estudio, debido a que los especialistas consideran el conocimiento, las habilidades y las capacidades para el cumplimiento de las PSI, además de la efectividad de los controles implementados de SI.

En síntesis, la discusión integrada evidencia que los resultados obtenidos no solo coinciden con estudios previos, sino que aportan robustez empírica al entendimiento de la seguridad desde una perspectiva sociocognitiva. Por lo que el cumplimiento de PSI es un fenómeno multifactorial donde intervienen, de forma articulada, la cultura organizacional, la claridad normativa, los procesos de aprendizaje, las percepciones individuales de riesgo, percepciones individuales de capacidad y los cambios sociales. En este sentido, los resultados no solo validan los modelos teóricos utilizados, sino que refuerzan la necesidad de normatividad que fortalezcan la gobernanza conductual, la comunicación interna, la formación continua y el compromiso institucional en las entidades públicas.

CONCLUSIONES

El factor humano constituye en eje central del cumplimiento de la PSI, sin embargo, las entidades públicas cuentan con lineamientos, directivas, procedimientos, controles técnicos y normativos, los resultados confirman que la intención de cumplimiento depende principalmente de variables cognitivo, conductuales y sociales, tales como la actitud, las normas subjetivas, la autoeficacia percibida y la evaluación de afrontamiento.

Mediante el estudio se comprobó que las normas subjetivas presentan una correlación elevada con la intención de cumplimiento ($r = 0.821$), que indica que la presión del entorno laboral y las expectativas del grupo forman de manera determinante la conducta.

Las dimensiones de intercambio de conocimiento de SI (0.676), la colaboración de SI (0.629), la intervención en SI (0.694) y la experiencia en SI (0.730), mostraron correlaciones fuertes con la actitud. Ello demuestra que el cumplimiento se sostiene mejor en ambientes donde los trabajadores comparten aprendizajes, discuten incidentes, participan en actividades formativas y la experiencia es considerado importante en personal clave de la SI. También la correlación entre la normatividad de la organización y normas subjetivas confirma que los servidores públicos tienden a adoptar comportamientos seguros cuando perciben que la organización posee reglas claras, bien comunicadas y coherentes.

Sin embargo, la relación hábito y la evaluación de amenazas no fue significativa, pero para la relación hábito y evaluación de afrontamiento ($r = 0.543$). Esto significa que para realizar prácticas seguras de manera consistente no necesariamente aumenta el sentido del riesgo, pero si fortalece la confianza en la propia capacidad para responder.

El modelo propuesto presenta alta consistencia teórica y empírica, se verificó una correlación muy fuerte entre el modelo de comportamiento y la intención de cumplimiento ($r = 0.917$), por lo que demuestra que las dimensiones seleccionadas responden coherentemente a los marcos PMT, TPB y SBT.

RECOMENDACIONES

Se recomienda que las entidades públicas del estado peruano orienten el fortalecimiento de sus Sistemas de Gestión de Seguridad de la Información (SGSI) hacia estrategias centradas en el factor humano, complementando los controles técnicos y normativos existentes con intervenciones que incidan en las dimensiones cognitivas, conductuales y sociales del cumplimiento. En particular, resulta prioritario potenciar la actitud positiva hacia el cumplimiento, reforzando las normas subjetivas mediante el liderazgo visible de directivos y jefaturas, la promoción de referentes conductuales y el establecimiento de expectativas claras dentro de los equipos de trabajo, considerando que la presión social y el entorno laboral influyen de manera determinante en la intención de cumplimiento.

Se recomienda institucionalizar mecanismos permanentes de intercambio de conocimiento, colaboración y formación en seguridad de la información, tales como comunidades de práctica, análisis de incidentes reales, talleres participativos y programas de capacitación continua, que permitan consolidar la experiencia del personal clave y fortalecer la confianza en la capacidad de respuesta ante amenazas. Del mismo modo, se sugiere reforzar la claridad, coherencia y difusión de los lineamientos, normativas y procedimientos de seguridad, asegurando su adecuada interiorización y alineación con la cultura organizacional. Finalmente, considerando que los hábitos fortalecen principalmente la evaluación de afrontamiento más que la percepción del riesgo, se recomienda promover la práctica sistemática de comportamientos seguros acompañada de retroalimentación y apoyo organizacional, con el fin de consolidar una intención de cumplimiento sostenible y coherente con los marcos teóricos de la Teoría del Comportamiento Planificado, la Teoría de la Motivación de Protección y la Teoría del Vínculo Social.

REFERENCIAS BIBLIOGRÁFICAS

- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567-575.
<https://doi.org/10.1016/j.chb.2015.03.054>
- Ali, O., Shrestha, A., Chatfield, A., & Murray, P. A. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 37(1), Article 101419. <https://doi.org/10.1016/j.giq.2019.101419>
- Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity*, 4(2), 104-107 <https://doi.org/10.7763/IJSSH.2014.V4.327>
- Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, 129, 103208. <https://doi.org/10.1016/j.cose.2023.103208>
- Alrawhani, E. M., Awanis, R., & Al-Sharafi, M. A. (2024). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(1), Article 100463. <https://doi.org/10.1016/j.joitmc.2024.100463>
- Axelsen, M., Green, P., & Ridley, G. (2017). Explaining the information systems auditor role in the public sector financial audit. *International Journal of Accounting Information Systems*, 24, 15-31.
<https://doi.org/10.1016/j.accinf.2016.12.003>
- Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9-25.
<https://doi.org/10.1016/j.cose.2016.02.007>
- Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & security*, 68, 145-159.
<https://doi.org/10.1016/j.cose.2017.04.009>

- Bürger, J., Strüber, D., Gärtner, S., Ruhroth, T., Jürjens, J., & Schneider, K. (2018). A framework for semi-automated co-evolution of security knowledge and system models. *Journal of Systems and Software*.139,142-160. <https://doi.org/10.1016/j.jss.2018.02.003>
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447-459. <https://doi.org/10.1016/j.cose.2013.09.009>
- Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*. 55(8),1049-1060. <https://doi.org/10.1016/j.im.2018.05.011>
- Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, 55(3), 11-19. <https://doi.org/10.1080/08874417.2015.11645767>
- Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of Employees' Demographic Characteristics on the Awareness and Compliance of Information Security Policy in Organizations. *Telematics and Informatics*.35(6), 1770-1780 <https://doi.org/10.1016/j.tele.2018.05.005>
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applications of social network analysis in behavioural information security research: concepts and empirical analysis. *Computers & Security*, 68, 1-15. <https://doi.org/10.1016/j.cose.2017.03.010>
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67, 196-206. <https://doi.org/10.1016/j.chb.2016.10.025>
- D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 56(7), Article 103151. <https://doi.org/10.1016/j.im.2019.02.006>

- Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, 28, 243-248. [https://doi.org/10.1016/S2212-5671\(15\)01106-5](https://doi.org/10.1016/S2212-5671(15)01106-5)
- Fischer-Preßler, D., Bonaretti, D., & Fischbach, K. (2021). A protection-motivation perspective to explain intention to use and continue to use mobile warning systems. *Business & Information Systems Engineering*, 64(2), 167–182. <https://doi.org/10.1007/s12599-021-00704-0>
- Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110. <https://doi.org/10.1016/j.cose.2014.03.004>
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & security*, 61, 169-183. <https://doi.org/10.1016/j.cose.2016.06.002>
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345–358. <https://doi.org/10.1016/j.cose.2017.11.015>
- Greene, G., & D'Arcy, J. (2010). Assessing the impact of security culture and the employee-organization relationship on IS security compliance. *5th annual symposium on information assurance*. 22(5),
- Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66, 52-65. <https://doi.org/10.1016/j.cose.2016.12.016>
- Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital. *Technological Forecasting and Social Change*, 126, 64-75. <https://doi.org/10.1016/j.techfore.2017.03.023>
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer & security*, 31(1), 83-95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and

- cognition. *Information & Management*, 51(1), 69-79.
<https://doi.org/10.1016/j.im.2013.10.001>
- Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers & Security*, 149, 104204.
<https://doi.org/10.1016/j.cose.2024.104204>
- Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59, 60-70.
<https://doi.org/10.1016/j.cose.2016.02.004>
- Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.
<https://doi.org/10.1016/j.im.2003.08.008>
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32-44. <https://doi.org/10.1016/j.chb.2018.01.028>
- Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, 40, 54-66.
<https://doi.org/10.1016/j.ijinfomgt.2018.01.001>
- Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, 40, 247-257. <https://doi.org/10.1016/j.jisa.2017.11.001>
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.
<https://doi.org/10.1016/j.cose.2015.10.006>
- Safa, N. S., & von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers & Security*, 57, 1-18.
<https://doi.org/10.1016/j.cose.2015.10.002>
- Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management

- (ISRM). *Journal of Information Security and Applications*, 36, 1-10.
<https://doi.org/10.1016/j.jisa.2017.07.004>
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177–191.
<https://doi.org/10.1016/j.cose.2015.01.002>
- Siponen, M., Mahmood, M. A., & Pahnla, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224. <https://doi.org/10.1016/j.im.2013.08.006>
- Skorodumov, B. I., Skorodumova, O. B., & Matronina, L. F. (2015). Research of human factors in information security. *Modern Applied Science*, 9(5), 287. <https://doi.org/10.5539/MAS.V9N5P287>
- Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). *Cyber-information security compliance and violation behaviour in organisations: A systematic review*. *Social Sciences*, 11(9), 386. <https://doi.org/10.3390/socsci11090386>
- Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42-57. <https://doi.org/10.1016/j.cose.2014.05.003>
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, 24(1), 38–58.
<https://doi.org/10.1057/ejis.2013.27>
- Van der Schyff, K., Flowerday, S., & Lowry, P. B. (2020). *Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment*. *Heliyon*, 6(8), e04714.
<https://doi.org/10.1016/j.heliyon.2020.e04714>
- Van Slyke, C., & Bélanger, F. (2020). Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective. *Computers & Security*, 99, Article 102064.
<https://doi.org/10.1016/j.cose.2020.102064>
- Verkijika, S. F. (2018). *Understanding smartphone security behaviors: An extension of protection motivation theory with anticipated regret*.

Computers & Security, **77**, 860–870.

<https://doi.org/10.1016/j.cose.2018.05.008>

Wei, Y. C., Wu, W. C., & Chu, Y. C. (2018). Performance evaluation of the recommendation mechanism of information security risk

identification. *Neurocomputing*. 279, 48-53.

<https://doi.org/10.1016/j.neucom.2017.05.106>

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*. 77, 807-823.

<https://doi.org/10.1016/j.cose.2018.02.001>

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support*

Systems, 92,36-46. <https://doi.org/10.1016/j.dss.2016.09.009>