FACULTAD DE CIENCIAS ADMINISTRATIVAS Y RECURSOS HUMANOS
UNIDAD DE POSGRADO

FACTORES QUE SE RELACIONAN CON EL CUMPLIMIENTO DE LAS PRÁCTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN POR PARTE DE LOS EMPLEADOS EN LAS TRES INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS MÁS GRANDES DE MÉXICO

PRESENTADA POR
AHELÍ DE ALBA GUERRA

ASESOR
PEDRO JUNIOR ARIZA RICALDI

TESIS

PARA OPTAR EL GRADO ACADÉMICO DE DOCTORA EN ADMINISTRACIÓN

LIMA – PERÚ
2023

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y RECURSOS HUMANOS

UNIDAD DE POSGRADO

TESIS

FACTORES QUE SE RELACIONAN CON EL CUMPLIMIENTO DE LAS PRÁCTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN POR PARTE DE LOS EMPLEADOS EN LAS TRES INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS MÁS GRANDES DE MÉXICO

PARA OPTAR

EL GRADO ACADÉMICO DE DOCTORA EN ADMINISTRACIÓN

PRESENTADO POR:

AHELÍ DE ALBA GUERRA

ASESOR:

DR. PEDRO JUNIOR ARIZA RICALDI

LIMA, PERÚ

2023

Hoja de firma de los integrantes del jurado

UNIVERSIDAD DE SAN MARTIN DE PORRES
FACULTAD DE CIENCIAS ADMINISTRATIVAS Y RECURSOS HUMANOS
UNIDAD DE POSGRADO

Comité doctoral de Tesis:

FACTORES QUE SE RELACIONAN CON EL CUMPLIMIENTO DE LAS PRÁCTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN POR PARTE DE LOS EMPLEADOS EN LAS TRES INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS MÁS GRANDES DE MÉXICO

Aprobación de la Tesis:

Dr. Pedro Junior Ariza Ricaldi
Es el director de Tesis
Presidente

Dra. María de Jesús Araiza Vázquez
Secretario

Dra. Zeidy Edith Chunga Liu
Vocal 1

Profesor invitado interno
Vocal 2

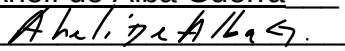
Profesor invitado interno o externo
Vocal 3

Lima, Perú.

Julio, 2023

DECLARACIÓN DE AUTENTICIDAD

Declaro solemnemente que el documento que enseguida presento es fruto de mi propio trabajo, y hasta donde estoy enterado no contiene material previamente publicado o escrito por otra persona, excepto aquellos materiales o ideas que por ser de otras personas les he dado el debido reconocimiento y los he citado debidamente en la bibliografía o referencias.
Declaro además que tampoco contiene material que haya sido aceptado para el otorgamiento de cualquier otro grado o diploma de alguna universidad o institución.

Nombre: Ahelí de Alba Guerra
Firma: 
Fecha: 06 de julio de 3023

ABREVIATURAS y TÉRMINOS TÉCNICOS

IES	Institución de Educación Superior.
SGSI:	Sistema de Gestión de la Seguridad de la Información.
ISO:	International Organization for Standardization.
IEC:	International Electrotechnical Commission.
ISACA	Information Systems Audit and Control Association.
TI	Tecnologías de Información.
IE	Intención del Empleado.
PD	Percepción de la Dirección.
CS	Concientización de la Seguridad de TI.
SF	Sanciones Formales de Disuasión.
SI	Sanciones Informales de Disuasión.
CL	Contexto Laboral.
TCP	Teoría del Comportamiento Planificado.
TAR	Teoría de la Acción Razonada.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo de esta investigación fue medir la relación que tienen la percepción de la participación de la dirección, la concientización de la seguridad de Tecnologías de Información, las sanciones formales de disuasión, así como las sanciones informales de disuasión y el contexto laboral, con el cumplimiento de las prácticas de seguridad de las Tecnologías de Información por parte de los empleados en las tres Instituciones de Educación Superior Públicas más grandes de México. La muestra que se utilizó para el desarrollo del modelo de regresión lineal múltiple consistió en una muestra de 182 participantes de ambos géneros de edades entre 21 y 61 años o más, que trabajan con las TI dentro o fuera de las instalaciones físicas de las Instituciones mandos medios y empleados del área de TI.

Este estudio demostró que existe una relación con el cumplimiento de las prácticas de seguridad de TI de manera moderada, con un valor de 0.406 lo que significa que es una correlación moderada, la concientización de la seguridad de TI tuvo una relación de .361 lo que significa que es una correlación baja, las sanciones formales de disuasión tuvo un valor de .415 lo que significa que es una correlación moderada, el contexto laboral mostró una relación de .755 la cual es una correlación alta, y las sanciones informales de disuasión obtuvieron un valor de .704 lo que significa que es una correlación alta.

Palabras clave: Percepción de la participación de la dirección, concientización de la seguridad de TI, Sanciones formales de disuasión, Sanciones informales de disuasión, contexto laboral.

ABSTRACT

The objective of this research was to measure the relationship of perceived management involvement, IT security awareness, formal deterrence sanctions, as well as informal deterrence sanctions and work context, with employee compliance with IT security practices at the three largest public higher education institutions in Mexico. The sample used for the development of the multiple linear regression model consisted of a sample of 182 participants of both genders aged 21 to 61 years or older, who work with IT inside or outside the physical facilities of the Institutions middle management and IT employees.

This study showed that there is a relationship with IT security practices compliance moderately, with a value of 0.406 which means it is a moderate correlation, IT security awareness had a relationship of .361 which means it is a low correlation, formal deterrence sanctions had a value of .415 which means it is a moderate correlation, work context showed a relationship of .755 which is a high correlation, and informal deterrence sanctions obtained a value of .704 which means it is a high correlation.

Keywords: Perception of management involvement, IT security awareness, Formal deterrence sanctions, Informal deterrence sanctions, work context.

NOMBRE DEL TRABAJO

114. TESIS DOCTORADO - AHELI DE ALBA - ASESOR DR. PEDRO ARIZA.docx

RECUENTO DE PALABRAS

23422 Words

RECUENTO DE CARACTERES

126801 Characters

RECUENTO DE PÁGINAS

94 Pages

TAMAÑO DEL ARCHIVO

736.3KB

FECHA DE ENTREGA

May 18, 2023 7:24 PM GMT-5

FECHA DEL INFORME

May 18, 2023 7:26 PM GMT-5

15% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 13% Base de datos de Internet
- Base de datos de Crossref
- 8% Base de datos de trabajos entregados
- 6% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Bloques de texto excluidos manualmente
- Material citado
- Coincidencia baja (menos de 10 palabras)

USMP UNIVERSIDAD DE SAN MARTÍN DE PORRES | Facultad de Ciencias Administrativas y Recursos Humanos

OFICINA DE GRADOS Y TÍTULOS

CONSTANCIA DE EVALUACIÓN DEL SISTEMA ANTIPLAGIO TURNITIN

FECHA	NOMBRE DEL DOCENTE	CORREO DEL DOCENTE
23/05/2023	DR. PEDRO JUNIOR ARIZA RICALDI	PARIZAR@USMP.PE

NOMBRE DE LA TESIS
FACTORES QUE INCIDEN EN LOS EMPLEADOS EN EL CUMPLIMIENTO DE LAS PRÁCTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LAS TRES INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS MÁS GRANDES DE MÉXICO.

NOMBRE DEL ASESORADO(A)	TELÉFONO Y CORREO	ESCUELA PROFESIONAL
AHELÍ DE ALBA GUERRA	528128248575 aheli.de@gmail.com aheli_dealba@usmp.pe	POSGRADO

RESULTADO:

15% (EXCLUYENDO CITAS Y BIBLIOGRAFÍA)

CONCLUSIÓN:

LA TESIS SE ENCUENTRA APTA PARA CONTINUAR CON EL SIGUIENTE TRÁMITE.

DR. PEDRO JUNIOR ARIZA RICALDI
NOMBRE Y FIRMA DEL ASESOR
DNI: 10698668

23/05/2023. 13:07

AHELÍ DE ALBA GUERRA
NOMBRE Y FIRMA DEL ASESORADO
DNI G16184901.

REVISADO POR: MG. CARLOS ANTONIO ESCUDERO CIPRIANI

INTRODUCCIÓN

La seguridad de la información es el medio para proteger los datos y los sistemas que los gobiernan en cuanto al acceso, uso, divulgación, interrupción, alteración, inspección o destrucción no autorizados (Susanto & Almunawar, 2012). Los ciberdelincuentes diseñan e implementan continuamente amenazas y ataques de seguridad innovadores para explotar las debilidades de las organizaciones no descubiertas aún (Ureña Centeno, 2015). La seguridad de la red en universidades ha sido un tema crítico en la primera década del siglo XXI, así como en la segunda década (González, et al., 2016). El robo de identidad, las violaciones a los datos y los delitos de tipo de exposición de datos han aumentado y están motivados por cuestiones financieras (Ramachandran & Ramanchandran, 2012).

Cada año, los desafíos de seguridad de la información se vuelven más complejos y sofisticados, lo que a su vez aumenta la probabilidad de incidentes y violaciones de los sistemas y recursos de tecnología de la información (TI). Para enfrentar estos desafíos, los gerentes de TI y el personal de seguridad dedican un tiempo significativo a resolver estos problemas. Sin embargo, este enfoque reactivo puede resultar ineficiente y costoso, por lo que cada vez más organizaciones están adoptando un enfoque proactivo en el que se implementan medidas preventivas para mitigar los riesgos de seguridad de la información antes de que ocurran incidentes o violaciones. Esto implica la adopción de políticas y procedimientos de seguridad de la información efectivos, la formación y concienciación de los empleados, la implementación de medidas de seguridad técnicas adecuadas, y el monitoreo y evaluación constantes para mantenerse al día con las amenazas emergentes (Boyle & Panko, 2015; Susanto et al., 2012; Violino, 2014).

Willison & Warkentin (2013), señalaron que la intención premeditada de una violación a la política de seguridad informática o de abuso informático tiene el mayor potencial de ocasionar pérdidas y daños a la organización. Las violaciones a las políticas de acceso a la información privilegiada son un gran

problema de seguridad para las organizaciones. Yupanqui y Oré (2017) afirmaron que las violaciones a las políticas de seguridad en una empresa comúnmente resultan en divulgación no autorizada, el robo de propiedad intelectual y otros abusos. Los gerentes en las organizaciones deben reconocer el rol importante que tienen los empleados en proteger los recursos de información, en lugar de depender y confiar solamente en la tecnología la cual provee protección de seguridad.

Por lo que es importante tomar en cuenta la participación del empleado, para salvaguardar la información a través de conducta de tener la intención de cumplir con las prácticas de seguridad de las tecnologías de información, de tal manera que, en este estudio se pretende demostrar que existe una relación positiva entre la percepción de la participación de la dirección, la concientización, de la seguridad de las tecnologías de información, las sanciones formales e informales de disuasión, más el contexto laboral, los cuales son factores que inciden en dicho comportamiento, y de esta forma buscar mejorar las estrategias de seguridad de las tecnologías de información.

El capítulo 1 presenta los antecedentes del problema y el planteamiento teórico del problema de investigación, seguido del problema central de la investigación, la metodología, seguido de la justificación de la investigación, la delimitación de la investigación y por último la matriz de congruencia.

Capítulo 1. NATURALEZA Y DIMENSIÓN DEL ESTUDIO

Este primer capítulo se desarrolla de la siguiente manera: Comenzando con los antecedentes del problema investigado, se discuten los hechos actuales que contextualizan el problema, seguido de las causas y consecuencias del problema investigado. Entonces el mapa es el concepto. Luego de presentar una descripción del fenómeno investigado, se presenta un abordaje teórico de la pregunta de investigación. Esto incluye los antecedentes teóricos de la variable dependiente del fenómeno, las relaciones que existen entre las variables del modelo y su enfoque teórico. Justificación, seguida de la pregunta central de investigación, objetivos generales, metas metodológicas, luego se mencionan las hipótesis generales, seguida de la metodología, seguida de la justificación del estudio, sus límites y finalmente la matriz de congruencia.

1.1. Antecedentes del Problema para investigar

Sabemos que las tecnologías de la información y comunicación han venido creciendo de una manera acelerada de tal manera que han tenido un impacto muy fuerte en las organizaciones tanto positiva como negativamente, por lo que la información se ha convertido en uno de los insumos más importantes que poseen, esto las ha llevado a adquirir diferentes sistemas de información y herramientas para facilitar el uso y procesamiento de los datos con el fin de generar reportes, informes, estadísticas, las cuales sirven para la toma de decisiones, para desempeñar y cumplir con las estrategias implementadas por cada compañía, mismas que buscan una forma de proteger la información.

Muchas de las compañías se hallan en proceso de consumación y adopción de lineamientos de seguridad de la información, normalmente por medio de capacidades de seguridad de la información, las cuales para que se cumplan o se lleven a cabo se necesita de una cultura, así como de una sensibilización por parte de todos los integrantes acerca de la seguridad de la información, ya que ninguna empresa está exenta de sufrir ataques en sus sistemas de información, los cuales están expuestos a un número cada vez más elevado de amenazas de distinta índole, llámese virus informáticos, *ransomware* (secuestro de datos), *phishing* (substitución de identificación de tercero de confianza), por mencionar

algunos. De la misma manera, hay que tomar en cuenta los eventos negativos que se pueden presentar, ante el peligro que representa la falta de seguridad causada de manera voluntaria e involuntariamente desde el interior de la organización, provocados por desastres naturales, fallas técnicas o humanas. Los Sistemas de Gestión de Seguridad de la Información salvaguardan los activos de información, sin distinguir el medio en el que se encuentren almacenados (Avila, 2016).

La información como activo está cobrando gran relevancia en las empresas que entienden que debe ser asegurada y protegida sin importar el medio en el que resida (digital o físico), y esto es fácil y uno al mismo tiempo. Tareas que requieren recursos, tiempo y compromiso.

La información es uno de los cimientos fundamentales de cualquier empresa, sin importar su tamaño o ubicación geográfica. Aunque esta realidad no es nueva, es en los últimos años que se ha tomado mayor conciencia sobre la importancia de la información, lo que ha llevado al surgimiento de diversas metodologías que permiten a las empresas optimizar sus procesos de seguridad de la información. A medida que la tecnología avanza, también lo hacen las amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de la información. Si una empresa no está adecuadamente preparada para proteger su información, puede poner en riesgo el cumplimiento de sus objetivos de negocio, especialmente en términos estratégicos, legales, operativos, económicos o de reputación (Garcés & Moreno, 2019).

La seguridad de la información se refiere a un conjunto de medidas y estrategias implementadas para proteger la información y los sistemas de información de posibles riesgos y amenazas. El objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, evitando su acceso, divulgación o modificación no autorizada. En este sentido, la seguridad de la información es fundamental para garantizar el cumplimiento de los objetivos de negocio, ya que una brecha de seguridad puede tener consecuencias graves en diferentes niveles, desde la estrategia, operaciones, reputación y económico. Con el avance tecnológico, es importante que las empresas implementen

medidas adecuadas para proteger su información y sistemas de información (Susanto & Almunawar, 2012).

Los ciberdelincuentes diseñan e implementan continuamente amenazas y ataques de seguridad innovadores para explotar las debilidades que las organizaciones no han descubierto aún (Ureña Centeno, 2015). La seguridad de la red en universidades ha sido un tema crítico en la primera década del siglo XXI, así como en la segunda década (González et al., 2016). El robo de identidad, las violaciones de datos y los delitos de tipo de exposición de datos, han aumentado y están motivados por cuestiones financieras (Ramachandran & Ramanchandran, 2012).

Cordovilla et al. (2020) comentan que las amenazas y los abusos en la seguridad informática y de la información están motivando a la administración de TI en las organizaciones a aclimatarse a un programa de seguridad más comprensivo y completo. Durante los años 2005 a 2009, se informaron 549 incidentes de violación de datos en instituciones educativas que exhiben en promedio 10.4 millones de registros (Collins, 2011). La gestión de la seguridad de la tecnología de información abarca una combinación de expectativas, procesos de descubrimiento y procesos de tipo de reacción, junto con una cadena de acciones que requieren actividades de monitoreo y control continuas para disminuir la posibilidad de ataques a la seguridad de la información (Issa-Salwe & Ahmed, 2011).

Estas afectaciones se manifiestan como lo señala Farfán, Franco, Gachuz, Hernández, & Lozano (2018), en un artículo, sobre el número de ciberataques en México en 2013, que fue de 100 mil empresas medianas. Por lo que en todo el país las pérdidas provocadas por los ciberdelincuentes ascendieron a $39,000 millones de pesos aproximadamente.

Otro estudio reciente encontró que México fue el país más afectado por ciberataques, ocupando el primer lugar en el cosmos en 2018. El 82 % de las compañías habían sido objeto de un ataque como mínimo en contra sus

sistemas, seguido de Francia con un 79 % y la India con el 76% en contraste con Japón quien obtuvo solo el 24%, siendo los principales riesgos a los que se enfrentan las empresas que son víctimas de un ciberataque, la pérdida de los datos, daños a la imagen de la empresa, la pérdida de tiempo y dinero, por lo que es de suma importancia proteger los activos de información a toda costa (Arellano, 2020).

De acuerdo con firmas de ciberseguridad, la mayoría de los ataques más destacados afectan a compañías que oscilan entre los 100 y 5,000 trabajadores en México, se ha demostrado que un 32% se ha enlazado a los sistemas a través de uniones maliciosas invadiendo por Internet; el 31% vía correo electrónico *phishing* (suplantación de identidad). Uno de cada cuatro asaltos se realizó por medio de memorias USB y dispositivos externos, mientras que el 12% de los ataques fue por vulnerabilidades en el software. También es sabido que los administradores no se han enterado ni cómo ni cuánto tiempo estuvo presente el ataque en su organización (Arellano, 2020).

Gerente general de Sophos México cita pérdida de datos, daño a la reputación, pérdida de tiempo y dinero como otros riesgos que enfrentan las empresas mexicanas que son víctimas de ciberataques, por lo que invertir $2.5 millones de pesos en sistemas de ataque dijo que es necesario (Arellano, 2020). También se marcó que los tipos de empresas con ciberataques más frecuentes a nivel universal fueron las de tecnologías de la información y comunicaciones (TIC) con el 15.9%; empresas de comercio que se caracteriza por vender al por menor, distribución y transporte del 13%; manufactura 13.7% y 11.6% de empresas prestadoras de servicios financieros. Ante este escenario se hace evidente que la seguridad de la información en las empresas ha dejado de ser un lujo para convertirse en una necesidad.

1.1.1. *Hechos actuales que contextualizan el problema*

En una organización, las tecnologías de información (TI) se componen de los sistemas de información, sus usuarios y la gerencia que las administra (Turban et al., 2013). También, señala que la infraestructura de las TI está compuesta, no solo de equipos, programas y bases de datos, sino también del

personal de TI y las redes de comunicación; incluyendo Internet e Intranet; las empresas dependen de los recursos de TI para lograr o alcanzar lo propuesto en sus metas y objetivos a corto y largo plazo. Asimismo, la evolución de los negocios está directamente relacionada con la calidad de la información. De la misma manera, definieron las características clave de la información de alta calidad como, pertinente, oportuna, confiable, precisa, fácil de entender y de utilizar.

En este mismo contexto, se comenta que el objetivo principal de la gerencia de TI es desarrollar e implementar un plan bien estructurado para administrar los sistemas de información e infraestructura de TI. Este plan incluye la formulación de políticas y prácticas, tales como: guías, estándares y procedimientos, para apoyar las necesidades de información, y la toma de decisiones en la empresa, de una manera efectiva y eficiente.

Según Luftman et al. (2012) el propósito principal de las políticas de seguridad de TI es brindar protección a los recursos de sistema de información y asistir a los usuarios de los sistemas de información y demás recursos de TI, en el uso seguro de los mismos. Boyle y Panko, (2015) explican que las políticas de seguridad de TI describen los roles y responsabilidades de los empleados, puntualizan en problemas de seguridad y en la importancia de proteger la información y los recursos de TI en la organización. También señalan que las políticas son declaraciones de lo que debe hacerse bajo determinadas circunstancias.

La Organización Internacional de Estandarización (ISO) lleva a cabo anualmente una encuesta que tiene como objetivo conocer el desarrollo de los sistemas de gestión ISO a nivel global. Los resultados obtenidos en dicha encuesta muestran un aumento constante en el número de certificaciones emitidas en ISO 27001. En el último año (2019), se estima que el número de certificados ha aumentado en un 45% en comparación con el año anterior (2018). Asimismo, en Sudamérica, la certificación en ISO 27001 ha experimentado un crecimiento progresivo, pasando de tan solo 18 certificados en el año 2006 a 117 en 2010 y a 564 en el año 2016, lo que representa un incremento del 1,7% en

una década. Este aumento en el número de certificaciones en ISO 27001 sugiere un mayor interés por parte de las organizaciones en la seguridad de la información y la adopción de un enfoque basado en la gestión de riesgos para proteger su información crítica.

En cuanto al top de los principales 10 países que más certificaciones tienen en ISO 27001 como se observa en la tabla 1. Japón es el primer país con más certificados con un total de 8.945, seguido del Reino Unido con 3,367, así como podemos observar el contraste que existe con los Países Bajos y España los cuales no llegan ni a 1,000 certificados.

Tabla 1. Los principales 10 países que más certificaciones tienen en ISO 27001.

Países	**Certificados**
Japón	8,945
Reino Unido	3,367
India	2,902
China	2,618
Alemania	1,338
Italia	1,220
Estados Unidos	1,115
Taipei	1,087
España	752
Países Bajos	670

Nota: Esta tabla muestra los países con más certificaciones ISO 27000 en el mundo.

En cuanto los países sudamericanos, los más representativos en cuanto a número de certificaciones obtenidas, se muestran en la tabla 2. Cabe destacar que México tiene el primer lugar obteniendo 221 certificaciones seguido de Colombia con 163, así como se puede observar el contraste tan marcado con los países como Chile, Perú, Costa Rica y Ecuador los cuales cuentan con menos de 50 certificados cada uno (ISO, *Tools Excellence* 2017).

Tabla 2. Países de Sudamérica con certificaciones en ISO 27001

Países	Certificados
México	221
Colombia	163
Brasil	117
Argentina	88
Chile	49
Perú	32
Costa Rica	21
Ecuador	11

1.1.2. *Causas y Consecuencias del problema a investigar*

Los problemas de la seguridad de la información y la seguridad informática afectan a todas las organizaciones de todos tamaños y giros incluyendo el educativo, una de las razones se debe a que todas manejan grandes cantidades de información, ya sea financiera o académica, lo que se torna un claro de posibles embestidas. Por lo que la seguridad informática está relacionada con las técnicas, metodologías, rutinas, que ayudan a resguardar los datos, estos métodos parten siendo estructurados con el uso de normas, protocolos, buenas prácticas, estándares que sirven para mermar los riesgos en una infraestructura tecnológica. Por otra parte, la seguridad de la información se fundamenta en tres pilares de la seguridad los cuales son: la confidencialidad, la integridad y la disponibilidad de la información (Imbaquingo et al., 2019).

Morales et al. (2019), comentan, que las IES públicas pueden provocar problemas por falta de medidas de ciberseguridad ya que con el transcurso del tiempo estas instituciones van creciendo en todos los sentidos incluyendo la información, los procesos, los servicios, y de igual forma aumenta la probabilidad de ser un objetivo de ataques informáticos y mayor será el impacto del riesgo. Por ejemplo, ellos señalan que uno de los ataques que frecuentemente es utilizado es el de fuerza bruta, el cual consiste en utilizar diccionarios que generan datos de manera aleatoria para probar contraseñas de acceso a calificaciones, información personal, bancaria, entre otras. Por lo que señalan que no existen investigaciones sobre el tema de ciberseguridad aplicadas a las IES en el país de Ecuador.

Con el avance constante de la tecnología, también han surgido amenazas cada vez más sofisticadas que pueden poner en peligro la seguridad de la información. Si una empresa no se prepara adecuadamente para proteger sus datos, corre el riesgo de comprometer la consecución de sus objetivos de negocio. Las posibles afectaciones pueden ser de diversa índole, como a nivel estratégico, legal, operacional, económico o de reputación. La implementación de estándares y marcos de referencia de seguridad es una forma efectiva de garantizar que las empresas estén protegiendo adecuadamente su información y cumpliendo con las regulaciones aplicables (Garcés & Moreno, 2019).

Según Luftman y Ben-Zvi (2011) la ampliación en la implementación de las tecnologías de información también ha traído preocupaciones entre los gerentes de TI. En el tercer trimestre del 2011, llevaron a cabo una encuesta a ejecutivos de TI, los investigadores revelaron que las principales preocupaciones de los ejecutivos de TI son: la alineación de TI al negocio, agilidad del negocio, reingeniería de procesos de negocio, la productividad empresarial, reducción de costos, y la planificación estratégica de TI, los gerentes que participaron en el estudio representaban 275 organizaciones miembros del *Society for Information Management* (SIM) con sede en Estados Unidos.

Desde el 1980, Luftman y Ben-Zvi (2011) han realizado varios estudios donde encuestaron a gerentes de TI en Estados Unidos e identificaron cuatro preocupaciones que han permanecido constantes en cada uno de los estudios realizados: la alineación de TI al negocio, reingeniería de procesos de negocio, la planificación estratégica de TI y la seguridad y la privacidad. Otro estudio que realizaron se llevó a cabo a nivel internacional en el verano de 2011; donde se aplicó una encuesta a los ejecutivos senior de TI ubicados en las regiones de Europa, Asia (incluyendo Australia), América Latina y Estados Unidos donde se obtuvieron respuestas de más de 600 ejecutivos de TI, lo que representó más de 620 organizaciones.

Luftman et al. (2012) descubrió que la seguridad y la intimidad estuvo entre las iniciales 10 intranquilidades de los gerentes de TI. Estos resultados

fueron similares a los estudios realizados en Estados Unidos. Además, encontraron que la seguridad y la privacidad obtuvieron el séptimo lugar entre las 10 preocupaciones de la gerencia de TI, tanto en Latinoamérica como a nivel mundial. Posteriormente, en 2013 y 2014, ellos realizaron estudios similares en Estados Unidos y Europa, con otros investigadores, permaneciendo la seguridad entre las primeras 10 preocupaciones de los gerentes de TI (Kappelman et al., 2013; Luftman & Derksen, 2014).

Los desafíos de Seguridad de la Información, los sucesos y las trasgresiones de validación a los sistemas y rentas de TI se han incrementado con frecuencia, provocando que los gerentes de TI y sus subordinados inviertan grandes cantidades de esfuerzo en controlar estas dificultades (Boyle & Panko, 2015; Susanto et al., 2012). Para garantizar que toda la información esté segura, es recomendable e indispensable el cumplimiento de las políticas, normas y procedimientos de seguridad de la información en las empresas (Boyle & Panko, 2015). Por otra parte, esta problemática es un elemento muy significativo de los activos intangibles de una empresa. (Susanto et al., 2012).

Los problemas de seguridad pueden ser causados por personas externas a la organización o por los empleados de esta. Las amenazas internas a los empleados son la preocupación número uno para las organizaciones porque hay muchas formas en que un empleado puede cometer un acto o actividad maliciosa. Los empleados pueden ser capaces de pasar por alto la seguridad física, por ejemplo, las puertas cerradas, y la seguridad técnica, así como las contraseñas. Sin embargo, estas medidas son impuestas por las organizaciones como mecanismos de protección para evitar el acceso a personas no autorizadas (Boyle & Panko, 2015). Turban et al. (2013) señalan que las defensas en la tecnología, tales como *firewalls*, sistemas de detección de intrusos y seguridad física en las puertas de acceso, son implementadas para proteger la información de las amenazas externas.

Los empleados de una empresa pueden ser estimados como la parte más débil en la gestión de la seguridad de los sistemas de información debido a su

falta de conciencia y capacitación en seguridad de la información (Boyle & Panko, 2015; Bulguru et al., 2010; D'Arcy & Devaraj, 2012; Guo et al., 2011; Hu et al., 2012). Boyle & Panko, (2015) concluyeron que esta situación se debe a que los empleados poseen conocimiento extenso y detallado de los sistemas, tienen credenciales que les dan acceso a información, conocen los mecanismos de control corporativo y gozan de la confianza de los usuarios y de la gerencia de la organización.

Willison & Warkentin, (2013), señalaron que la intención premeditada de un quebrantamiento al manejo de seguridad informática o de abuso informático tiene el mayor potencial de ocasionar pérdidas y daños a la organización. Las infracciones de las políticas de acceso a la información privilegiada son un gran problema de seguridad para las organizaciones; así como las trasgresiones a las políticas de seguridad en una empresa comúnmente resultan en divulgación no autorizada, el robo de propiedad intelectual y otros abusos. Los gerentes en las organizaciones deben reconocer el rol tan importante que tienen los empleados en proteger los recursos de información, en lugar de depender y confiar solamente en la tecnología la cual provee protección de seguridad.

Según Posey et al., (2013) y Turban et al., (2013) afirman que, si las organizaciones quieren tener éxito, sobrevivir y mantenerse ante los constantes cambios que están ocurriendo globalmente, tienen que actuar de forma rápida y proactiva en atender los problemas de seguridad ocasionados por sus empleados. La alta gerencia debe darles participación a los empleados en el plan de seguridad, con el fin de fomentar el compromiso con el cumplimiento de las políticas y prácticas de seguridad de las TI en sus organizaciones. Estas son un problema que repercute en costos sustanciales para las organizaciones (Vance et al., 2015).

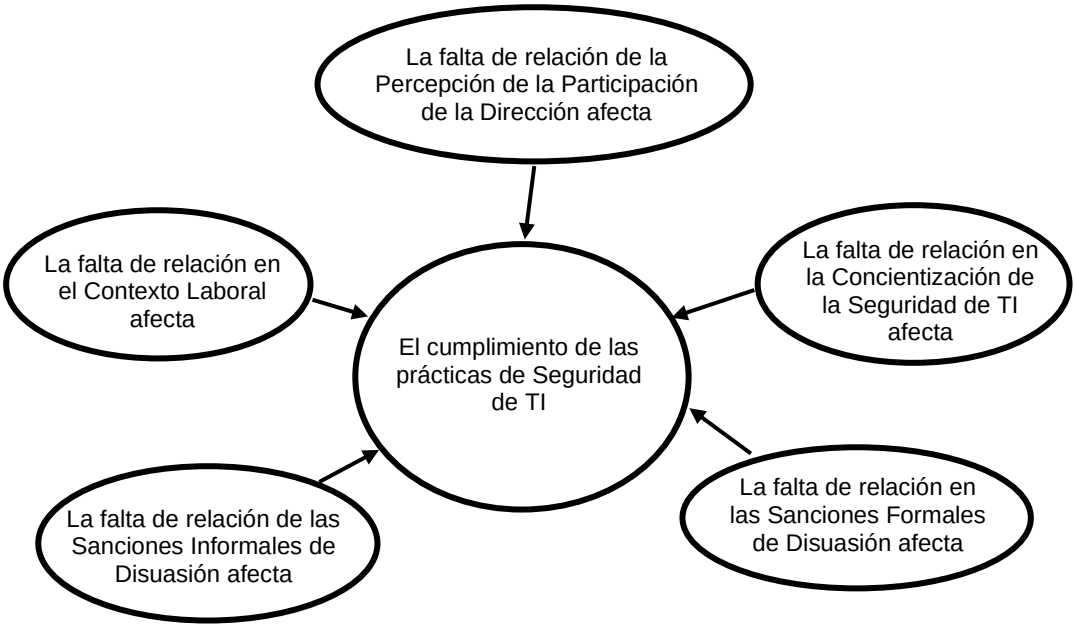
Los programas de adiestramiento y las sanciones se han utilizado como mecanismos para reducir las violaciones de las políticas de seguridad, sin embargo, este problema persiste y es necesario identificar alternativas para reducir las violaciones a las políticas de acceso, sobre todo para los sistemas

que proporcionan un amplio acceso a los datos de la empresa. (Vance et al., 2015).

1.1.3. *Mapa conceptual del Problema a investigar*

La Figura 1 muestra la problemática a analizar a través del mapa conceptual que describe el problema de estudio.

Figura 1. Mapa Conceptual del Problema Bajo Estudio.



Fuente: Elaboración propia

1.2. Planteamiento Teórico del Problema de Investigación

Concurre una disputa fuerte sobre el resguardo de la data en las organizaciones. Por lo que les ha hecho falta contar con un sistema de gestión que asegure la misma, o por lo menos contenga controles, políticas, medidas, procedimientos de seguridad obligatorios encaminados a asegurar sus activos, tales como: documentos, *software*, *hardware*, entre otros. Si bien es cierto las empresas de alguna forma mantienen algún tipo de vigilancia de su información, en ocasiones esto no es garantía para conservar seguro este activo tan importante para las compañías (Flores & Herrera, 2018).

Así mismo, sabemos que las universidades recaban grandes cantidades de información personal, de mayor confidencialidad que las del ámbito corporativo, por mencionar algunos ejemplos, están las bases de datos con información personal e historial clínico de los estudiantes y la planta docente, bases de datos financieras, documentación de títulos de pregrado y posgrado, registro de las calificaciones de los alumnos, por mencionar algunos.

Las organizaciones centran sus preocupaciones sobre la seguridad de la información más en los aspectos técnicos de la seguridad, pero existe la necesidad de ofrecer a las universidades tácticas de gestión de la seguridad de la información que incluyan el progreso, la exploración y el acatamiento de las reglas de seguridad, además de emprender cuestiones de seguridad importantes, como la concientización, formación, confidencialidad, tipificación de trances críticos. Para una gestión eficaz de este proceso es necesario que todos los integrantes de la universidad como empleados, estudiantes, autoridades, docentes sean conscientes de la importancia de la seguridad de la información y el aporte a la calidad y eficiencia de los procesos críticos en las universidades (Rayme, 2007).

Los costos asociados con las violaciones de datos aumentaron y continúa motivando a los departamentos de TI a implementar nuevas medidas de seguridad de protección de la información (Hoadley et al., 2012). Para Ayyagari y Tyks, (2012) es importante concientizar sobre los problemas de seguridad de la información que enfrentan las instituciones académicas, porque la mayoría de las infracciones reportadas en 2011 se han producido en un ámbito educativo. La mayoría de las violaciones de datos desde 2005 se han producido en entornos educativos, por lo tanto, la seguridad de la información es una de las preocupaciones principales para las IES, ya que los ataques de los *hackers* son dirigidos a instituciones de educación en todos los niveles para robar recursos informáticos, propiedad intelectual y datos sensibles.

Los investigadores Fisher y Shorter, (2013), Guo et al., (2011), Furnell et al., (2010) han encontrado que la seguridad de TI es una preocupación importante

para las organizaciones, pero muy pocas se han centrado en las necesidades específicas de una escuela o universidad, y debido al aumento de TI las violaciones de seguridad en entornos educativos también ha ido en aumento, por lo que han recomendado que se debe explorar con mayor profundidad el tema, para mejorar la seguridad de TI de las escuelas y universidades.

Por otro lado, si los trabajadores no consuman las políticas de seguridad de TI, las instituciones no pueden resguardar la información y responder sobe su confidencialidad, totalidad y su reserva. Para que la gerencia de TI pueda garantizar la seguridad de la información, es recomendable e indispensable que los empleados cumplan con las políticas, normas y procedimientos de seguridad de la información de las IES, con el fin de brindar amparo a los recursos de sistema de información (Boyle & Panko, 2015).

1.2.1. *Antecedentes Teóricos del fenómeno a investigar (cumplimiento de las prácticas de seguridad de TI):*

El propósito de los encargados en consumar las prácticas de seguridad de TI – Se refiere al propósito que los trabajadores tienen de realizar sus tareas con las reglas de seguridad de TI. (Bulguru et al., 2010; D'Arcy & Devaraj, 2012; Hu et al., 2012). Muchos estudios han investigado el impacto de creencias justificativas y autoeficacia en las actitudes de los involucrados en el cumplimiento de las aplicaciones de seguridad de TI en las instituciones (Chen et al., 2012; D'Arcy & Devaraj, 2012; D'Arcy et al., 2014; Hu et al., 2012; Johnston et al., 2015; Vance et al., 2015; Willison & Warketin, 2013).

La teoría de la acción razonada es ampliamente utilizada para predecir el comportamiento humano combinada con la influencia de las normas sociales, puede determinar su intención real de cumplir con dichas políticas. Por lo tanto, es importante para las organizaciones no solo establecer políticas de seguridad efectivas, sino también fomentar una cultura de seguridad en la que los empleados entiendan la importancia de la seguridad de la información y estén motivados para cumplir con las políticas establecidas. Además, la educación y la capacitación sobre la seguridad de la información también pueden ayudar a

mejorar la comprensión de los trabajadores sobre los riesgos de seguridad y la importancia de cumplir con dichas políticas (Siponen et al., 2014).

Hu et al, (2012), investigó la influencia de la alta gerencia y la cultura organizacional en las creencias cognitivas y su impacto en la intención de cumplimiento por parte de los empleados. Sin embargo, hay pocos estudios de la variable de gobierno en combinación con las variables de conciencia de seguridad de TI y sanciones disuasorias. Las organizaciones mantienen información muy valiosa de activos que deben protegerse, tales como: impuestos de individuos, activos financieros, expedientes médicos, evaluaciones de empleados, secretos comerciales, desarrollo de productos nuevos, y datos de clientes, (Luftman & Ben-Zvi, 2011). Por otra parte, Willison y Warkentin (2013), comentan que una de las inquietudes de los gerentes de seguridad de TI es la amenaza de un colaborador del departamento de TI. Las amenazas de un empleado se consideran importantes, ya que tienen un impacto significativo, tanto de la imagen de la organización, como en lo económico, por los costos relacionados a atender incidentes de seguridad.

Luftman et al. (2012) informaron en su estudio que la seguridad y la privacidad se encontraron en el séptimo lugar a nivel mundial de las primeras diez preocupaciones de los ejecutivos de TI. Turban et al. (2013) indicó que la seguridad es problema de todos los empleados de la organización. Sin embargo, afirmó que los altos mandos son los responsables de la gobernanza de la seguridad de las TI. Además, la alta gerencia es la responsable de tomar decisiones acertadas y ágiles en cuanto a las políticas, guías, estándares y procedimientos requeridos que sirvan de disuasivo a los empleados para que cumplan con las políticas de seguridad.

Los estudios que han adoptado la teoría de conducta planificada indican que la intención está directamente relacionada con la actitud, las normas sociales y la percepción de control de los empleados (Cavallari, 2011; Guo et al. 2011; Liang, & Xue, 2010). Por otra parte, los estudios de concientización y adiestramiento en seguridad indican que los empleados que conocen las

políticas de seguridad de TI y las sanciones de disuasión, son más propensos a cumplir con dichas políticas (Bulguru et al., 2010; D'Arcy & Devaraj, 2012; D'Arcy et al., 2014; Guo et al., 2011; McCrohan et al., 2010; Puhakainen & Siponen, 2010; Vance et al., 2015; Willison & Warketin, 2013).

De acuerdo con la literatura revisada, la alta gerencia también debería darles participación a los empleados en el plan de seguridad. Según Boyle & Panko, (2015) y Turban et al. (2013), esta práctica convertirá a los empleados de ser una amenaza para estar en la primera línea de defensa de seguridad de la empresa, así que permitirles participación a los empleados los comprometería con la seguridad de TI en la organización y con el propósito de consumar las políticas de seguridad de TI. La capacitación de los empleados y de la dirección son puntos clave para la organización; más aún, aquellos seminarios en los que se repasen los valores de la organización y principios éticos sobre los cuales esos valores están sustentados (Chen et al., 2012). Estos seminarios afectarán las tres variables de la teoría de conducta planificada, las cuales se ha comprobado en múltiples estudios, que influencian al empleado en el cumplimiento de las políticas de seguridad de TI.

Del mismo modo, Turban et al. (2013) menciona que el aspecto de participación, estilo gerencial, liderazgo de la alta gerencia son indispensables, ya que los llevaría a ser los primeros en cumplir así, como en mantener un liderazgo que motive a los empleados a cumplir con dichas políticas. Esta investigación se enfocó en los factores del comportamiento de la gerencia, percibidos por los empleados, en la finalidad de los colaboradores del departamento de TI en cumplir con las prácticas de seguridad en las TI.

De acuerdo con lo anterior, es importante comprender los factores que influyen debido al importante papel que desempeñan los empleados en la seguridad de la información. La aportación de este estudio es informar a la gerencia los factores que influyen, para que estos tomen las medidas pertinentes para enfatizar la concientización de la seguridad y estableciendo sanciones de disuasión efectivas. Estas medidas, a su vez, ayudan a salvaguardar la

información y la TI y avalan su confidencialidad, entereza y acervo dentro de la organización (Turban et al., 2013).

1.2.2. *Relación teórica variable dependiente con independientes:*

Percepción de la participación de la gerencia. Para que las acciones de la gerencia tengan algún impacto en las creencias cognitivas de los colaboradores, estas deben ser observadas y comprendidas por los mismos. La gerencia puede influenciar las creencias, normas y actitudes, a través de los siguientes mecanismos: legitimidad, compromiso, equidad y justicia. La legitimidad, implica que la gerencia defienda nuevas iniciativas, programas o prácticas de seguridad de TI, a través de la articulación y establecimiento de la visión, estrategias claras, metas, objetivos, programas o políticas (Hu et al., 2011).

Tyler et al. (2007) demostró que el juicio de un individuo acerca de la legitimidad de las normas y políticas de la organización tienen una marca reveladora en la finalidad de los empleados en seguir las reglas y cumplir con las políticas. La participación de la gerencia les da legitimidad a las iniciativas de seguridad enviando un mensaje convincente a los otros gerentes y demás empleados de la empresa. El compromiso implica que los empleados perciban que la gerencia está comprometida con las prácticas establecidas en la organización; la equidad y justicia implican que los empleados perciban que la gerencia practica la equidad y justicia al definir, establecer y hacer cumplir las prácticas de seguridad de TI (Hu et al., 2011).

Concientización de la seguridad de TI – es el conocimiento general del empleado en el campo de la seguridad de la información y su conocimiento de los métodos para garantizar la seguridad de TI en su organización. (Bulguru, et al., 2010). Las dimensiones de concientización de la seguridad de TI son: concientización de seguridad en general, y concientización de las prácticas de seguridad de TI. Concientización de seguridad en general, se define como el conocimiento y la comprensión de los problemas potenciales relacionados con la seguridad de la información y sus ramificaciones en general. Más allá de la concientización de seguridad en general, las organizaciones tienen expectativas específicas de sus empleados que se reflejan en la concientización para cumplir

las prácticas de seguridad de TI. Continúa Bulguru et al. (2010) en su explicación que la concientización de las prácticas de seguridad de TI, se define como el conocimiento de un empleado y la comprensión de los requisitos prescritos en las prácticas de seguridad de TI de la organización y los objetivos de dichos requisitos.

Sanciones formales de disuasión - Se relacionan con la convicción y dureza de las sanciones percibidas por los empleados asignadas por una organización por el uso ilícito o no autorizado de TI. (D'Arcy & Herath, 2011). Estudios de disuasión en el contexto de la organización, han definido sanciones formales como la probabilidad percibida por los empleados, de ser descubiertos, reprendidos y castigados por la organización, debido a una conducta ilícita en el lugar de trabajo. Las dimensiones de las sanciones formales de disuasión son: certeza y severidad. La certeza y la severidad percibida por los empleados pueden controlar la intención de estos de cumplir con las prácticas de seguridad de TI por el castigo relacionado al no cumplimiento con las mismas (D'Arcy & Herath, 2011).

Sanciones informales de disuasión – Se relacionan con los costos sociales y de autoempleo que los empleados consideran antes de tomar decisiones sobre el incumplimiento de las reglas de seguridad de TI. (D'Arcy & Devaraj, 2012). Las dimensiones de las sanciones informales de disuasión son: actitud hacia el cumplimiento, normas subjetivas hacia el cumplimiento y control percibido hacia el cumplimiento (Hu et al., 2012). Las tres dimensiones mencionadas forman parte del marco conceptual de la teoría de conducta planificada (Ajzen & Fishbein, 1980; Ajzen, 1991; D'Arcy & Devaraj, 2012; Hu et al., 2012).

Contexto laboral – Se refiere al argumento inmediato de ocupación y a las peculiaridades del trabajo (D'Arcy & Devaraj, 2012). Las dimensiones de contexto laboral son: trabajo virtual y jerarquía de empleo. El trabajo virtual se refiere al grado de trabajo que un empleado realiza desde lugares dispersos en contraposición a las facilidades principales de la empresa (Wiesenfeld et al.,

1999). La jerarquía de empleo para propósitos de esta investigación se refiere a si es puesto gerencial o no gerencial el cual puede contribuir a perpetrar las prácticas de seguridad de TI (D'Arcy & Devaraj, 2012).

1.2.3. *La justificación teórica y/o aplicada de las variables independientes:*

Percepción de la participación de la gerencia – Mediación de la dirección en cuestiones de seguridad de TI a partir la vista de los empleados (Hu et al., 2011). Sustentado en la Teoría del comportamiento planificado. (Hu et al., 2012; Aurigemma & Panko, 2012).

Concientización de la seguridad de TI – "son los conocimientos generales de un empleado sobre seguridad de la información y su conocimiento de las prácticas de seguridad de TI de su organización" (Bulguru, et al., 2010). Apoyada en la Teoría del comportamiento planificado. (Hu et al., 2012; Aurigemma, & Panko, 2012).

Sanciones formales de disuasión - Se relacionan con la convicción y dureza de las sanciones percibidas por los empleados atribuidas por un organismo por el uso indebido o no facultado de TI (D'Arcy & Herath, 2011). Variable sustentada en la Teoría de la disuasión general. (D'Arcy & Devaraj, 2012).

Sanciones informales de disuasión – Se relacionan con los costos sociales y de autoempleo que los empleados consideran antes de tomar decisiones sobre el incumplimiento de las reglas de seguridad de TI. (D'Arcy & Devaraj, 2012; Hu et al., 2012). Teoría de la conducta planificada. (Hu et al., 2012).

Contexto laboral – Se refiere al contexto inmediato de empleo y a las peculiaridades del trabajo (D'Arcy & Devaraj, 2012). En su estudio, evaluaron el impacto del contexto laboral en la intención de uso no adecuado de la tecnología. Teoría de la disuasión general y Teoría del comportamiento planificado. (D'Arcy & Devaraj, 2012) y (Hu et al., 2012; Aurigemma, & Panko, 2012).

1.3. Pregunta Central de Investigación

¿Cuáles son los factores que se relacionan con el cumplimiento las prácticas de seguridad de tecnologías de información por parte de los empleados en las tres instituciones de educación superior públicas más grandes de México?

1.4. Objetivo General de la Investigación

Determinar los factores que se relacionan con el cumplimiento de las prácticas de seguridad de tecnologías de información por parte de los empleados en las tres instituciones de educación superior públicas más grandes de México.

1.4.1. *Objetivos Metodológicos de la Investigación*

1. Analizar los antecedentes del problema a investigar
2. Revisión del Marco Teórico
3. Elaborar el instrumento con que serán medidas las variables
4. Validar y Aplicar el instrumento a la población objetivo o en su caso a la muestra.
5. Analizar los resultados que permitan aprobar o desaprobar la existencia de una relación de las variables independientes con la dependiente en las hipótesis del estudio.

1.5. Hipótesis General de la Investigación

La percepción y colaboración de la dirección, la concienciación de la seguridad de tecnologías de información, las sanciones formales de disuasión, las sanciones informales de disuasión y el contexto laboral se relacionan con el cumplimiento de las prácticas de seguridad de tecnologías de información por parte de los empleados en las tres IES públicas más grandes de México.

1.6. Metodología

El diseño de esta investigación es cuantitativo, con un alcance, descriptivo, correlacional, no experimental, transeccional, ya que se pretende proporcionar información acerca de la presencia de una correspondencia entre las variables asociadas con el propósito de que los empleados puedan cumplir estas reglas relacionadas con su trabajo. Adicionalmente se propone un modelo de regresión

con las variables en su conjunto. La población serán todos los empleados que trabajan con tecnologías de información, como parte de su trabajo diario que pertenecen a las tres IES más grandes de México, se pretenderá utilizar una muestra estratificada no probabilística a la cual se le aplicará una encuesta de aproximadamente 37 preguntas con una escala de tipo Likert para la recolección de los datos, los cuales se buscará analizarlos a través de estadística multivariante con un modelo de ecuaciones estructurales.

1.7. Justificación de la Investigación

1) **Justificación práctica:** Esta investigación es importante porque se analizarán los factores del comportamiento de la gerencia, percibidos por los empleados, que influyen en el propósito de estos, para realizar las prácticas de seguridad en las TI en las tres IES públicas más grandes de México las cuales se verán beneficiadas. La aportación de este estudio es informar a las autoridades de las IES, los factores que afectan, para que se tomen las medidas apropiadas para aumentar el objetivo de que los empleados ejecuten las reglas de seguridad de TI, enfatizar la conciencia y aplicar sanciones respecto al tema. Estas medidas, a su vez, ayudarán a proteger y a garantizar la disponibilidad de la información en la institución.

2) **Justificación Metodológica:** En este estudio se propondrá una metodología que permitirá responder los problemas, los objetivos y las hipótesis de la presente investigación a través de la aplicación de una encuesta que ayudará a las IES a mejorar las reglamentaciones y quehaceres relacionados con el tema en cuestión.

3) **Justificación Teórica:** En esta investigación se analizarán teorías sobre los factores que impactan la finalidad de los empleados en cumplir con las reglas de salvaguarda de las prácticas de TI en las IES, debido al rol importante que los empleados juegan en la seguridad de la información. Muchos estudios han investigado el impacto de creencias justificativas (*normative beliefs*) y autoeficacia (self-*efficacy*) en las actitudes (*attitudes*)

de los trabajadores y en el cumplimiento relacionado con el resguardo de la información como parte de su compromiso en las organizaciones (Bulgurcu et al., 2010; Chen et al., 2012; D'Arcy & Devaraj, 2012; D'Arcy et al., 2014; Hu et al., 2012; Johnston et al., 2015). Hu et al. (2012), investigaron la influencia de la alta gerencia y la cultura organizacional en las creencias cognitivas (*cognitive* beliefs) y su impacto en la intención de cumplimiento por parte de los empleados. Sin embargo, muy pocos han examinado la variable de gobierno en combinación con la conciencia de seguridad de TI y las variables de sanciones disuasorias.

Por otro lado, la amenaza que representan los empleados es una de las mayores preocupaciones de los gerentes de seguridad de TI. (Willison & Warkentin, 2013). Las IES mantienen información muy importante y valiosa que deben proteger tales como: datos personales de los alumnos, información financiera de la institución, expedientes médicos, evaluaciones de empleados.

1.8. Delimitaciones del estudio

1) **Espaciales:** La presente indagación se realizó en las tres IES públicas más grandes de México: UANL, UNAM. y U de G.

2) **Demográficas**: Esta investigación estuvo dirigida a todos los empleados que trabajan con tecnologías de información, como parte de su trabajo diario que pertenecen a las tres IES públicas más grandes de México: UANL, UNAM. y U de G.

3) **Temporales**: Esta investigación fue de corte transeccional, en la cual se llevó a cabo la colocación y concentración de las encuestas en el período del 2022, la recolección de datos fue aproximadamente de 6 meses.

1.9. Matriz de Congruencia

A continuación, se muestra la tabla 3 la matriz de congruencia donde se observan el objetivo de investigación, la pregunta, el marco teórico la hipótesis, así como las variables de estudio.

Tabla 3. Matriz de Congruencia Metodológica.

Objetivo de Investigación	Pregunta de Investigación	Marco Teórico	Hipótesis	Variables
Determinar los factores que se relacionan con el cumplimiento de las prácticas de seguridad de tecnologías de información por parte de los empleados en las tres IES públicas más grandes de México.	¿Cuáles son los factores que se relacionan con el cumplimiento de las prácticas de seguridad de tecnologías de información por parte de los empleados en las tres IES públicas más grandes de México?	Teoría de Disuasión General (D'Arcy y Herath, 2012). Teoría de Conducta Planificada (Hu et al., 2012) La Teoría de la Acción Razonada (Siponen M. et al., 2014)	La percepción y participación de la gerencia, la concientización de la seguridad de tecnologías de información, las sanciones formales de disuasión, las sanciones informales de disuasión y el contexto laboral se relacionan con el cumplimiento de las prácticas de seguridad de tecnologías de información por parte de los empleados de las tres IES públicas más grandes de México.	V1: La Percepción y Participación de la Dirección V2: Concientización de la Seguridad de TI V3: Sanciones Formales de Disuasión V4: Norma Social V5: Contexto Laboral V: Cumplimiento de los empleados con las prácticas de Seguridad de TI

Capítulo 2. MARCO TEÓRICO

2.1. Marco Teórico de la variable Cumplimiento de las prácticas de Seguridad de TI.

2.1.1. *Teorías, definiciones e investigaciones aplicadas*

a) ***Teorías y Definiciones*** **de la variable Cumplimiento de las prácticas de seguridad de TI.**

A continuación, se describen de las teorías, así como de las definiciones revisadas en la literatura, las cuales dan soporte a la variable dependiente, iniciando con la Teoría de la Acción Razonada (Ajzen & Fishbein, 1980) que se utiliza ampliamente para predecir el comportamiento de las personas. La teoría contempla dos variables que influyen: la actitud hacia el comportamiento y la norma subjetiva del individuo. La Teoría de la Acción razonada, la cual fue propuesta inicialmente por Icek Ajzen y Martin Fishbein a finales de los años sesenta. Publicaron sus ideas y conclusiones en varias obras, y desde entonces la teoría ha sido objeto de perfeccionamientos y ampliaciones. Posteriormente, Ajzen desarrolló la Teoría del Comportamiento Planificado, que integraba el concepto de control del comportamiento. La Teoría de la Acción Razonada (TRA) es una teoría psicológica social que explica el comportamiento humano centrándose en la relación entre actitudes, intenciones y comportamiento. Las partes más importantes de la teoría pueden resumirse como sigue:

Actitud: La actitud se refiere a la evaluación general de una persona de un comportamiento particular. Estas calificaciones dependen de las creencias de las personas sobre los resultados del comportamiento y la importancia de esos resultados. Las actitudes pueden ser positivas o negativas.

Normas subjetivas: las normas subjetivas representan presiones sociales percibidas o expectativas de otras personas significativas que influyen en la intención de un individuo de realizar un determinado comportamiento. Consta de dos componentes: (a) las creencias de un individuo acerca de si otras personas significativas piensan que deben actuar (creencias normativas) y (b) la motivación de un individuo para cumplir con los deseos de esas personas significativas (motivación de cumplimiento).

Intención de comportamiento: La intención de comportamiento es el plan o el deseo de una persona de realizar un determinado comportamiento. Están influidos tanto por las actitudes como por las normas subjetivas. Cuanto más fuerte sea la actitud positiva hacia el comportamiento y la presión social percibida, más probable es que el individuo tenga una fuerte intención de realizar el comportamiento.

Control conductual: Este elemento se añadió posteriormente en la versión ampliada de la teoría, conocida como Teoría del Comportamiento Planificado (TCP). Sugiere que los individuos no siempre tienen pleno control sobre sus conductas debido a diversas limitaciones y factores externos. El control conductual tiene en cuenta la facilidad o dificultad percibida para realizar la conducta.

En resumen, la Teoría de la Acción Razonada considera que las creencias, las actitudes, las normas subjetivas y las intenciones son factores importantes para predecir el comportamiento humano (Ajzen, 1991). De acuerdo con Rueda et al. (2013) esta teoría es un modelo muy importante en la literatura sobre el comportamiento individual, según el cual el comportamiento humano se explica en términos de relaciones creencia-actitud-intención-comportamiento. (Siponen et al., 2014).

Así mismo la Teoría del Comportamiento Planificado es el descendiente de la Teoría de la Acción razonada de Ajzen y Fishbein (1975; 1980). Esta teoría se basa en dogmas de vigilancia: éstas son reconocimientos sobre la figura de componentes que consiguen proporcionar, o pueden paralizar, el ejercicio de la conducta, por lo que esta teoría se considera uno de los marcos teóricos más predominantes en los estudios de la conducta humana (Aurigemma & Panko, 2012; Hu et al., 2012).

De acuerdo con lo anterior la Teoría del Comportamiento Planificado la cual es una teoría de psicología social ampliamente utilizada que explica y predice el comportamiento humano basándose en las actitudes individuales, las normas sociales y el control conductual percibido. Desarrollada por Icek Ajzen,

la TCP amplía la anterior Teoría de la Acción Razonada (TAR) al incluir el elemento del control conductual percibido. La TCP postula que estos tres factores -actitud, norma subjetiva y control conductual percibido- interactúan para influir en la intención de una persona de realizar un comportamiento específico, lo que a su vez predice el comportamiento real. La teoría es particularmente útil para comprender y predecir el comportamiento guiado por la conciencia e implica cierto grado de conciencia. TCP se ha utilizado en diversos campos, como la salud, el medio ambiente, el marketing, el comportamiento organizacional. Desglosemos los componentes de la Teoría del Comportamiento Planificado.

Creencias conductuales: Creencias sobre los resultados asociados con la realización del comportamiento. Evaluación de resultados: una evaluación individual de la conveniencia o el valor de esos resultados. Fuerza de la actitud: una evaluación general de la fuerza que influye en la influencia de las actitudes en las intenciones.

Las normas subjetivas reflejan presiones sociales percibidas o expectativas de comportamiento. Si una persona significativa aprueba o desaprueba una actividad es una cuestión de opinión. Las normas subjetivas constan de dos componentes:

Creencias normativas: Creencias sobre lo que otros piensan o esperan sobre el comportamiento. Motivación de conformidad: la motivación de un individuo es ajustarse a las expectativas percibidas de los demás.

Control conductual percibido (CCP): El control conductual percibido se refiere a la percepción del individuo sobre la facilidad o dificultad de realizar la conducta. Incorpora factores internos y externos que pueden facilitar o dificultar la conducta. El CCP incluye dos componentes:

Creencias de control: Creencias sobre los factores que pueden facilitar o dificultar la conducta.

Poder Percibido: Percepción del individuo sobre el grado de control que tiene sobre estos factores facilitadores u obstaculizadores.

Intención de comportamiento (BI): La intención de comportamiento es la intención o motivación de un individuo para realizar un determinado comportamiento. Está influenciado por actitudes, normas subjetivas y control conductual percibido. Las intenciones pueden predecir directamente el comportamiento real.

Comportamiento real: Aunque la teoría del comportamiento planificado se centra en la predicción de las intenciones, asume que las intenciones son fuertes predictores del comportamiento real. Sin embargo, la TCP reconoce que los factores externos y las circunstancias imprevistas pueden influir en la transformación de la intención en conducta.

Utilizando en sus estudios la Teoría del Comportamiento Planificado, Definir la intención de cumplir con la intención del empleado de proteger la información y los activos tecnológicos de la organización de posibles infracciones de seguridad. (Ajzen, 1991; Fishbein & Ajzen, 1975).

También se define la conducta de la intención de cumplir con la seguridad de la información como el comportamiento que hace alusión al conjunto de centralizar las actividades que los usuarios finales deben cumplir, para mantener esta actividad según lo determinado por las políticas de la seguridad de la información de la institución. (Ifinedo, 2016).

Con base a la literatura revisada el concepto que se utiliza para esta investigación es el siguiente: La intención es la conducta que los individuos deben desempeñar en las experiencias de seguridad de TI.

Investigaciones Aplicadas **de la variable Cumplimiento d las prácticas de Seguridad de TI.**

Existen estudios que han investigado el impacto de creencias justificativas y autoeficacia en las actitudes de los empleados y cumplimiento con experiencias

de seguridad de TI en las instituciones (Chen et al., 2012; D'Arcy & Devaraj, 2012; D'Arcy et al., 2014; Hu et al., 2012; Johnston et al., 2015; Vance et al., 2015; Willison & Warketin, 2013).

En un estudio realizado por Johnston & Warkentin, (2010) en varias unidades de una universidad de Estados Unidos, donde hablan acerca de la influencia de su modelo de las apelaciones del miedo, la cual influye en la intención del comportamiento de los empleados y estudiantes para el cumplimiento las acciones de la seguridad informática para contrarrestar las amenazas, el estudio fue de tipo cuantitativo donde se aplicaron ecuaciones estructurales como mínimos cuadrados parciales con una muestra de 311 sujetos y se determinó que la variable intención en el comportamiento salió significativa a lo que se aconseja que para ejercer el miedo como un motivador de manera eficaz, los gerentes de TI deben diseñar una estrategia en la que los sujetos estén expuestos a las apelaciones del miedo como un lenguaje adecuado a su nivel de eficacia, así que los gerentes de seguridad pueden desear reevaluar su estrategia de gobierno de seguridad de TI para garantizar el mayor nivel de cumplimiento con la política de seguridad de la organización.

En el orden de las ideas anteriores, en Canadá se realizó un estudio cuantitativo con base en la teoría del comportamiento planificado, investigando factores basados en la racionalidad que impulsa a un empleado a cumplir con los requisitos de las políticas de seguridad con respecto a la protección de los recursos de información y tecnología de la organización. Bulguru et al. (2010) postularon que, junto con la creencia normativa y la autoeficacia, la manera de un empleado hacia la obediencia que determina la intención de cumplir con la política de seguridad de información; utilizando ecuaciones estructurales con una muestra de 464 participantes, donde se determinó que la variable intención de un empleado de cumplir con los requisitos de las políticas de seguridad de la información resultó muy significativa mostrando relación con la variable dependiente de este estudio.

En este orden de ideas se puede citar a Ifinedo (2016) en su investigación empírica realizada en Canadá, donde examinó el análisis costo – beneficio de los empleados, las consideraciones de disuasión, así como el apoyo y las creencias de la alta gerencia como factores que impactan sobre el cumplimiento de la política de seguridad de los sistemas de información, siendo un estudio cuantitativo aplicó ecuaciones estructurales utilizando una muestra de 176 sujetos, obteniendo como resultado que el comportamiento hacia el cumplimiento de las políticas de seguridad y su intención, se ven impactados positiva y significativamente por mecanismos de disuasión en forma de sanción y el apoyo de la alta dirección, relacionándose fuertemente con la variable principal de esta investigación la cual era la intención de los empleados en cumplir con las prácticas de seguridad de TI.

Por otro lado, Siponen et al. (2014) desarrollaron un modelo basado en varias teorías, siendo una de ellas la teoría de la acción razonada, para investigar la intención, así como el cumplimiento real de las políticas de seguridad de la información, utilizando una muestra de 669 participantes de cuatro corporaciones en Finlandia, los resultados basados en ecuaciones estructurales, mostraron el designio de perpetrar las políticas de seguridad de la información tuvo un impacto positivo y significativo en el cumplimiento real de dichas políticas.

2.1.2. *Estudios de investigaciones aplicadas sobre la relación de la variable Cumplimiento de las prácticas de Seguridad de TI con la Percepción de la Participación de la Dirección, la Concientización de la Seguridad de TI, las Sanciones Formales de Disuasión las Sanciones Informales de Disuasión, el Contexto Laboral.*

Con base en la revisión de la literatura consultada, existen distintos factores que influyen en la intención de los empleados en el cumplimiento de las políticas de seguridad de las tecnologías de información como son la precepción de la participación de la dirección, la concientización de la seguridad de tecnologías de información, las sanciones formales e informales de disuasión, así como el contexto laboral. Según Hu et al. (2012) el rol que desempeña la alta

dirección y la cultura organizacional es integrado en cuanto a cómo puede influir la alta dirección en el comportamiento del cumplimiento de la seguridad de la información por parte de los empleados, en su modelo probaron las relaciones que tuvieron la participación de la gerencia, la cultura organizacional a lo que descubrieron que los empleados fueron influidos directa e indirectamente de una forma muy significativa en las actitudes de los mismos hacia las normas subjetivas y de vigilancia de conducta percibido.

Así mismo Ifinedo (2016) encontró en su estudio al examinar los impactos que tiene el análisis de costo-beneficio de los empleados, las consideraciones de disuasión como también el apoyo y las creencias de la alta gerencia sobre la intención en el cumplimiento de las políticas de seguridad de los sistemas de información canadienses, que fueron significativamente influyentes en la intención de los empleados en dicho cumplimiento.

Por otra parte Shaw (2012) añade a través de los resultados de su estudio, la comprensión de las relaciones entre la cultura organizacional y las actitudes hacia la política de la seguridad de la información, contribuyendo a que existe una relación estadísticamente significativa entre ambas, explicando que un excelente liderazgo aprovecha el inconsciente, las creencias, percepciones, pensamientos y sentimientos de la organización para facilitar el logro de las metas y estrategias con la fuerza laboral que tiene de cada individuo y de esta manera influir en las actitudes sobre las prácticas de seguridad de la información.

De acuerdo con un estudio realizado en Estados Unidos, se investigó acerca de la influencia de las apelaciones del miedo, la cual influye en la intención del comportamiento de los empleados y estudiantes para el cumplimiento las acciones de la seguridad informática para contrarrestar las amenazas, obteniendo el resultado se determinó que la intención en el comportamiento fue significativo, a lo que se aconseja que para ejercer temor como un motivador de manera eficaz, los gerentes de TI deben diseñar una estrategia en la que los empleados estén expuestos a las apelaciones del miedo como un lenguaje adecuado a su nivel de eficacia, así que los gerentes de

seguridad pueden desear reevaluar su estrategia de gobierno de seguridad de TI para garantizar el mayor nivel de cumplimiento con la política de seguridad de la organización (Johnston & Warkentin, 2010).

En cuanto a la concientización de la seguridad de TI, el estudio de Alarcón y Orjeda (2019) está centrado en la manera de profetizar el actuar de los empleados de TI frente a las políticas de seguridad de la información donde se determinó que la concientización a través de la capacitación tiene un mayor impacto en el comportamiento, la intención y el compromiso de salvaguardar la información.

Bulguru et al. (2010) identifican que la racionalidad, la creencia normativa y la autoeficacia impulsan a un empleado a cumplir con la política de seguridad de la compañía por lo que postulan que la actitud de un trabajador está influenciada por el beneficio del cumplimiento, el costo del cumplimiento y el costo del no cumplimiento por lo que el impacto de conciencia de la seguridad de la información se basa sobre las creencias, los resultados y la actitud hacia el cumplimiento de las políticas de seguridad de la información.

También en Australia se llevó a cabo un estudio cualitativo, exploratorio, donde tuvo como propósito evaluar la efectividad de diversos programas de sensibilización y concienciación de la seguridad de la información, realizaron tres sesiones de concientización sobre seguridad de la información utilizando métodos de entrega basados en texto, juegos y video, empleando una muestra de 60 participantes, basándose en experiencias metodológicas, obteniendo como resultado que la capacitación en la concientización sobre la seguridad de la información es un medio poderoso para que los empleados cumplan con las políticas de seguridad de la información Abawajy (2014).

En cuanto a las sanciones formales de disuasión Montesdeoca, & Gonzaga. (2018) realizaron una investigación en la cual determinaron que la intención del cumplimiento de las políticas de seguridad de la información está

influenciada por la actitud, frente a la política de seguridad y la dureza del castigo a través de las sanciones formales de disuasión.

Por otra parte el modelo integral de violación a la política de seguridad de la información por parte de los empleados en el entorno organizacional, desarrollado por Hu et al. (2011) lo basan en muchas teorías de criminología, donde los empleados tienen una gran creencia moral sobre el bien y el mal por lo que están menos inclinados a cometer faltas aun y se les presente la oportunidad, por lo que determinaron que las sanciones formales de disuasión son efectivas en el cumplimiento de las políticas de seguridad de la información acompañadas de una motivación intrínseca.

En Estados Unidos se realizó un estudio cuantitativo en el cual probaron empíricamente el modelo teórico de los efectos incentivadores de las sanciones, presiones y efectividad de los empleados en el cumplimento de las políticas de seguridad de la información, teniendo como resultado que las sanciones formales e informales de disuasión tienen un impacto positivo (Herath & Rao, 2009).

También Herath y Rao (2009) realizaron una investigación, desarrollando un modelo de protección, motivación y disuasión en el cumplimiento de la política de seguridad de la información, además evaluaron el efecto del compromiso organizacional sobre las intenciones de los empleados en el cumplimiento de la seguridad, en donde se determinó que la disuasión a través de la sanción formal e informal tienen un impacto positivo en la intención de del cumplimento de la política de seguridad de la información.

Continuando con las sanciones informales de disuasión Johnston, Warkentin & Siponen, (2015) desarrollaron un estudio cuantitativo en Finlandia con 559 participantes donde se constató que la gravedad de las sanciones informales y la certeza de las sanciones informales de disuasión, fueron significativas en sus funciones como determinantes directos de la intención del cumplimiento de los empleados en las políticas de seguridad de la información.

Por otra parte, Hovav & D'Arcy, (2012) llevaron a cabo una investigación, donde realizaron una comparación entre Estados Unidos y Corea haciendo la misma investigación en ambos países para ver si la cultura influía en las capacidades disuasorias de las políticas de seguridad obteniendo como resultado que en ambas partes fue significativa la sanción informal de disuasión para el cumplimiento de las políticas de seguridad de la información.

En cuanto al contexto laboral se realizó un estudio donde D'Arcy & Devaraj, (2012) determinaron que la influencia del contexto laboral, cuando los empleados trabajan de manera remota, no hace mal uso de la tecnología ni de la información de la compañía, cuando tienen un cargo de gerencia, siendo más propensos a cumplir con las políticas de seguridad de la información.

Así también se perpetró una investigación donde se desdobló un modelo que alerta sobre los factores importantes que inciden en el proceder deliberado y no deliberado de los trabajadores de tecnologías de información, donde se determinó que el contexto laboral influye en el cumplimiento de las políticas de seguridad de la información (Celi & Díaz, 2017).

De acuerdo con Wiesenfeld et al. (1999) quienes realizaron un estudio en Estados Unidos donde evaluaron el grado de trabajo que un empleado realiza en lugares dispersos en contraposición a realizar trabajos en las facilidades físicas de la empresa, explorando el papel que juega la TI en la instauración y el mantenimiento de una identidad común entre los miembros de la organización desconectados. En este contexto laboral virtual los empleados tienden a cumplir con las prácticas de seguridad de la información en mayor medida si su categoría dentro de la empresa es de un nivel de jefe, gerente o mayor.

2.2. Marco Teórico y Estudios de investigaciones aplicadas a las variables Independientes.

2.2.1. *Variable independiente V1 Percepción de la Participación de la dirección.*

a) Teorías y Definiciones de la variable V1 Percepción de la participación de la dirección.

A continuación, se describen las teorías que sustentan la variable percepción de la participación de la dirección, así como de las definiciones revisadas en la literatura, las cuales dan soporte a la variable independiente Percepción de la participación de la dirección iniciando con la Teoría de la Acción razonada, la cual fue propuesta inicialmente por Icek Ajzen y Martin Fishbein a finales de los años sesenta. Publicaron sus ideas y conclusiones en varias obras, y desde entonces la teoría ha sido objeto de perfeccionamientos y ampliaciones. Posteriormente, Ajzen desarrolló la Teoría del Comportamiento Planificado, que integraba el concepto de control del comportamiento. La Teoría de la Acción Razonada (TRA) es una teoría psicológica social que explica el comportamiento humano centrándose en la relación entre actitudes, intenciones y comportamiento. Las partes más importantes de la teoría pueden resumirse como sigue:

Actitud: La actitud se refiere a la evaluación general de una persona de un comportamiento particular. Estas calificaciones dependen de las creencias de las personas sobre los resultados del comportamiento y la importancia de esos resultados. Las actitudes pueden ser positivas o negativas.

Normas subjetivas: las normas subjetivas representan presiones sociales percibidas o expectativas de otras personas significativas que influyen en la intención de un individuo de realizar un determinado comportamiento. Consta de dos componentes: (a) las creencias de un individuo acerca de si otras personas significativas piensan que deben actuar (creencias normativas) y (b) la motivación de un individuo para cumplir con los deseos de esas personas significativas (motivación de cumplimiento).

Intención de comportamiento: La intención de comportamiento es el plan o el deseo de una persona de realizar un determinado comportamiento. Están influidos tanto por las actitudes como por las normas subjetivas. Cuanto más fuerte sea la actitud positiva hacia el comportamiento y la presión social

percibida, más probable es que el individuo tenga una fuerte intención de realizar el comportamiento.

Control conductual: Este elemento se añadió posteriormente en la versión ampliada de la teoría, conocida como Teoría del Comportamiento Planificado (TCP). Sugiere que los individuos no siempre tienen pleno control sobre sus conductas debido a diversas limitaciones y factores externos. El control conductual tiene en cuenta la facilidad o dificultad percibida para realizar la conducta.

De acuerdo con lo anterior la Teoría del Comportamiento Planificado la cual es una teoría de psicología social ampliamente utilizada que explica y predice el comportamiento humano basándose en las actitudes individuales, las normas sociales y el control conductual percibido. Desarrollada por Icek Ajzen, la TCP amplía la anterior Teoría de la Acción Razonada (TAR) al incluir el elemento del control conductual percibido. La TCP postula que estos tres factores -actitud, norma subjetiva y control conductual percibido- interactúan para influir en la intención de una persona de realizar un comportamiento específico, lo que a su vez predice el comportamiento real. La teoría es particularmente útil para comprender y predecir el comportamiento guiado por la conciencia e implica cierto grado de conciencia. TCP se ha utilizado en diversos campos, como la salud, el medio ambiente, el marketing, el comportamiento organizacional (Aurigemma & Panko, 2012; Hu et al., 2012).

Así mismo se desglosan los componentes de la Teoría del Comportamiento Planificado.

Creencias conductuales: Creencias sobre los resultados asociados con la realización del comportamiento. Evaluación de resultados: una evaluación individual de la conveniencia o el valor de esos resultados. Fuerza de la actitud: una evaluación general de la fuerza que influye en la influencia de las actitudes en las intenciones.

Las normas subjetivas reflejan presiones sociales percibidas o expectativas de comportamiento. Si una persona significativa aprueba o desaprueba una actividad es una cuestión de opinión. Las normas subjetivas constan de dos componentes:

Creencias normativas: Creencias sobre lo que otros piensan o esperan sobre el comportamiento. Motivación de conformidad: la motivación de un individuo es ajustarse a las expectativas percibidas de los demás.

Control conductual percibido (CCP): El control conductual percibido se refiere a la percepción del individuo sobre la facilidad o dificultad de realizar la conducta. Incorpora factores internos y externos que pueden facilitar o dificultar la conducta. El CCP incluye dos componentes:

Creencias de control: Creencias sobre los factores que pueden facilitar o dificultar la conducta.

Poder Percibido: Percepción del individuo sobre el grado de control que tiene sobre estos factores facilitadores u obstaculizadores.

Intención de comportamiento (IC): La intención de comportamiento es la intención o motivación de un individuo para realizar un determinado comportamiento. Está influenciado por actitudes, normas subjetivas y control conductual percibido. Las intenciones pueden predecir directamente el comportamiento real.

Comportamiento real:

Aunque la teoría del comportamiento planificado se centra en la predicción de las intenciones, asume que las intenciones son fuertes predictores del comportamiento real. Sin embargo, la TCP reconoce que los factores externos y las circunstancias imprevistas pueden influir en la transformación de la intención en la conducta (Ajzen, 1991).

Con referencia a lo anterior, se describe a continuación algunas definiciones de la variable percepción de la participación de la dirección, la cual se refiere al grado en que los empleados perciben que los líderes y gerentes de

la organización participan activamente, se comunican y responden a las necesidades e inquietudes de los empleados (Mullins, 2010).

La percepción de la participación de la dirección es la valoración subjetiva que tienen los empleados sobre el grado en que la dirección participa activamente en diversos aspectos del lugar de trabajo, como la toma de decisiones, la comunicación y la resolución de los problemas de los empleados (Coulter & DeCenzo, 2017).

Con base a la literatura revisada el concepto que se utiliza para esta investigación es el siguiente: Percepción de la participación de la gerencia, grado en el que perciben los empleados el compromiso por parte de la gerencia en tomar parte o involucrarse en cuestiones de la seguridad de TI.

b) Investigaciones Aplicadas de la variable independiente (Percepción de la Participación de la Dirección)

Hu et al. (2012) realizaron un estudio cuantitativo llevado a cabo en Estados Unidos, donde utilizaron ecuaciones estructurales con una muestra de 148 sujetos, lo que determinó que la participación de los directivos de mayor rango en las decisiones de seguridad de la información tiene un impacto positivo muy fuerte en la percepción de los empleados en las intenciones de cumplir con las políticas de seguridad de TI al percibir que la gerencia puede desempeñar un papel proactivo.

En Canadá se realizó un estudio cuantitativo en el cual se aplicaron ecuaciones estructurales a una muestra de 176 participantes, donde se efectuó una encuesta de campo para la recopilación de datos. Los ítems del cuestionario se derivaron de escalas que han sido validadas en bibliografías existentes. 10 personas participaron en la prueba previa del cuestionario, incluidos profesionales con conocimiento de política de seguridad de los sistemas de información. Los datos se recopilaron mediante cuestionarios en papel y en línea. Las respuestas se recopilaron utilizando una variedad de fuentes: gerentes que

no pertenecen a SI, profesionales de SI y profesionales de las redes sociales. Proporciona un incentivo para participar y garantiza el anonimato.

Se evaluaron las propiedades psicométricas del modelo, incluidas la consistencia interna, la validez convergente y la validez discriminante. Se calcularon los valores de fiabilidad compuesta, alfa de Cronbach y AVE, que cumplían criterios aceptables. La validez discriminante se demostró mediante los valores AVE y las cargas cruzadas de los constructos. Las hipótesis se comprobaron mediante el modelo de ecuaciones estructurales por mínimos cuadrados parciales (PLS). Las hipótesis relacionadas con el apoyo de la alta dirección, el análisis coste-beneficio y la gravedad de la sanción resultaron confirmadas. La hipótesis relativa al impacto de la probabilidad de detección en la intención de comportamiento no se confirmó. Los constructos explicaron el 30% de la varianza en la intención de comportamiento del ISSP.

Los resultados contribuyen a la base de conocimientos en este campo y ofrecen implicaciones prácticas para la gestión del cumplimiento de la política de seguridad de los sistemas de información. En general, la investigación se centró en la comprensión de las influencias sobre el cumplimiento de las directrices de la política de seguridad de los sistemas de información (ISSP) por parte de los trabajadores y destacó la importancia de factores como el apoyo de la alta dirección, el análisis coste-beneficio y la gravedad de la sanción, de tal manera que se determinó que la variable apoyo y las creencias de la alta gerencia el análisis de costo-beneficio como factores que impactan la percepción e intención en el cumplimiento de la política de seguridad de TI por parte de los empleados resultaron significativas (Ifinedo, 2016).

Se realizó un estudio en Estados Unidos de tipo cuantitativo donde se aplicaron ecuaciones estructurales a 250 sujetos, determinando que la percepción de los trabajadores acerca de la cooperación de las autoridades en las políticas de seguridad de la información trajo un efecto positivo en el cumplimiento por parte de los empleados de dichas políticas. (Shaw, 2012).

2.2.2. *Variable V2 Concientización de la Seguridad de TI.*

Teorías y Definiciones de la variable Concientización de la Seguridad de TI.

En el orden de las ideas anteriores, a continuación se describen las teorías, así como de las definiciones revisadas en la literatura, las cuales dan soporte a la variable independiente Concientización de la seguridad de TI iniciando con la Teoría del Comportamiento Planificado la cual se basa en afirmaciones de vigilancia: éstas son dogmas sobre la figura de componentes que pueden proporcionar, o pueden frenar, el cometido del proceder, por lo que esta teoría se considera uno de los marcos teóricos más predominantes en los estudios de la conducta humana (Aurigemma & Panko, 2012; Hu et al., 2012), la Teoría del Comportamiento Planificado propone que la intención de un individuo de realizar una conducta está influida por sus actitudes hacia la conducta, las normas subjetivas y el control conductual percibido. Estas intenciones, a su vez, predicen el comportamiento real, aunque también pueden influir factores externos. La TCP proporciona un marco estructurado para comprender y predecir el comportamiento humano, lo que la hace valiosa para diseñar intervenciones y estrategias que fomenten o desincentiven acciones específicas. Y la Teoría de la Acción razonada, que son las creencias que una persona tiene acerca del comportamiento que va a realizar y que influyen en su actitud hacia ese comportamiento. Por otro lado, esas creencias normativas influyen en la norma subjetiva de la persona. (Ajzen, 1991).

De acuerdo con lo anterior la Teoría del Comportamiento Planificado la cual es una teoría de psicología social ampliamente utilizada que explica y predice el comportamiento humano basándose en las actitudes individuales, las normas sociales y el control conductual percibido. Desarrollada por Icek Ajzen, la TCP amplía la anterior Teoría de la Acción Razonada (TAR) al incluir el elemento del control conductual percibido. La TCP postula que estos tres factores -actitud, norma subjetiva y control conductual percibido- interactúan para influir en la intención de una persona de realizar un comportamiento específico, lo que a su vez predice el comportamiento real. La teoría es particularmente útil para comprender y predecir el comportamiento guiado por la conciencia e implica cierto grado de conciencia. TCP se ha utilizado en diversos

campos, como la salud, el medio ambiente, el marketing, el comportamiento organizacional (Aurigemma & Panko, 2012; Hu et al., 2012).

Así mismo se desglosan los componentes de la Teoría del Comportamiento Planificado. Creencias conductuales: Creencias sobre los resultados asociados con la realización del comportamiento. Evaluación de resultados: una evaluación individual de la conveniencia o el valor de esos resultados. Fuerza de la actitud: una evaluación general de la fuerza que influye en la influencia de las actitudes en las intenciones.

Las normas subjetivas reflejan presiones sociales percibidas o expectativas de comportamiento. Si una persona significativa aprueba o desaprueba una actividad es una cuestión de opinión. Las normas subjetivas constan de dos componentes:

Creencias normativas: Creencias sobre lo que otros piensan o esperan sobre el comportamiento. Motivación de conformidad: la motivación de un individuo es ajustarse a las expectativas percibidas de los demás.

Control conductual percibido (CCP): El control conductual percibido se refiere a la percepción del individuo sobre la facilidad o dificultad de realizar la conducta. Incorpora factores internos y externos que pueden facilitar o dificultar la conducta. El CCP incluye dos componentes:

Creencias de control: Creencias sobre los factores que pueden facilitar o dificultar la conducta.

Poder Percibido: Percepción del individuo sobre el grado de control que tiene sobre estos factores facilitadores u obstaculizadores.

Intención de comportamiento (IC): La intención de comportamiento es la intención o motivación de un individuo para realizar un determinado comportamiento. Está influenciado por actitudes, normas subjetivas y control conductual percibido. Las intenciones pueden predecir directamente el comportamiento real.

Comportamiento real: Aunque la teoría del comportamiento planificado se centra en la predicción de las intenciones, asume que las intenciones son fuertes predictores del comportamiento real. Sin embargo, la TCP reconoce que los factores externos y las circunstancias imprevistas pueden influir en la transformación de la intención en conducta (Ajzen, 1991).

Por las consideraciones anteriores enseguida se mencionan las definiciones de la variable Concientización de la seguridad de TI lo cual son los conocimientos generales de los empleados en el campo de la seguridad de la información y su conocimiento de los métodos para garantizar la seguridad de TI en su organización. (Bulguru et al., 2010).

Según Vargas (2018) “las campañas de concientización de seguridad de la información están diseñadas para cambiar el comportamiento y reforzar buenas prácticas de seguridad de los usuarios” p. (9). Por lo general estos son responsables de la información y profesionales capaces de visión y respuesta proactiva.

Alarcón y Orjeda (2019) definen que la conciencia en seguridad de la información es fundamental para garantizar una adecuada salvaguarda de los activos intangibles de la organización. Cuando los empleados comprenden la importancia de la seguridad de la información y se les capacita en buenas prácticas de seguridad, son menos propensos a cometer errores o a caer en trampas de ingeniería social. Además, la conciencia en seguridad de la información es un factor clave en la prevención de amenazas internas, como los ataques de *phishing* y los robos de información. En resumen, la conciencia en seguridad de la información es una herramienta esencial para garantizar una adecuada gestión de la seguridad de la información en una organización.

Con base a la literatura revisada el concepto que se utiliza para esta investigación es el siguiente: Concientización de la seguridad de la información es el grado de conciencia y conocimiento acerca de los empleados de las

políticas y/o prácticas de seguridad de la información en las organizaciones, las cuales definen su comportamiento.

Investigaciones Aplicadas de la variable independiente (Concientización de la Seguridad de TI)

Alarcón & Orjeda (2019) consumaron una publicación del tipo cuantitativo a través de la regresión múltiple en Perú, donde analizaron en una muestra de 61 participantes, centrando su investigación en la manera de predecir el actuar de los empleados de TI frente a las políticas de seguridad de la información basándose en las teorías del comportamiento planificado, acción razonada y disuasión, donde se determinó que la variable concienciación de la seguridad de la información resultó significativa en el comportamiento de los empleados para cumplir con las políticas de seguridad de la información.

Bulguru et al. (2010) realizaron un estudio en Canadá con una muestra de 464 sujetos, en esta investigación cuantitativa utilizaron ecuaciones estructurales para determinar que la concienciación de la seguridad de la información tuvo un impacto positivo en el cumplimiento de las políticas de seguridad de la información.

En Australia se estudió a través de un análisis cualitativo, exploratorio, de una indagación que tuvo como objetivo evaluar la efectividad de diversos programas de sensibilización y concienciación de la seguridad de la información, realizaron tres sesiones de concientización sobre seguridad de la información utilizando métodos de entrega basados en texto, juegos y video, empleando una muestra de 60 participantes, basándose en experiencias metodológicas, obteniendo como resultado que la capacitación en la concientización sobre la seguridad de la información es un medio poderoso para que los empleados cumplan con las políticas de seguridad de la información Abawajy (2014).

2.2.3. *Variable V3 Sanciones Formales de Disuasión.*

Teorías y Definiciones de la variable Sanciones Formales de Disuasión.

De nuevo se describen las teorías, así como las definiciones revisadas en la literatura, las cuales dan soporte a la variable independiente Sanciones formales de disuasión haciendo mención inicialmente de la Teoría de la disuasión general la cual Gibbs (1975) postula que, a mayor certeza, severidad y celeridad del castigo, menor tasa de delito.

El aspecto más importante de la Teoría de la Disuasión General es la idea de que los delincuentes potenciales se ven disuadidos de cometer delitos cuando perciben la amenaza de un castigo rápido, seguro y severo. Esta teoría postula que el miedo a enfrentarse a un castigo sirve como elemento disuasorio para los individuos que se plantean participar en conductas delictivas. Entre los autores que han contribuido al desarrollo y la articulación de la teoría general de la disuasión se incluyen:

Cesare Beccaria: Criminólogo y filósofo italiano, Beccaria suele ser considerado una de las figuras fundadoras de la escuela clásica de criminología. Su obra "Sobre los delitos y las penas" (1764) sentó las bases de la teoría general de la disuasión al hacer hincapié en la importancia de los castigos proporcionados y determinados para disuadir a los posibles delincuentes.

Jeremy Bentham: Filósofo y reformador social inglés, las ideas de Bentham sobre el utilitarismo y su concepto del diseño carcelario del "panóptico" contribuyeron al desarrollo de la teoría de la disuasión. Su énfasis en el cálculo racional del placer y el dolor influyó en los debates sobre la eficacia del castigo como elemento disuasorio.

Gary S. Becker: Economista estadounidense, Becker extendió el concepto de disuasión al ámbito del análisis económico. En su obra "Crime and Punishment: An Economic Approach" (1968), aplicó principios económicos para explicar el comportamiento delictivo y argumentó que los delincuentes potenciales toman decisiones racionales basadas en los costes y beneficios esperados de cometer un delito. Estos autores, entre otros, han dado forma a la teoría general de la disuasión aportando marcos teóricos, pruebas empíricas y conocimientos sobre los factores que influyen en la eficacia de la disuasión para prevenir el comportamiento delictivo (Gibbs, 1975).

En igual forma se define a las sanciones formales de disuasión las cuales se relacionan con el convencimiento y rigor de las sanciones percibidas por los empleados impuestas por una organización por el uso indebido o no autorizado de TI. (D'Arcy & Herath, 2011).

Según Trajtenberg y Aloisio (2009) las sanciones formales de disuasión "pueden ser de dos tipos, específica y genérica, donde en la primera, los individuos que cometen un delito y son detectados y castigados, se ven disuadidos de reincidir, la segunda cuando el castigo de los ofensores desestimula el involucramiento de nuevos sujetos en actividades criminales".

Las sanciones formales de disuasión influyen en el comportamiento ilícito con base en tres aspectos, la sanción formal e informal, detección y ejecución (Montesdeoca & Gonzaga, 2018).

Con base a la literatura revisada el concepto que se utiliza para esta investigación es el siguiente: Sanciones formales de disuasión se define como la percepción de los empleados al castigo impuesto por la organización a la violación de la política de seguridad de la información.

Investigaciones Aplicadas de la variable independiente (Sanciones Formales de Disuasión)

En Ecuador Montesdeoca y Gonzaga (2018) realizaron una investigación cuantitativa para determinar los factores que influyen en la intención del cumplimiento de las políticas de seguridad de la información en su país, utilizando una muestra de 592 participantes analizaron los datos a través de ecuaciones estructurales donde determinaron que las sanciones formales de disuasión inciden ciertamente en el cumplimiento de las políticas de seguridad de la información.

Se realizó una investigación cuantitativa en China donde se aplicaron ecuaciones estructurales a una muestra de 207 sujetos donde se determinó que las sanciones formales de disuasión son efectivas en el cumplimiento de las

políticas de seguridad de la información acompañadas de una motivación intrínseca (Hu et al., 2011).

Por otro lado, se realizó en Estados Unidos un estudio cuantitativo donde se aplicaron ecuaciones estructurales a una muestra de 312 sujetos en el cual probaron empíricamente su modelo teórico de los efectos incentivadores de las sanciones, presiones y efectividad de los empleados en el cumplimento de las políticas de seguridad de la información, teniendo como resultado que las sanciones formales de disuasión tienen un impacto positivo (Herath & Rao, 2009).

2.2.4. *Variable V4 Sanciones Informales de Disuasión.*

Teorías y Definiciones de la variable Sanciones Informales de Disuasión.

Teoría de la disuasión general en su versión clásica de la teoría de disuasión se enfocó en sanciones formales (legales) y estableció que a mayor la convicción y rigor de las sanciones por un acto indebido, mayor será la disuasión hacia cometer el acto (Gibbs, 1975).

Así mismo el aspecto más importante de la Teoría de la Disuasión General es la idea de que los delincuentes potenciales se ven disuadidos de cometer delitos cuando perciben la amenaza de un castigo rápido, seguro y severo. Esta teoría postula que el miedo a enfrentarse a un castigo sirve como elemento disuasorio para los individuos que se plantean participar en conductas delictivas. Entre los autores que han contribuido al desarrollo y la articulación de la teoría general de la disuasión se incluyen:

Cesare Beccaria: Criminólogo y filósofo italiano, Beccaria suele ser considerado una de las figuras fundadoras de la escuela clásica de criminología. Su obra "Sobre los delitos y las penas" (1764) sentó las bases de la teoría general de la disuasión al hacer hincapié en la importancia de los castigos proporcionados y determinados para disuadir a los posibles delincuentes.

Jeremy Bentham: Filósofo y reformador social inglés, las ideas de Bentham sobre el utilitarismo y su concepto del diseño carcelario del "panóptico" contribuyeron al desarrollo de la teoría de la disuasión. Su énfasis en el cálculo

racional del placer y el dolor influyó en los debates sobre la eficacia del castigo como elemento disuasorio.

Gary S. Becker: Economista estadounidense, Becker extendió el concepto de disuasión al ámbito del análisis económico. En su obra "Crime and Punishment: An Economic Approach" (1968), aplicó principios económicos para explicar el comportamiento delictivo y argumentó que los delincuentes potenciales toman decisiones racionales basadas en los costes y beneficios esperados de cometer un delito. Estos autores, entre otros, han dado forma a la teoría general de la disuasión aportando marcos teóricos, pruebas empíricas y conocimientos sobre los factores que influyen en la eficacia de la disuasión para prevenir el comportamiento delictivo (Gibbs, 1975).

Así mismo La parte más importante de la Teoría de la Disuasión Contemporánea gira en torno al concepto de estrategias de disuasión creíbles y eficaces en el mundo moderno. Esta teoría hace hincapié en que una postura de disuasión fuerte puede evitar que los adversarios emprendan acciones agresivas haciendo que los costes potenciales superen los beneficios percibidos. Implica una combinación de capacidades militares, determinación política y estrategias de comunicación para transmitir la intención y la capacidad de responder enérgicamente a una agresión (Thomas, 1960).

Entre los autores que han contribuido significativamente a la teoría de la disuasión contemporánea se encuentran: Thomas C. Schelling: El trabajo de Schelling, especialmente en su libro "The Strategy of Conflict" (1960), sentó las bases para la comprensión moderna de la disuasión. Introdujo el concepto de "amenaza que deja algo al azar", según el cual la ambigüedad y la imprevisibilidad de la respuesta podían influir en la toma de decisiones del adversario. Herman Kahn: La influyente obra de Kahn, como "Thinking About the Unthinkable" (1962), exploró varios escenarios de guerra nuclear y escalada. Introdujo el concepto de "dominio de la escalada", que se refiere a la capacidad de una nación para controlar y gestionar la escalada de los conflictos.

Con base en la misma forma se define el concepto de sanciones informales de disuasión según D'Arcy y Devaraj (2012) quienes adoptaron como marco teórico la teoría de disuasión contemporánea, la cual integró las sanciones informales a la Teoría de disuasión general y la Teoría del comportamiento planificado.

Las sanciones informales de disuasión influyen en el comportamiento ilícito con base en tres aspectos, la sanción formal e informal, detección y ejecución (Montesdeoca & Gonzaga, 2018).

Johnston et al. (2015) definen a las sanciones informales de disuasión, cuando se refieren a la dureza y la inevitabilidad, respectivamente, de las sanciones impuestas por amigos o un grupo de pares debido a violaciones de la política de seguridad de la información.

Con base a la literatura revisada el concepto que se utiliza para esta investigación es el siguiente: Sanciones informales de disuasión se define como la severidad con la que percibe el empleado el daño a su reputación determinado por los compañeros de trabajo o amistades por causa de un comportamiento ilícito.

Investigaciones Aplicadas de la variable independiente (Sanciones Informales de Disuasión)

Johnston et al. (2015) desarrollaron un estudio cuantitativo en Finlandia con ecuaciones estructurales en una muestra de 559 participantes se constató que la gravedad de las sanciones informales y la certeza de las sanciones informales de disuasión, fueron significativas en sus funciones como determinantes directos de la intención de cumplimiento de los empleados en las políticas de seguridad de la información.

Herath y Rao (2009) realizaron en Estados Unidos una investigación cuantitativa por medio de ecuaciones estructurales, desarrollando un modelo de protección, motivación y disuasión en el cumplimiento de la política de seguridad

de la información, además avaluaron el efecto del compromiso organizacional sobre las intenciones de los empleados en el cumplimiento de la seguridad, en una muestra de 312 participantes donde se determinó que la disuasión a través de la sanción informal tiene un impacto positivo en la intención de del cumplimento de la política de seguridad de la información.

Hovav y D'Arcy (2012) llevaron a cabo una investigación cuantitativa con ecuaciones estructurales, donde realizaron una comparación entre Estados Unidos y Corea haciendo la misma investigación con una muestra de 360 participantes en ambos países para ver si la cultura influía en las capacidades disuasorias de las políticas de seguridad obteniendo como resultado que en ambas partes fue significativa la sanción informal de disuasión para el cumplimiento de las políticas de seguridad de la información.

2.2.5. *Variable V5 Contexto Laboral.*

Teorías y Definiciones de la variable Contexto Laboral.

La variable Contexto laboral explicada a través de la Teoría del comportamiento planificado, se basa en afirmaciones de control: éstas son creencias sobre la representación de componentes que pueden suministrar, o pueden reprimir, el desempeño de un comportamiento, (Aurigemma & Panko, 2012; Hu et al., 2012). La Teoría del Comportamiento Planificado propone que la intención de un individuo de realizar una conducta está influida por sus actitudes hacia la conducta, las normas subjetivas y el control conductual percibido. Estas intenciones, a su vez, predicen el comportamiento real, aunque también pueden influir factores externos. La TCP proporciona un marco estructurado para comprender y predecir el comportamiento humano, lo que la hace valiosa para diseñar intervenciones y estrategias que fomenten o desincentiven acciones específicas. Y la Teoría de la Acción razonada, que son las creencias que una persona tiene acerca del comportamiento que va a realizar y que influyen en su actitud hacia ese comportamiento. Por otro lado, esas creencias normativas influyen en la norma subjetiva de la persona. (Ajzen, 1991).

De acuerdo con lo anterior la Teoría del Comportamiento Planificado la cual es una teoría de psicología social ampliamente utilizada que explica y predice el comportamiento humano basándose en las actitudes individuales, las normas sociales y el control conductual percibido. Desarrollada por Icek Ajzen, la TCP amplía la anterior Teoría de la Acción Razonada (TAR) al incluir el elemento del control conductual percibido. La TCP postula que estos tres factores -actitud, norma subjetiva y control conductual percibido- interactúan para influir en la intención de una persona de realizar un comportamiento específico, lo que a su vez predice el comportamiento real. La teoría es particularmente útil para comprender y predecir el comportamiento guiado por la conciencia e implica cierto grado de conciencia. TCP se ha utilizado en diversos campos, como la salud, el medio ambiente, el marketing, el comportamiento organizacional (Aurigemma & Panko, 2012; Hu et al., 2012).

Así mismo se desglosan los componentes de la Teoría del Comportamiento Planificado. Creencias conductuales: Creencias sobre los resultados asociados con la realización del comportamiento. Evaluación de resultados: una evaluación individual de la conveniencia o el valor de esos resultados. Fuerza de la actitud: una evaluación general de la fuerza que influye en la influencia de las actitudes en las intenciones.

Las normas subjetivas reflejan presiones sociales percibidas o expectativas de comportamiento. Si una persona significativa aprueba o desaprueba una actividad es una cuestión de opinión. Las normas subjetivas constan de dos componentes:

Creencias normativas: Creencias sobre lo que otros piensan o esperan sobre el comportamiento. Motivación de conformidad: la motivación de un individuo es ajustarse a las expectativas percibidas de los demás.

Control conductual percibido (CCP): El control conductual percibido se refiere a la percepción del individuo sobre la facilidad o dificultad de realizar la conducta. Incorpora factores internos y externos que pueden facilitar o dificultar la conducta. El CCP incluye dos componentes:

Creencias de control: Creencias sobre los factores que pueden facilitar o dificultar la conducta.

Poder Percibido: Percepción del individuo sobre el grado de control que tiene sobre estos factores facilitadores u obstaculizadores.

Intención de comportamiento (BI): La intención de comportamiento es la intención o motivación de un individuo para realizar un determinado comportamiento. Está influenciado por actitudes, normas subjetivas y control conductual percibido. Las intenciones pueden predecir directamente el comportamiento real.

Comportamiento real: Aunque la teoría del comportamiento planificado se centra en la predicción de las intenciones, asume que las intenciones son fuertes predictores del comportamiento real. Sin embargo, la TCP reconoce que los factores externos y las circunstancias imprevistas pueden influir en la transformación de la intención en conducta (Ajzen, 1991).

A continuación, se define el Contexto laboral el cual se refiere al argumento contiguo de ocupación y a las peculiaridades del trabajo (D'Arcy & Devaraj, 2012).

Con base a la literatura revisada el concepto que se utiliza para esta investigación es el siguiente: Contexto laboral se refiere al entorno físico, situacional cultural de un empleo y sus características

Investigaciones Aplicadas de la variable independiente (Contexto Laboral)

Se realizó una investigación cuantitativa en Estados Unidos donde se aplicó una regresión múltiple en una muestra de 411 participantes donde determinaron que la influencia del contexto laboral cuando los empleados trabajan de manera remota no hace mal uso de la tecnología ni de la información de la empresa, cuando tienen un cargo de gerencia, siendo más propensos a cumplir con las políticas de seguridad (D'Arcy & Devaraj, 2012).

En Perú se realizó una investigación cuantitativa con una muestra de 110 sujetos utilizando el método estadístico de regresión múltiple donde se determinó que el contexto laboral influye positivamente en el cumplimiento de las políticas de seguridad de la información (Celi & Díaz, 2017).

Wiesenfeld et al., (1999) realizaron un estudio cuantitativo a través de regresión múltiple en Estados Unidos utilizando una muestra de 276 participantes donde evaluaron y determinaron en sus resultados que la variable contexto laboral salió significativa.

2.3. Hipótesis Específicas

En la investigación con una orientación positivista, mayoritariamente cuantitativo, las hipótesis son esclarecimientos preliminares relacionadas con el problema en cuestión. Son enunciados en forma de suposiciones a través de oraciones narrativas que se someten a comprobación empírica y vinculan lo que ya se sabe con lo que se busca.

H1= La percepción de la participación de la dirección se relaciona con el cumplimiento de las prácticas de seguridad de TI por parte de los empleados.

H2= La concientización de la seguridad de TI se relaciona con el cumplimiento de las prácticas de seguridad de TI por parte de los empleados.

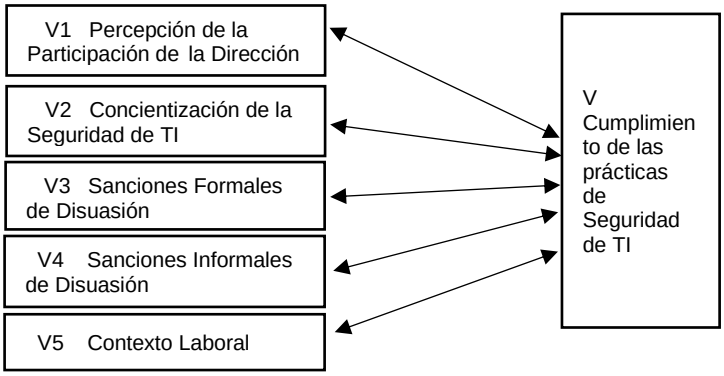
H3= Las sanciones formales de disuasión se relaciona con el cumplimiento de las prácticas de seguridad de TI por parte de los empleados.

H4= La sanciones informales de disuasión se relaciona con el cumplimiento de las prácticas de seguridad de TI por parte de los empleados.

H5= El contexto laboral se relaciona con el cumplimiento de las prácticas de seguridad de TI por parte de los empleados.

2.3.1. Modelo Gráfico de la Hipótesis

Figura 2. Modelo Gráfico de Variables.



2.3.2. Modelo de Relaciones teóricas con las Hipótesis

En la tabla 4 se observa la relación estructural de las hipótesis con respecto al marco teórico de este estudio.

Tabla 4. Tabla de Relación Estructural Hipótesis - Marco Teórico

Referencia	V1	X2	X3	X4	X5	Y
Abawajy (2014).		X				X
Bulguru et al. (2010).		X	X			X
Celi y Díaz (2017).		X	X		X	X
Herath y Rao (2009).			X	X		X
Herath y Rao (2009).			X	X		X
Hovav & D'Arcy (2012).			X	X		X
Hu et al. (2012)	X					X
Hu et al. (2011).	X		X			X
Ifinedo (2016).	X		X		X	X
Johnstonet al. (2015).			X	X		X
Montesdeoca Vásquez et al. (2018).		X	X			X
Johnston y Warkentin (2010)	X					X
Rueda et al. (2013).						X
Shaw (2012)	X					X
Siponen et al. (2014)			X			X
Wiesenfeld et al. (1999).					X	X
Willison y Warkentin (2013)			X			X

En este capítulo se examinaron estudios realizados donde se investigó el impacto de las variables independientes del estudio sobre la intención de los empleados en cumplir con las prácticas de seguridad de TI la cual es la variable dependiente, proporcionando evidencia de los factores que se relacionan con los empleados para cumplir con las prácticas de seguridad de TI.

En el siguiente capítulo se describirá la metodología, el diseño de la investigación, del instrumento de investigación, descripción de la muestra, recopilación de los datos y su análisis estadístico con un enfoque cuantitativo.

Capítulo 3. ESTRATEGIA METODOLÓGICA

3.1. Tipo y diseño de la investigación

Este capítulo describe la metodología utilizada durante el estudio para recopilar datos de acuerdo con un enfoque cuantitativo para lograr los objetivos de este estudio. A continuación, se describe el tipo y diseño del estudio, así como el método e instrumento de recolección de datos, la población examinada y la muestra.

3.1.1. *Tipos de Investigación*

De acuerdo con Hernández et al. (2010) el diseño del estudio, dentro de la metodología de la investigación, es el método que se lleva a cabo para la obtención de la información requerida en una investigación. El enfoque de la presente tesis es cuantitativo ya que se utiliza la recaudación y el análisis de los datos para argumentar a las cuestiones de investigación, así como probar las hipótesis planteadas, utilizando el análisis estadístico.

Con respecto a los alcances de la investigación, el exploratorio es aquel que investiga fenómenos poco estudiados, de los cuales se tienen dudas o bien no se han abordado, este alcance es la base para estudios más amplios o profundos. El tipo descriptivo se caracteriza por aclarar propiedades, características de conceptos, variables, hechos, etc. En este contexto, muestran y cuantifican las dimensiones del fenómeno. Los estudios correlacionales tienen como finalidad conocer el grado de relación que existe entre dos o más conceptos, variables, etc. en un contexto dado, y su característica es que permiten cierto grado de predicción. En cuanto al alcance causal o explicativo, son aquellos que están altamente estructurados ya que su objetivo es determinar la causa de los fenómenos, conceptos, variables, o problemas estudiados, crean un sentido de entendimiento y explicación (Hernández & Mendoza, 2018). Esta investigación cuantitativa causal tiene como objetivo someter a prueba las hipótesis establecidas y responder la pregunta de investigación, el estudio es no experimental ya que no se manipulan deliberadamente las variables.

3.1.2. *Diseño de la Investigación*

El diseño de investigación es la estrategia que se desarrolla para obtener información con la finalidad de responder de manera satisfactoria el planteamiento del problema (Hernández & Mendoza, 2018).

El diseño de esta investigación de campo es no experimental, transeccional, explicativo ya que se pretende proporcionar información acerca de la existencia de una relación entre las variables asociadas con la incidencia en los empleados en cumplir con las prácticas de seguridad de TI.

El estudio es no experimental ya que no se manipulan intencionadamente las variables, observando únicamente el fenómeno estudiado en su ambiente natural para posteriormente analizarlo con el objetivo de someter a prueba las hipótesis establecidas y responder la pregunta de investigación. Es transversal en el sentido de que los datos se recopilan en un punto a través de la encuesta como herramienta de medición; Correlación-causal cuando se describen relaciones entre dos o más variables en términos correlativos o causales (Hernández & Mendoza, 2018).

3.2. Métodos de recolección de datos

Para la realización de la investigación, así como el trabajo de campo, se utilizó una encuesta, la cual en parte está conformada por un instrumento ya validado y otra parte por ítems construidos por quien realiza este estudio, la encuesta está adaptada al contexto del objeto de estudio para la prueba piloto y posteriormente para la muestra final.

Para tener acceso a la aplicación del instrumento a la muestra determinada, se solicitó la autorización previa de las tres IES más grandes de México, donde se les notificó que la recolección de los datos es para una investigación académica, a la cual tendrán acceso a los resultados de esta, así como especificar la confidencialidad de la información de los empleados y el

anonimato de sus respuestas. La información se recopiló de manera electrónica y en un período de seis meses en 2022.

Para la recolección de los datos se utilizó la técnica de muestreo no probabilístico por conveniencia, para captar el mayor número de participantes, por la proximidad, fácil acceso, sencillez, a las cuales se les envió la liga de acceso a la encuesta electrónica en *Google Forms* a través de correo electrónico. En la invitación se les hizo llegar la carta informativa explicando el propósito del estudio, mostrando que la participación será completamente voluntaria, anónima y confidencial.

Una vez recopilados los datos a través de la encuesta electrónica, solo la investigadora y sus directores de tesis tendrán acceso a los mismos antes de ser procesados, protegiendo de esta forma la identidad, la privacidad y la confidencialidad de los participantes.

Validez del instrumento: De acuerdo con Hernández et al. (2018), la validez de un instrumento de medición se evalúa sobre la base de todos los tipos de evidencia. La validez total es la suma de la validez de contenido, la validez de criterio y la validez de constructo. Así como es un requisito que el instrumento de medición demuestre ser válido y confiable. Es válido cuando mide lo que se pretende medir y es confiable si es consistente con los resultados que produce.

Validez de contenido: “grado en que un instrumento refleja un dominio específico de contenido de la variable que se mide” (Hernández et al. 2018). La validez de contenido ha sido evaluada a través de la revisión de la literatura, donde se estudió como habían sido medidas las variables por otros investigadores en estudios similares. En esta investigación se incorporaron variables que fueron medidas y analizadas tanto cuantitativamente como estadísticamente con otros constructos en otros estudios realizados por Bulguru et al., (2010); D’Arcy y Devaraj (2012); Hu et al., (2012).

Como parte de la validez de contenido, se envió por correo electrónico, el instrumento y una carta informativa a un panel de tres expertos para invitarlos a

ser parte del grupo evaluador, los cuales deben contar con el grado de PhD. Se elaboró una plantilla para la evaluación por parte de los expertos, esta contiene todos los ítems de la encuesta; se le solicitó al panel completar la plantilla, donde deberá ubicar los ítems en cada constructo según la definición proporcionada.

Confiabilidad del instrumento: Se evaluó la confiabilidad del instrumento poniendo a prueba la encuesta, a un grupo piloto con un número de participantes representativo de la población, con la finalidad de evaluar el proceso de recolección de los datos y conocer la opinión de los participantes. Para medir la consistencia interna del instrumento, se realizó el análisis del Alfa de Cronbach. Este coeficiente es comúnmente utilizado para determinar la confiabilidad de las escalas compuestas por varios ítems (Hernández & Mendoza, 2018). El Alfa de Cronbach indica si los diferentes ítems utilizados en la escala convergen, sirviendo esto como un indicador de calidad de la escala. Entre más cercano esté el valor del Alfa de Cronbach a uno, mayor será la confiabilidad de que los ítems de la escala del instrumento midan lo que tienen que medir; de tal manera de que un coeficiente de Alfa de Cronbach tenga un valor igual o mayor de 0.70 se considera suficiente para avalar una escala confiable. (Zikmund et al., 2010).

3.2.1. *Elaboración del Instrumento*

Para la recolección de los datos se elaboró un cuestionario para la investigación y someter a prueba las hipótesis por medio de este. La encuesta fue diseñada con base en los constructos y variables utilizados en investigaciones similares elaboradas por Bulguru et al. (2010); D'Arcy y Devaraj (2012); Hu et al. (2012) resultado de la consulta de fuentes de información como, tesis, artículos científicos. Los ítems fueron revisados, traducidos al español y adaptados para incluirlos en el instrumento de medición para esta investigación.

De esta manera se creó una encuesta estructurada, la cual está integrada por 38 ítems dividido en siete secciones, la primera parte está conformada por los datos demográficos y laborales de la encuesta con 7 ítems, de la 1 a la 7; la segunda parte con 5 ítems a la variable dependiente Y Intención de los empleados en cumplir con las prácticas de seguridad de TI con las preguntas de la 8 a la 12, la tercera sección con 7 ítems relacionados con la variable X1

Percepción y Participación de la Gerencia de la 13 a la 19, la cuarta sección con la variable X2 Concientización de la seguridad de TI con 3 ítems de la 20 a la 22, la quinta parte de cuestionario con la X3 Sanciones Formales de Disuasión con 4 ítems de la 23 a la 26, la sexta sección para evaluar con X4 Sanciones Informales de Disuasión integrando 7 ítems de la 27 a la 33, y la séptima sección relacionada con X5 Contexto laboral con 5 ítems de la 34 a la 38 como se muestra en la tabla 3. Se utiliza una escala de Likert de cinco puntos que van desde 1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre, 5= Siempre.

Tabla 5. Estructura de la encuesta

Sección	Descripción
Primera parte	Información demográfica
Segunda parte	Intención
Tercera parte	Percepción de la participación de la gerencia
Cuarta parte	Concientización de la seguridad de TI
Quinta parte	Sanciones Formales de Disuasión
Sexta parte	Sanciones Informales de Disuasión
Séptima parte	Contexto laboral

3.2.2. *Operacionalización de las variables de la hipótesis*

En la tabla 6 se muestra la operacionalización de las variables de la hipótesis de estudio.

Tabla 6. Variables de Investigación e Indicadores de Gestión

Variable	Definición	Unidad de Medición
V_1 Percepción y Participación de la Gerencia	Hu et al., (2011) precisa que la equidad y la justicia implican que los empleados perciban que la gerencia practica justicia y equidad al establecer, definir y hacer cumplir las prácticas de seguridad de TI	Escala Likert 1.-Nunca 2.-Casi nunca 3.- A veces 4.- Casi siempre 5.- Siempre Alpha de Cronbach de 0.867
V_2 Concientización de la Seguridad de TI	Son los conocimientos generales de un empleado sobre seguridad de la información y su conocimiento de las prácticas de seguridad de TI de su organización (Bulguru et al., 2010).	Escala Likert 1.-Nunca 2.-Casi nunca 3.- A veces 4.- Casi siempre 5.- Siempre Alpha de Cronbach de 0.862
V_3 Sanciones Formales de Disuasión	Disuasión “se refieren a la certeza y la gravedad percibidas por los empleados, de las sanciones impuestas por la organización por el mal uso, o uso no autorizado de las TI” (D’Arcy & Herath, 2011).	Escala Likert 1.-Nunca 2.-Casi nunca 3.- A veces 4.- Casi siempre 5.- Siempre Alpha de Cronbach de 0.857
V_4 Sanciones Informales de Disuasión	Se refieren a “los costos sociales y autoimpuestos por los empleados, tomados en consideración por estos antes de tomar decisiones de no cumplir con las prácticas de seguridad de TI” (D’Arcy & Devaraj, 2012; Hu et al.,	Escala Likert 1.-Nunca 2.-Casi nunca 3.- A veces 4.- Casi siempre 5.- Siempre Alpha de Cronbach de 0.775

	2012)	
Variable	Definición	Unidad de Medición
V_5 Contexto Laboral.	se refiere al “contexto Inmediato de empleo y a las características del trabajo” (D’Arcy & Devaraj, 2012).	Escala Likert 1.-Nunca 2.-Casi nunca 3.- A veces 4.- Casi siempre 5.- Siempre Alpha de Cronbach de 0.858
V Intención de los empleados en cumplir con las prácticas de Seguridad de TI	El comportamiento de seguridad de la información conforme se refiere al conjunto de actividades de seguridad de la información centrales que los usuarios finales deben cumplir para mantener la seguridad de la información según lo definido por las políticas de la seguridad de la información (Ifinedo, 2016).	Escala Likert 1.-Nunca 2.-Casi nunca 3.- A veces 4.- Casi siempre 5.- Siempre Alpha de Cronbach de 0.908

3.3. Población, marco muestral y muestra

La población de esencia del estudio de esta exploración, son todos los empleados que pertenecen al departamento de sistemas, los cuales trabajan con tecnologías de información, como parte de su trabajo diario y que pertenecen a las tres IES públicas más grandes de México, ubicadas una de ellas en el estado de Nuevo León, otra en el estado de México, y la última en el estado de Jalisco.

Para el marco muestral, según UNAM (2021) la página electrónica oficial de la IES de la ciudad de México en su directorio de escuelas y facultades de la entidad se cuenta con veinte facultades, así mismo la universidad ubicada en Nuevo León en su página virtual oficial, se cuenta con veintisiete facultades en esta institución (UANL, 2021), por otra parte, la de Jalisco de igual forma en su sitio electrónico oficial cuentan con quince facultades según el directorio de la institución de educación superior (Guadalajara, 2021), dando un total de sesenta

y dos facultades, con un promedio de cinco empleados en el área de tecnologías de información.

3.3.1. *Tamaño de la muestra*

El muestreo fue no probabilístico (a conveniencia) para la elección de los elementos de la muestra, ya que se desconoce la lista completa de los trabajadores que forman la población, por lo que no se tiene la misma posibilidad de ser elegidos de manera aleatoria. Acorde con Hernández y Mendoza (2018) en el muestreo probabilístico, la elección de las unidades depende de los conocimientos afines con las particularidades y el contexto del estudio.

Se utilizó una muestra estratificada dividiendo la población en segmentos para posteriormente seleccionar una muestra por cada estrato (Hernández et al., 2018), ya que cada IES cuenta con un número distinto de dependencias. Teniendo así la IES de la ciudad de México veinte dependencias por cinco sujetos, la población del estrato es de cien, para la del estado de Nuevo León con veintisiete facultades por cinco empleados del área de sistemas da un total de ciento treinta y cinco trabajadores, la Institución de Educación Superior de Jalisco con quince por cinco personas laborando en el área, tenemos una población para el estrato de setenta y cinco sujetos.

Ecuación 1. Cálculo del tamaño de la muestra.

Conforme al tamaño de la población obtenida en promedio de 310 sujetos, con un nivel de confianza del 95% (1.96), un margen de error del 5% (0.05), con el nivel de porcentaje estimado de la muestra del 50% (p= 0.5 y q= 0.5)

$$n = \frac{z^2 * p * q * N}{e^2(N-1) + Z^2 * p * q}$$

Donde:
N = 310
Z = 95% (1.96)
p = 50% (0.5)
q = 50% (0.5)
e = 5% (0.05)

Entonces:

$$n = \frac{(1.96)^2 * .5 * .5 * 310}{(.05)^2(310-1) + (1.96)^2 * .5 * .5}$$

$$n = \frac{297.724}{1.7329} = 171.8067$$

Ecuación 2. Cálculo del tamaño de la muestra estratificada.

Una vez teniendo el tamaño de la muestra general se obtiene la fracción constante para determinar la muestra para cada estrato de la población.
Ksh = fh = fracción constante.

$$ksh = \frac{nh}{Nh} \qquad ksh = \frac{171.8067}{310} = 0.5542$$

Tabla 7. Muestra estratificada

IES	Nh	nh
UANL	135	74.817
UNAM	100	55.420
U de G.	75	41.565

3.3.2. *Sujetos de estudio:*

La población objeto de estudio de esta investigación, son todos los empleados que pertenecen al departamento de sistemas, los cuales trabajan con tecnologías de información, como parte de su trabajo diario y que pertenecen a las tres IES públicas más grandes de México.

La muestra está formada por empleados de ambos géneros de las IES, entre los 21 y 65 años, los cuales trabajan con las tecnologías de información dentro o fuera de las instalaciones físicas de las instituciones, de tal manera que ellos tienen el conocimiento acerca de las prácticas de seguridad de TI, quienes son las personas idóneas para contestar la encuesta. La selección de la muestra principalmente se basa en la disponibilidad de los empleados que cumplan con los requisitos anteriormente descritos. Se excluyen a directores, gerentes, practicantes; se incluyen los mandos medios y empleados del área de TI.

3.4. Métodos de Análisis

Para esta investigación se pretende utilizar un análisis descriptivo utilizando frecuencias, medidas de tendencia central y de variabilidad, así como un método de análisis estadístico inferencial, como lo es el multivariante para medir las relaciones de las variables, análisis factorial para medir las dimensiones de las variables, se usó la regresión lineal múltiple porque estudiamos la posible relación entre varias variables independientes (predictoras o explicativas) y otra variable dependiente.

Los resultados que se obtengan de las encuestas se tabularon y se analizaron utilizando los programas de análisis estadístico *Statistical Package for the Social Sciences* (SPSS) versión 22. El primer análisis que se realizó fue un análisis descriptivo univariado utilizando frecuencias, porcentajes, medidas de tendencia central y dispersión. Después se realizó un análisis estadístico inferencial, como el análisis factorial para la medición de las dimensiones de las variables, así como el multivariante para medir las relaciones entre las variables.

Se aplicó el análisis de regresión lineal multivariante para medir en conjunto las variables de estudio; utilizando la herramienta de SPSS versión 22. En esta investigación se trabajan con variables no observables como: Percepción de la participación de la dirección, concientización de la seguridad de TI, sanciones formales de disuasión, sanciones informales de disuasión, e intención de los empleados en cumplir con las prácticas de seguridad de TI.

A los datos obtenidos en la prueba piloto se les realizó el análisis Alpha de Cronbach con el software SPSS para medir la consistencia del instrumento, el cual es frecuentemente utilizado para determinar la confiabilidad de las escalas compuestas de múltiples ítems (Hernández et al., 2018).

Luego se realizó un análisis descriptivo univariado utilizando frecuencias, medidas de tendencia central y variabilidad de variables, con la primera sección dedicada al perfil del encuestado y la segunda sección al perfil de la encuesta.

Se utilizó un método de análisis estadístico inferencial, como lo es el multivariante para medir las relaciones de las variables.

Se evaluó la validez convergente para ver si un conjunto de indicadores realmente mide un constructo determinado (*Average Variance Extracted* - AVE).

Se realizó la prueba de la colinealidad. La colinealidad se refiere a la independencia de las variables predictoras, lo que suele ocurrir en el análisis de regresión. (Dormann et al.,2013). Para evitar el problema de colinealidad, como regla general, se debe tener un factor de inflación de la varianza (*Variance Inflation Factor* – VIF).

En el capítulo fueron descritos la metodología para la recolección de los datos y su análisis, la muestra, el instrumento, la validación del instrumento, el diseño del estudio el cual es una investigación cuantitativa, no experimental transversal, correlacional.

Capítulo 4. ANÁLISIS DE RESULTADOS Y DISCUSIÓN

4.1. Prueba piloto

Para evaluar la consistencia interna del instrumento, se realizó el análisis de Alpha de Cronbach, el cual es usado comúnmente para determinar la confiabilidad de escalas compuestas de múltiples ítems (Hernández et al., 2018).

Se realizó una prueba piloto consistente de 20 encuestas para comprobar la confiabilidad del instrumento a aplicar, lo que permite corroborar, así como modificar preguntas en el caso en que los valores obtenidos sean menores a 0.700. Obteniendo un Alpha general de 0.912, como se muestra en la tabla 8

Tabla 8. Alpha de Cronbach.

Variable	Resultados
V_1 Percepción de la participación de la Gerencia	0.750
V_2 Concientización de la Seguridad de TI	0.832
V_3 Sanciones Formales de Disuasión	0.826
V_4 Sanciones Informales de Disuasión	0.700
V_5 Contexto Laboral	0.807
V Intención de los empleados en cumplir con las prácticas de Seguridad de TI	0.911

Con base a los resultados se eliminó el ítem 26 correspondiente a la variable Sanciones Formales de Disuasión ya que resultó negativa mejorando el Alpha de Cronbach de 0.657 a 0.826.

4.2. Resultados

4.2.1. *Estadística descriptiva*

El instrumento recopiló datos relacionados a los constructos del modelo de investigación sugerida y también de otras variables relacionadas a la intención de los empleados en cumplir con las prácticas de seguridad de TI.

Estas variables fueron: demográficas de los participantes, posición en la Institución de Educación Superior donde trabajan, tiempo que llevaba laborando

en la institución y si trabajaba en el departamento de TI. A continuación, se describen los datos recopilados de los 182 participantes.

Datos demográficos. Las variables que se obtuvieron de los participantes en esta investigación fueron: Edad, Género, Escolaridad, Posición en la Institución, Años laborando y si trabaja en el departamento de TI.

Edad: en la tabla 9 se observa el resultado de los 182 participantes, donde se observa que la tendencia es que la mayoría oscila en un rango de edad entre los 21 a 30 años.

Tabla 9. *Distribución de la muestra por rango de edad.*

Edad	Frecuencias	% del Total	% Acumulado
21 a 30 años	125	68.7 %	68.7 %
31 a 40 años	42	23.1 %	91.8 %
41 a 50 años	15	8.2 %	100.0 %

Como se observa en la tabla 10 el género que predomina es el masculino con el 73.6% de los encuestados para este estudio.

Tabla 10. *Distribución por Género.*

Genero	Frecuencias	% del Total	% Acumulado
Masculino	134	73.6 %	73.6 %
Femenino	48	26.4 %	100.0 %

Con respecto a la escolaridad, como se muestra en la tabla 11, la mayoría cuenta con grado de licenciatura.

Tabla 11. Escolaridad**.**

Escolaridad	Frecuencias	% del Total	% Acumulado
Licenciatura	132	72.5 %	72.5 %
Maestría	50	27.5 %	100.0 %

En la tabla 12, se observa que casi el 90% de las personas encuestadas son solteras, lo cual es lógico ya que la mayoría oscila entre los 21 a 30 años.

Tabla 12. Estado Civil.

Estado civil	Frecuencias	% del Total	% Acumulado
Casado/a	18	9.9 %	9.9 %
Soltero/a	162	89.0 %	98.9 %
Otro	2	1.1 %	100.0 %

Se observa en la tabla 13 que la mayoría de las personas que laboran en el área de TI cuentan con una categoría de empleado como puesto dentro de la institución.

Tabla 13. Posición en la Institución de Educación Superior.

Posición en la Institución de Educación Superior	Frecuencias	% del Total	% Acumulado
Responsable del área de TI	30	16.5 %	16.5 %
Empleado del área de TI	152	83.5 %	100.0 %

El tiempo que los encuestados llevan laborando en las IES, como se muestra en la tabla 14, el 70% oscila entre uno y diez años de antigüedad.

Tabla 14. Indique los años que lleva trabajando en la institución de educación superior.

Indique los años que lleva trabajando en la institución de educación superior	Frecuencias	% del Total	% Acumulado
Menos de 1 año	24	13.2 %	13.2 %
1 a 10 años	127	69.8 %	83.0 %
11 a 20 años	31	17.0 %	100.0 %

Como se puede apreciar en la tabla 15, todos los encuestados laboran en el área o departamento de TI de las IES a la que pertenecen.

Tabla 15. Trabaja usted en alguno de los siguientes departamentos informática.

Trabaja usted en alguno de los siguientes departamentos informáticos	Frecuencias	% del Total	% Acumulado
Sí	182	100.0 %	100.0 %

4.2.2. *Análisis estadístico Fiabilidad*

Se realizó el análisis estadístico de los datos con los resultados de los 182 casos obtenidos a través del sistema SPSS, iniciando con un análisis de fiabilidad obteniendo un Alpha de Cronbach general de 0.947, posteriormente se calculó el Alpha de cada una de las variables por medio del sistema SPSS versión 22 como se observa en la tabla 16.

Tabla 16. *Estadística de Fiabilidad.*

Variable	Alpha de Cronbach
V_1 Percepción de la participación de la Dirección	0.867
X_2 Concientización de la Seguridad de TI	0.862
X_3 Sanciones Formales de Disuasión	0.857
X_4 Sanciones Informales de Disuasión	0.775
X_5 Contexto Laboral	0.858
Y Cumplimiento de las prácticas de Seguridad de TI	0.908

En la tabla 17 se muestran los resultados de los cálculos de la media, desviación estándar y la población

Tabla 17. Media y Desviación estándar.

	Media	Desviación estándar	N
Cumplimiento de las prácticas de Seguridad de TI	19.5604	3.93934	182
Percepción de la Participación de la Dirección	23.2967	6.70531	182
Concientización de la Seguridad de TI	12.5165	2.48248	182
Sanciones Formales	16.1209	3.95928	182
Sanciones Informales	30.6813	4.72066	182
Contexto Laboral	19.6044	4.75796	182

4.2.3. *Prueba de Colinealidad*

La prueba de colinealidad mide la autonomía de las variables predictoras que se encuentran comúnmente en el análisis de regresión. (Dormann et al., 2013). Para que este problema de colinealidad no se presente, se debe tener un

factor de inflación de la varianza (*Variance Inflation Factor* – VIF) menor o igual a 5.0 y un nivel de tolerancia mayor o igual a 0.2 (Hair et al., 2014; Wong, 3013).

La prueba de colinealidad que se muestra en la tabla 18, se realizó con el programa SPSS, la cual muestra los índices de la VIF fluctúan entre 1.772 y 3.819; el nivel de tolerancia oscila entre 0.262 y 0.564. Los dos índices se localizan dentro de los parámetros aceptables.

Tabla 18. Factor de inflación de la Varianza.

Modelo	Estadística de Colinealidad	
	Tolerancia	VIF
Percepción de la participación de la Dirección	0.374	2.671
Concientización de la Seguridad de TI	0.298	3.355
Sanciones Formales	0.352	2.845
Sanciones Informales	0.564	1.772
Contexto Laboral	0.262	3.819

Nota: La variable dependiente es el Cumplimiento de las Prácticas de Seguridad de TI.

Posteriormente se realizó el análisis de la varianza extraída como se observa en la tabla 19 (*Average Variance Extracted* AVE), se consideran la varianza extraída media y las cargas externas de los indicadores para formar la validez convergente (Hair et al., 2014). Por lo general una variable latente debe explicar una parte importante de la varianza de cada indicador, por lo que el AVE debe ser mayor o igual a 0.50 (Chin, 1998; Hair et al., 2014). Por lo que todas las variables son mayores oscilando entre 0.63 y 0.92.

Tabla 19. *Varianza Extraída Media (AVE).*

Constructo	AVE
Cumplimiento de las prácticas de Seguridad de TI	0.702
Percepción de la Participación de la Dirección	0.877
Concientización de la Seguridad de TI	0.921
Sanciones Formales	0.716
Sanciones Informales	0.777
Contexto Laboral	0.639

Posteriormente se realizó el análisis de los componentes principales conocida como la prueba de esfericidad de Bartlett y la medida de adecuación muestral Kaiser – Meyer-Olkin (KMO), el análisis implica un procedimiento estadístico que mide las dimensiones de las variables y determina las dimensiones subyacentes de la medición (Karthwohl, 2009). Para determinar si el análisis de los factores fue estadísticamente correcto. La medida de KMO fue 0.783. Este valor es mejor cuanto más se acerca a 1.00 y el criterio de esfericidad de Bartlett fue 0.000, muestra que es inferior a 0.05, como se muestra en la tabla 18. Esto permitió confirmar que el estudio es válido para hacer el análisis de factores.

El análisis factorial se realiza exclusivamente en la muestra general a través de tres fases. Antes de realizar el primer análisis se tomaron en consideración algunos criterios para valorar la viabilidad de este, como se observa en los resultados de la prueba de esfericidad de Bartlett y el análisis de KMO los cuales indicaron que era pertinente un análisis factorial de la matriz de correlaciones (Visauta & Martori, 2005). Así mismo se efectuó una estimación de las comunalidades de los ítems que construyen la escala de positividad mediante el método de extracción denominado, máxima verosimilitud, y sus resultados se pueden observar en la tabla 20, así como el estadístico de la tabla 21 donde se muestra la varianza total explicada.

Tabla 20. Prueba de Kaiser-Meyer-Olkin (KMO) y Esfericidad de Bartlett.

Medida Kaiser-Meyer-Olkin de adecuación de muestreo		.783
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	782.644
	Gl	15
	Sig.	.000

Análisis Factorial

En la tabla 21, las comunalidades indican la cantidad de varianza en cada variable que se contabiliza, por el método de extracción a través del análisis de componentes principales.

Tabla 21. Comunalidades.

	Inicial	Extracción
V1_Participación de la Dirección	1.000	.693
V3_Sanciones Formales	1.000	.702
V5_Contexto Laboral	1.000	.447
V2_Concientizacion de la Seguridad	1.000	.752
V4_Sanciones Informales	1.000	.826

Nota: Método de extracción: análisis de componentes principales.

Como se observa las comunalidades iniciales son estimaciones de la varianza en cada variable contabilizada por todos los componentes o factores. Para la extracción de componentes principales, siempre es igual a 1.0 para los análisis de correlación. Si un valor es mayor a 0.50 o mayor se considera aceptable, más si un valor es mayor a 0.80, es considerado bueno (Salkind, 2012). De tal manera que los resultados se muestran entre .447 y .826.

En la tabla 22 se observa la varianza total explicada, la cual se usa para medir la discrepancia entre un modelo y los datos reales, es decir, es la parte de la varianza total del modelo que se explica por los factores que realmente están presentes y no se debe a la varianza del error. Entre más alto sea el porcentaje de la varianza explicada indica una mayor fuerza de asociación, lo que significa que se hacen mejores predicciones. (Rosenthal & Rosenthal, 2011).

Tabla 22. Varianza total explicada.

	Autovalores iniciales			Sumas de extracción de cargas al cuadrado			Sumas de rotación de cargas al cuadrado		
Componente	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	3.919	65.324	65.324	3.919	65.324	65.324	1.195	19.919	19.919
2	1.054	17.569	82.894	1.054	17.569	82.894	1.191	19.844	39.763
3	.447	7.449	90.343	.447	7.449	90.343	1.178	19.637	59.400
4	.238	3.959	94.301	.238	3.959	94.301	.985	16.415	75.815
5	.201	3.354	97.656	.201	3.354	97.656	.865	14.410	90.225
6	.141	2.344	100.000	.141	2.344	100.000	.586	9.775	100.000

Nota: Método de extracción: análisis de componentes principales.

Normalidad

Posterior al análisis mencionado anteriormente, se procedió a realizar la prueba de la normalidad de los datos, se revisó la distribución de estos con el propósito de seleccionar las pruebas estadísticas más pertinentes para realizar los análisis estadísticos. Las pruebas de Kolmogorov-Smirnov y de Shapiro-Wilk son las pruebas más utilizadas por los investigadores para evaluar si los datos tienen distribución normal (Hair et al., 2014; Sarstedt & Mooi, 2019). En esta investigación se llevó a cabo la prueba de Kolmogorov Smirnov a las variables de la investigación, ya que esta es la más adecuada para determinar si existe o no distribución normal en los datos cuando estos sobre pasan las 50 observaciones (Hair et al., 2014).

La hipótesis nula (H0) de esta prueba asume que los datos de la muestra tienen una distribución normal. Los resultados indicaron que todos los ítems obtuvieron un valor p (significancia) de 0.000. Por lo tanto, se rechaza la hipótesis nula porque el valor p (nivel de significancia Alpha-α) fue menor de 0.05 y se concluye que los datos no poseen una distribución normal como se muestra en la tabla 23. Como consecuencia, se procedió a utilizar pruebas estadísticas no paramétricas para realizar los análisis estadísticos de esta investigación.

Tabla 23. Pruebas de normalidad.

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CE	.116	182	.000	.930	182	.000
PD	.212	182	.000	.927	182	.000
CS	.199	182	.000	.831	182	.000
SF	.164	182	.000	.843	182	.000
CL	.158	182	.000	.878	182	.000

a. Corrección de significación de Lilliefors

Correlación

Con respecto a los resultados de las correlaciones de Spearman, como se observa en la tabla 24 donde se describe el nivel de correlación que existe

entre las variables independientes con la variable dependiente, así como su significancia.

Tabla 24. Correlaciones Rho de Spearman.

			CPS	PD	CS	SF	CL	SI
Rho de Spearman	CE	Coeficiente de correlación	1.000	.406**	.361**	.415**	.755**	.704**
		Sig. (bilateral)	.	.000	.000	.000	.000	.000
		N	182	182	182	182	182	182
	PD	Coeficiente de correlación	.406**	1.000	.735**	.515**	.722**	.415**
		Sig. (bilateral)	.000	.	.000	.000	.000	.000
		N	182	182	182	182	182	182
	CS	Coeficiente de correlación	.361**	.735**	1.000	.805**	.763**	.492**
		Sig. (bilateral)	.000	.000	.	.000	.000	.000
		N	182	182	182	182	182	182
	SF	Coeficiente de correlación	.415**	.515**	.805**	1.000	.748**	.545**
		Sig. (bilateral)	.000	.000	.000	.	.000	.000
		N	182	182	182	182	182	182
	CL	Coeficiente de correlación	.755**	.722**	.763**	.748**	1.000	.686**
		Sig. (bilateral)	.000	.000	.000	.000	.	.000
			CPS	PD	CS	SF	CL	SI
		N	182	182	182	182	182	182
	SI	Coeficiente de correlación	.704**	.415**	.492**	.545**	.686**	1.000
		Sig. (bilateral)	.000	.000	.000	.000	.000	.
		N	182	182	182	182	182	182

**. La correlación es significativa en el nivel 0,01 (2 colas).

H1. Participación de la dirección tiene relación con el Cumplimiento de las prácticas de Seguridad de TI de .406 lo que significa que es una correlación moderada, y el p valor .000 por lo que se concluye que es estadísticamente significativa.

H2. Concientización de la seguridad de TI tiene relación con el Cumplimiento de las prácticas de Seguridad de TI de .361 lo que significa que es una correlación

baja, y el p valor .000 por lo que se concluye que es estadísticamente significativa.

H3. Sanciones formales de disuasión tiene relación con el Cumplimiento de las prácticas de Seguridad de TI de .415 lo que significa que es una correlación moderada, y el p valor .000 por lo que se concluye que es estadísticamente significativa.

H4. Contexto laboral tiene relación con el Cumplimiento de las prácticas de Seguridad de TI de .755 lo que significa que es una correlación alta, y el p valor .000 por lo que se concluye que es estadísticamente significativa.

H5. Sanciones informales de disuasión tiene relación con el Cumplimiento de las prácticas de Seguridad de TI de .704 lo que significa que es una correlación alta, y el p valor .000 por lo que se concluye que es estadísticamente significativa.

Como se observa en la tabla 25 las correlaciones de Rho de Spearman acorde con Mayorga, (2022) el coeficiente rho varía de -1 a 1, si es el “0” la relación es nula. Cuanto más se acerca el valor a ± 1 se asume mayor correlación, si la rho es positiva la relación es directa, si la rho es negativa la relación es inversa.

Tabla 25. Interpretación del coeficiente de correlación de Rho de Spearman.

Nivel de correlación	rho
Perfecta	±1
Muy Alta	± 0.800… - 0.99…
Alta	± 0.600… - 0.79…
Moderada	± 0.400… - 0.59…
Baja	± 0.200… - 0.39…
Muy baja	± 0.000… - 0.19…
Nula	0

Nota: La relación puede ser directa (+) o negativa (-)

Fuente: Mayorga, L.A. (2022). Manual de Metodología de la investigación. Cusco: Yachay.

En la Tabla 26 se observan los resultados de las hipótesis, su correlación, su significancia y resultado.

Tabla 26. Resultados de las hipótesis.

Hipótesis	Correlación	Significancia	Resultado
H_1: La percepción de la Participación de la Dirección tiene relación con el cumplimiento de las prácticas de TI.	.406	.000	Moderada
H_1: La Concientización de la Seguridad de TI tiene relación con el cumplimiento de las prácticas de TI.	.361	.000	Baja
H_3: Las Sanciones Formales de Disuasión tiene relación con el cumplimiento de las prácticas de TI.	.415	. 000	Moderada
H_4: Las Sanciones Informales de Disuasión tiene relación con el cumplimiento de las prácticas de TI.	.704	.000	Alta
H_5: El Contexto Laboral tiene relación con el cumplimiento de las prácticas de TI.	.755	.000	Alta

En la tabla 27 se puede observar que ninguna variable fue eliminada en el análisis factorial, donde se muestra que todas las variables son solicitadas.

Tabla 27. Variables entradas/eliminadas[a].

Modelo	Variables introducidas	Variables eliminadas	Método
1	V5_Contexto Laboral, V2_Concientizacion de la Seguridad, V1_Participación de la Dirección, V3_Sanciones Formales, V4_Sanciones Informales[b]	.	Intro

a. Variable dependiente: V_ cumplimiento de las prácticas de seguridad de TI

b. Todas las variables solicitadas introducidas.

A continuación, se plantea un modelo de regresión lineal con las variables estudiadas.

Regresión Lineal Múltiple

Se realizó la técnica estadística de regresión lineal múltiple, como se observa en la tabla 28 el resumen del modelo, donde se explica el modelo en un 70.6% de la intención de los empleados de llevar a cabo las prácticas de seguridad de TI. También se observa el resultado de Durbin-Watson que los datos de pueden generalizar desde 1.7 – 2.0 unidades, como se muestra el resultado es muy cercano a las 2 unidades. Por otro lado, se observa que no se eliminó ninguna de las variables.

Tabla 28. Resumen del modelo[b].

					Estadísticas de cambios					Durbin-Watson
Modelo	R	R^2	R^2 ajustado	Error estándar de la estimación	Cambio de cuadrado de R	Cambio en F	df 1	df2	Sig. Cambio en F	
1	.840[a]	.706	.697	.43335	.706	84.455	5	176	.000	1.919

a. Predictores: (Constante), X5_Contexto Laboral, X2_Concientizacion de la Seguridad, X1_Participación de la Dirección, X3_Sanciones Formales, X4_Sanciones Informales

b. Variable dependiente: Y_Cumplimiento del Empleado

Como se observa en la tabla 29 el ANOVA la significancia es 0.000 esto significa que el modelo encaja. Aparte del hecho de que predice la intención de los empleados el 70.6% de las veces, consideramos que es significativo. También significa que los datos no se basan en problemas aleatorios, es decir no son producto del azar.

Tabla 29. ANOVA[a].

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	79.301	5	15.860	84.455	.000[b]
	Residuo	33.052	176	.188		
	Total	112.353	181			

a. Variable dependiente: Y_Cumplimiento de las Prácticas de Seguridad de TI
b. Predictores: (Constante), X5_Contexto Laboral, X2_Concientizacion de la Seguridad, X1_Participación de la Dirección, X3_Sanciones Formales, X4_Sanciones Informales

En los resultados de la tabla 30 podemos observar que la Percepción de la de la Participación de la Dirección tiene una beta de -.098 lo que significa que a menor percepción del empleado de la intervención de la dirección aumenta el cumplimiento de las prácticas de TI, con respecto a la concientización de la seguridad de TI, el valor beta es de .018 con una significancia de .800 de tal manera que a pesar de que es positiva la beta de la concientización, el cumplimiento de las prácticas de TI es poca, si se realizan campañas no habrá gran diferencia es muy poco el beneficio que traería el realizar campañas de concientización en los empleados, por otra parte las sanciones formales de disuasión se obtuvo un valor beta de -.055 y una significancia de .319, por lo que entre menos sanciones formales de disuasión a través de memorándums, actas administrativas para sancionar a los empleados aumentará el cumplimiento de las prácticas de seguridad de TI, respecto a las sanciones informales de disuasión se obtuvo una beta de .354 y una significancia de .000, de tal manera que es muy significativa por lo que el sancionar a los empleados de manera informal y personal provoca que tengan mayor el cumplimiento de las prácticas de TI y el contexto laboral registró una beta de .694 con una significancia de .000, por lo que también resultó muy significativa, así que entre más concientización a los empleados en el contexto laboral en el que se encuentran aumenta el cumplimiento de las prácticas de TI, dados los resultados mostrados significa que no son producto del azar.

En los estadísticos de colinealidad la tolerancia debe estar arriba de 0.20 como se puede ver en el gráfico, todas se encuentran arriba del 0.20, en cuanto

al VIF como podemos observar ninguna está por arriba de 10 unidades ya que oscilan entre 1.775 y 3.815 por lo tanto no existe colinealidad en las variables, tal como se muestra en la tabla 30.

Tabla 30. Coeficientes[a].

Modelo	Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.	95.0% intervalo de confianza para B		Correlaciones			Estadísticas de colinealidad	
	B	Error estándar	Beta			Límite inf	Límite sup	Order cero	Parcial	Parte	Tolerancia	VIF
1 (Constante)	-.047	.243		-.192	.848	-.527	.433					
X1_Participación de la Dirección	-.098	.055	-.119	-1.783	.076	-.206	.010	.407	-.133	-.073	.376	2.660
X2_Concientización de la Seguridad	.018	.071	.019	.254	.800	-.123	.159	.395	.019	.010	.299	3.348
X3_Sanciones Formales	-.055	.055	-.069	-.999	.319	-.163	.053	.426	-.075	-.041	.352	2.842
X4_Sanciones Informales	.354	.066	.428	5.356	.000	.224	.485	.698	.374	.219	.262	3.815
X5_Contexto Laboral	.694	.064	.595	10.917	.000	.568	.819	.803	.635	.446	.563	1.775

a. Variable dependiente: Y =Cumplimiento de las prácticas de seguridad de TI.

Ecuación 1. Modelo operacional de regresión lineal múltiple

$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5$

$Y = -.047 - .098\ X_1 + .018 X_2 - .055\ X_3 + .354 X_4 + .694\ X_5$

Cumplimiento de las prácticas de TI = -.047 - .098 percepción de la participación de la dirección + .018 concientización de la seguridad de TI - .055 sanciones formales + .354 sanciones informales + .694 contexto laboral.

A continuación, en la tabla 31 se puede observar los resultados de la regresión lineal múltiple, de cada variable se observa la beta con su significancia así como la interpretación de las mismas.

Tabla 31. Resultados e interpretación de la regresión.

Variable	Beta	Significancia	Interpretación
Percepción de la Participación de la Dirección.	-.098	.076	A menor intervención de la dirección aumenta el cumplimiento de las prácticas de TI por parte de los empleados.
La Concientización de la Seguridad de TI.	.018	.800	Al aumentar la concientización de la seguridad de TI, aumenta el cumplimiento de las prácticas de TI en el cumplimiento de los empleados.
Sanciones Formales de Disuasión.	-.055	.319	A menor sanciones formales aumenta el cumplimiento de las prácticas de TI por parte de los empleados.
Sanciones Informales de Disuasión.	.354	.000	Aumentar las sanciones informales de disuasión, aumenta el cumplimiento de las prácticas de TI por parte de los empleados.
Contexto Laboral.	.694	.000	Al aumentar el conocimiento del contexto laboral aumenta el cumplimiento de las prácticas de TI por parte de los empleados.

4.2.4. *Comprobación de Hipótesis*

En la comprobación de las hipótesis como se observa en la tabla 26 la **H_1** la Percepción de la Participación de la Dirección tiene relación con el cumplimiento de las prácticas de seguridad de TI, de manera moderada con un valor de .406, además de ser estadísticamente significativa con valor de p de 0.000, con respecto a la **H_2** Concientización de la seguridad de TI tiene relación con el cumplimiento de las prácticas de seguridad de TI, con un valor de .361 lo que significa que es una correlación baja, y el p valor .000 por lo que es estadísticamente significativa.

La **H_3**. Sanciones formales de disuasión también tiene relación con el cumplimiento de las prácticas de seguridad de TI, con un valor de .415 lo que significa que es una correlación moderada, y el p valor .000 por lo que se concluye que es estadísticamente significativa. **H_4**. Sanciones informales de disuasión tiene relación con el cumplimiento de las prácticas de seguridad de TI, con valor de .704 lo que significa que es una correlación alta, y el p valor .000 por lo que se concluye que es estadísticamente significativa. La **H_5**. Contexto laboral tiene relación con el cumplimiento de las prácticas de seguridad de TI, con un valor de .755 lo que significa que es una correlación alta, y el p valor .000 lo que indica que es estadísticamente significativa, de tal manera que las cinco hipótesis se aprueban ya que todas tienen relación con el cumplimiento de las prácticas de TI en diferente medida y todas son estadísticamente significativas.

En este capítulo se presentó el análisis de los resultados obtenidos de la investigación. Se realizaron las pruebas utilizando el SPSS v. 22 se describieron resultados de fiabilidad, así como diferentes resultados de los análisis estadísticos para obtener la relación de las variables independientes sobre la variable dependiente cumplimiento de las prácticas de seguridad de TI.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se realizaron los análisis pertinentes en la investigación donde podemos concluir, que la pregunta de investigación se respondió de la siguiente manera, de las cinco variables tomadas en cuenta para determinar los factores que se relacionan con el cumplimiento de las prácticas de seguridad de TI, se aprobaron todas las hipótesis de tal manera que, la percepción de la participación de la dirección resultó con una correlación moderada hacia la variable dependiente, la concientización de la seguridad de TI reflejó una correlación baja con respecto a la variable dependiente el cumplimiento de las prácticas de seguridad de TI, las sanciones formales de disuasión tuvieron también una correlación moderada hacia la variable dependiente, por otra parte las sanciones informales de disuasión y el contexto laboral tuvieron una correlación alta hacia el cumplimiento de las prácticas de seguridad de TI. Todas las correlaciones anteriores tuvieron un valor p de 0.000 por lo que todas son estadísticamente significativas.

Por otra parte en los resultados de la regresión podemos observar en las tablas 28 y 31 respectivamente, que el modelo explica en un 70.6% la investigación realizada por lo que la percepción de la de la participación de la dirección tiene una beta de -.098 lo que significa que a menor intervención de la dirección aumenta el cumplimiento de las prácticas de seguridad de TI por parte de los empleados, con respecto a la concientización de la seguridad de TI, el valor beta es de .018 con una significancia de .800 de tal manera que al aumentar la concientización de la seguridad de TI, aumenta el cumplimiento de las prácticas de seguridad de TI, más sin embargo el aumento es poco, por ejemplo, si se realizan campañas de concientización de la seguridad de TI, no habrá gran diferencia y sería muy poco el beneficio, por otra parte las sanciones formales de disuasión se obtuvo un valor beta de -.055 y una significancia de .319, por lo que entre menos sanciones formales aumenta el cumplimiento de las prácticas de seguridad de TI, es decir entre menos sanciones formales a través de memorándums, actas administrativas se les hagan y que manchen el expediente del trabajador para sancionarlo, aumenta el cumplimiento de las prácticas de

seguridad de TI, respecto a las sanciones informales de disuasión se obtuvo una beta de .354 y una significancia de .000, de tal manera que es muy significativa por lo que al aumentar las sanciones informales de disuasión aumenta el cumplimiento de las prácticas de seguridad de TI, es decir al sancionar a los empleados de manera personal a través de una llamada de atención de manera personal sin que se manche su expediente, provoca que tengan un mayor cumplimiento de las prácticas de seguridad de TI y con respecto al contexto laboral, registró una beta de .694 con una significancia de .000, por lo que también resultó muy significativa, así que al aumentar la concientización en los empleados del contexto laboral en el que se desempeñan, haciendo conciencia de que la información que manejan es sensible y que su trabajo es muy importante para la institución resultó que aumenta el cumplimiento de las prácticas de seguridad de TI, así que dados los resultados mostrados significa que no son producto del azar.

Cumplimiento de objetivos:

De acuerdo a los resultados de la investigación se pudo cumplir con el objetivo principal de determinar cuáles son los factores que se relacionan con el cumplimiento de las prácticas de seguridad de TI por parte de los empleados, logrando determinar que la percepción de la participación de la dirección, la concientización de la seguridad de TI, las sanciones formales de disuasión, las sanciones informales de disuasión y el contexto laboral, son factores que se relacionan en el cumplimiento de las prácticas de seguridad de TI, de tal manera que todas las hipótesis fueron aprobadas.

Síntesis y Discusión de resultados:

H_1: De acuerdo con la literatura revisada Ifinedo (2016) en su estudio realizado en Canadá, encontró que la variable Percepción de la participación de la gerencia tiene relación con el cumplimiento de las prácticas de seguridad de TI con una correlación muy alta de 0.870, contrastando con este estudio donde el resultado fue que la Percepción de la Participación de la dirección presenta una relación con el cumplimiento de las prácticas de seguridad de TI de manera moderada, con un valor de 0.406, además de ser estadísticamente

significativa con valor de p de 0.000 se concluye que se tuvieron resultados similares con el presente estudio.

Con respecto a la Hipótesis **H_2** Concientización de la seguridad de TI, Alarcón y Orjeda (2019) realizaron en Perú un estudio donde la Concientización de la seguridad de TI resultó con una correlación moderada de 0.405 con el cumplimiento de las prácticas de seguridad de TI, el resultado obtenido en esta investigación fue que en la Concientización de la seguridad de TI existe una relación con el cumplimiento de las prácticas de seguridad de TI con un valor de 0.361 lo que significa que es una correlación baja, por lo que se concluye que la diferencia en los resultados, es que el estudio se realizó en Perú y el investigador combinó la concientización con el entrenamiento en su modelo para que este resultara con mayor aporte para explicar el comportamiento de los empleados para cumplir con las prácticas de seguridad de TI y en esta investigación la variable concientización se utilizó una relación directa con la variable dependiente.

H_3: Así mismo en Ecuador en una investigación realizada por Montesdeoca y Gonzaga (2018) realizaron un estudio donde las Sanciones formales de disuasión tuvieron una relación con el cumplimiento de las prácticas de seguridad de TI con una correlación moderada de 0.524, en contraste con este estudio las sanciones formales de disuasión tuvieron una correlación también moderada de 0.415 con el cumplimiento de las prácticas de seguridad de TI, con lo que se concluye que se tuvo una similitud con los autores en su estudio para esta investigación.

H_4: Con respecto a las Sanciones informales de disuasión, Johnston, Warkentin y Siponen (2015) realizaron una investigación en Finlandia donde las sanciones informales de disuasión tuvieron una relación significativa como determinantes directos en el cumplimiento de las prácticas de seguridad de TI, con una correlación alta de 0.789, de igual manera de acuerdo con este estudio las Sanciones informales de disuasión resultaron con una correlación alta de

0.755 en el cumplimiento de las prácticas de seguridad de TI, de tal forma que se tuvo similitud en los resultados en ambas investigaciones.

H_5: Finalmente el Contexto laboral tuvo una relación positiva en el cumplimiento de las prácticas de seguridad de TI por parte de los empleados en un estudio realizado por D'Arcy y Devaraj (2012) en Estados Unidos, determinaron que el contexto laboral resultó ser alta la correlación con 0.793 en el cumplimiento de las prácticas de seguridad de TI, así como en el presente estudio el contexto laboral obtuvo una correlación alta de 0.704 en la relación con los empleados por cumplir con las prácticas de seguridad de TI, por lo que concluimos que se tuvo similitud con el estudio de los autores con respecto a la variable estudiada.

Las aportaciones de este estudio son, que las hipótesis planteadas en esta investigación con respecto a otros autores todas se aprueban en el cumplimiento de las prácticas de seguridad de TI por parte de los empleados. De acuerdo con este estudio la aportación es que se realizó en IES públicas y de acuerdo con la literatura este tipo de fenómeno se ha investigado solo en empresas u organizaciones.

Implicaciones prácticas:

El estudio propone que las prácticas de seguridad de TI son un aspecto crítico en los tiempos actuales, por lo que en las IES es necesario concientizar a los empleados en el correcto uso de la información, se recomienda que tanto la percepción de la participación de la dirección, la concientización de la seguridad de TI, las sanciones formales e informales de disuasión así como el contexto laboral se realicen y se lleven a cabo para poder lograr en los empleados el cumplimiento de las prácticas de seguridad de TI, ya que por el contrario, una reacción intimidante por parte de los jefes para tomar acciones correctivas podría tener un resultado inverso, puesto que según el estudio las personas no reaccionan favorablemente a acciones de represión o sanciones,

más bien reaccionan positivamente a estímulos o actos de prevención sin necesidad de perjudicar sus hojas de desempeño laboral.

También el beneficio es que en las IES públicas estudiadas, si se realiza una inversión con respecto a los resultados obtenidos, se deben de enfocar en invertir en concientizar el contexto laboral en el que se encuentran los empleados y de la importancia que tiene la información que manejan ya que es sensible y que es muy importante su desempeño al llevar a cabo las prácticas de seguridad de TI, así como motivar a los jefes quizá con capacitación en coaching para tomar ante los empleados una actitud de sancionar de manera informal y personal a los empleados sin manchar su expediente laboral para conseguir que tengan mayor intención de cumplir con dichas prácticas para que se tenga mayor seguridad de la información en las Instituciones de Educación Superior ya que se ha visto que también son blanco de la ciberdelincuencia.

Adicionalmente se propuso un modelo de regresión con las variables en conjunto que explican el cumplimiento de las prácticas de seguridad de TI por parte de los empleados. En caso de ser usada en las IES públicas podrían servir para la mejor gestión de un presupuesto.

Limitaciones de la investigación:

La primera limitación fue el tiempo ya que la encuesta se aplicó en un período específico, de tal manera que no se pudo recolectar más información para el estudio, además la situación de la pandemia de COVID-19 fue un factor limitante para visitar las IES y aplicar las encuestas de manera presencial, otra limitación fue encontrada durante el desarrollo de esta investigación en que las IES al igual que las organizaciones públicas y privadas son celosas de su información, de tal manera que fue compleja la recolección de los datos, aunque al final se logró el objetivo, sin embargo, fue difícil conseguirlo. Finalmente, otra limitación es que no se pueden generalizar los datos en este punto ya que se realizó solo en las tres IES más grandes de México.

Recomendaciones:

Se recomienda continuar con esta investigación y abarcar otros estados de la República; se recomienda impulsar cada vez más los mecanismos de conocimiento, concientización en el contexto laboral e impulsar las sanciones informales de disuasión para una mejor práctica de las políticas y prácticas de seguridad de TI en las IES públicas y privadas.

Ampliar el sujeto de estudio no solo al personal que labora en el área de TI, sino a todo el personal administrativo de las instituciones ya que todos manejan información sensible y deben tener conocimiento de las prácticas de seguridad de TI para llevarlas a cabo y resguardar de mejor manera la información que manejan.

Otra recomendación es que al asignar una partida presupuestar a las IES el enfoque sea dirigido hacia los empleados del área de TI para su capacitación en coaching y sensibilización del grado de importancia que tiene la información que tienen a su cargo para evitar lo mayormente posible los errores internos como caer víctimas de la ciberdelincuencia.

También es recomendable se realice el estudio en IES privadas para ver qué tan similares o diferentes serían los resultados contrastando los mismos con instituciones de educación superior públicas.

Las futuras líneas de investigación:

Se deberá llevar este estudio a otros niveles educativos o a otras instancias educativas como la educación media superior y la básica para lograr salvaguardar la información de las Instituciones.

Realizar el estudio en más IES públicas para abarcar mayor población, incluyendo otros estados de la República para realizar comparaciones entre IES ellas y poder en algún punto generalizar los datos.

Realizar el estudio en IES privadas para conocer el grado de cumplimiento de las prácticas de TI para comparaciones con otras instituciones privadas y también públicas.

Efectuar un estudio con ecuaciones estructurales para profundizar más la investigación para ver si hubiese variables moderadoras, mediadoras, extrañas, así como observar el comportamiento de las variables.

Ya que se propuso un modelo de regresión lineal múltiple para dejar antecedente y se siga una investigación para determinar el impacto de las variables independientes con la dependiente, ya que en la investigación se comprobó la relación entre las variables estudiadas.

REFERENCIAS BIBLIOGRÁFICAS

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

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

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Alarcón Cubas, F. D. A., y Orjeda Ramírez, J. A. (2019). *La gestión de conductas y comportamientos en los usuarios de TI y la concientización en la seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo-Chiclayo-Lambayeque.* [Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo]. http://repositorio.unprg.edu.pe:8080/bitstream/handle/20.500.12893/3476/BC-TES-TMP-2283.pdf?sequence=1&isAllowed=y

Arellano S. (2020, octubre 9). *México, segundo país con más ciberataques en el mundo*. *Milenio Noticias*. https://www.milenio.com/negocios/mexico-pais-con-mas-ciberataques-en-el-mundo.

Aurigemma, S., & Panko, R. (2012, January). A composite framework for behavioral compliance with information security policies. *In 2012 45th Hawaii International Conference on System Sciences* (pp. 3248-3257). IEEE.

Ayyagari, R., & Tyks, J. (2012). Disaster at a university: A case study in information security. *Journal of Information Technology Education*, *11*, 85-96.

Boyle, R. J., & Panko, R. R. (2015). *Corporate computer security* (4th ed.). New Jersey, NJ: Pearson Education.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548

Cavallari, M. (2011). The organizational relationship between compliance and information security. *International Journal of the Academic Business World 5*(2), 63-76.

Celi Arévalo, E. K., y Díaz Plaza, R. J. A. (2017). *Políticas de Seguridad de la Información en Función del Comportamiento de los Usuarios de Tecnologías de la Información en el Sector Microfinanciero de Lambayeque.* [Tesis de doctorado, Universidad Nacional Pedro Ruiz Gallo].https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/1365/BC-TES-TMP-201.pdf?sequence=1&isAllowed=y

Chaudhry, P. E., Chaudhry, S. S., & Reese, R. (2012). Developing a model for enterprise information systems security. *Economics, Management and Financial Markets. 7(4), 587.*

Chen, Y., Ramamurthy, K. K., & Wen, K. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chin, W.W. (1998). Issues and Opinion on Structural Equation Modeling*, MIS Quarterly, 22*(1), vii-xvi.

Collins, J., Sainato, V. y Khey, D. (2011). Violaciones de datos organizacionales *Internacional de Ciber criminología,* 5, 794–810.

Cordovilla, F. E. A., Sigcho, I. B. O., Larenas, F. P., & Matamoros, V. J. S. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Dominio de las Ciencias*, *6*(2), 835-846.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43* (6), 1091-1124.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318

Dormann, C. F., Elith, J., Bacher, S., Buchmann, C., Carl, G., Carré, G., ... & Lautenbach, S. (2013). Collinearity: a review of methods to deal with it and a simulation study evaluating their performance. *Ecography, 36*(1), 27-46.

Excellence, I. (2020). Plataforma Tecnológica para la Gestión de la Excelencia. De: Calidad y excelencia: https://www. isotools. org/2018/03/05/la-norma-iso-iec-27000-va-a-ser-revisada.

Farfán Chávez, O. C., Franco Luna, J. E., Gachuz Montaño, H. E., Hernández Viquez, J. J., & Lozano Ortega, J. A. (2018). *Propuesta de baseline de seguridad informática con base en mejores prácticas para áreas informáticas de empresas de reciente creación.* [Tesis de pregrado, Instituto Politecnico Nacional]. http://tesis.ipn.mx/handle/123456789/24786

Fisher, K., & Shorter, J. (2013). Emerging ethical issues: universities and information warfare. *Journal of Academic and Business Ethics*, *7*, 1. 1-10

Furnell, S. M., Clarke, N., Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*. 18(1), 26-42.

Garcés Realpe, O. J., & Moreno Serrano, J. A. (2019). *Diseño del sistema de gestión de seguridad de la información para los procesos de administración de bases de datos y administración de hosting de aplicaciones de la empresa Softdev LTDA., basado en la norma ISO IEC 27001: 2013* [Tesis de doctorado, Universidad Piloto De Colombia] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4981/00005144.pdf?sequence=1&isAllowed=y

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier.

González Paz, A., Beltrán Casanova, D., y Fuentes Gari, E. R. (2016). Propuesta de Protocolos de Seguridad para la Red Inalámbrica Local de la

Universidad de Cienfuegos. *Universidad y Sociedad [seriada en línea]*, 8 (4), pp. 128-135.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems*, *28*(2), 203-236.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A Primer on Partial*

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación.* McGraw-Hill/Interamericana

Hernández, R., Mendoza, C. (2018). *Metodología de la investigación*. McGraw-Hill/Interamericana

Hoadley, E. D., Deibel, J., Kistner, C., Rice, P., & Sokhey, S. (2012). Seeking best practices in the balancing act between data security and operational effectiveness. *International Journal of Management & Information Systems (IJMIS)*, *16*(2), 183-188.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54-60.

Ifinedo, P. (2016). Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, 33(1), 30-41.

Imbaquingo, D. E., Herrera-Granda, E. P., Herrera-Granda, I. D., Arciniega, S. R., Guamán, V. L., & Ortega-Bustamante, M. C. (2019). Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E22), 349-362.

Issa-Salwe, A. M., & Ahmed, M. (2011). Risk management of an information system by assessing threat, vulnerability, and countermeasure. *International Journal of Research and Reviews in Computer Science*, *2*(1), 111-114.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study*. MIS Quarterly,* 34(3), 549-A4

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

Kappelman, L., McLean, E., Luftman, J., & Johnson, V. (2013). Key Issues of IT Organizations and Their Leadership: The 2013 SIM IT Trends Study. *MIS Quarterly Executive*, *12*(4).227-240.

Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods*. Waveland Press.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*,*11*(7), 1 394-413.

Luftman, J., & Ben-Zvi, T. (2011). Key issues for IT executives 2011: Cautious optimism in uncertain economic times. *MIS Quarterly Executive*, 10(4), 203-212

Luftman, J., Derksen, B. (2014). European key IT and management issues & trends for 2014. *CIONET Europe and Business & IT Trend Institute* 1, 36.

Luftman, J., Zadeh, H. S., Derksen, B., Santana, M., Rigoni, E. H., & Huang, Z. (2012). Key information technology and management issues 2011-2012: An international study. *Journal of Information Technology*, 27(3), 198-212

Mayorga, L.A. (2022). Manual de Metodología de la investigación. Cusco: Yachay.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, 9(1), 23-41.

UNAM (2021). Directorio de Facultades y Escuelas. En: de Universidad Nacional Autónoma de México: https://www.unam.mx/comunidad/estudiantes/facultades-y-escuelas. 23 abril 2021

Montesdeoca Vásquez, G. J., & Gonzaga Acuña, A. C. (2018). Réplica de un modelo de cumplimiento de la política de seguridad de la información en las organizaciones [Tesis de maestría Universidad Espíritu Santo]. http://201.159.223.2/bitstream/123456789/2768/1/MONTESDEOCA%20VASQUEZ%20GABRIELA%20JAZMIN%20Y%20GONZAGA%20ACU%C3%91A.pdf

Morales J.J., Avellan N., Mera J.S. y Zambrano M. (2019). Ciberseguridad y su aplicación en las Instituciones de Educación Superior. *Revista Ibérica de Sistemas e Tecnologias de Informação,* (E20), 438-448.

Mujica Flores, S. D., y Herrera Anchundia, J. J. (2018). *Diseño de un sistema de gestión de la seguridad de la información alineado bajo la norma ISO/IEC 27001: 2013 para el consorcio metro-Bastión* [Tesis de Licenciatura. Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/36876.

Mullins, L. J. (2010). "Gestión y comportamiento organizativo". Pearson Education.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Quarterly*, 1189-1210.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Ramachandran, A. & Ramachandran, S. (2012). Rapid and Proactive Approach on Exploration of Database Vulnerabilities. *International Journal on Computer Science and Engineering (IJCSE), 4* 224-234.

Robbins, S. P., Coulter, M., & DeCenzo, D. A. (2017). "Fundamentos de la administración ". Pearson

Rosenthal, G. & Rosenthal, J. (2011). Estadística e Interpretación de Datos para Trabajo Social. Editorial Springer.

Rueda Sampedro, M. I., Fernández Laviada, A., & Herrero Crespo, A. (2013). Aplicación de la teoría de la acción razonada al ámbito emprendedor en un contexto universitario. *Investigaciones Regionales, 26*, 141-158.

Salkind, N. J. (2012). *Statistics for people who (think they) hate statistics: Excel 2010 edition*. Sage.

Sarstedt, M., & Mooi, E. (2019). *A concise guide to market research*. Springer.

Serrano, R. (2007). *Gestión de seguridad de la información y los servicios críticos de las universidades: un estudio de tres casos en Lima Metropolitana*. [Tesis de maestría Universidad Nacional Mayor de San Marcos]. http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/428/Rayme_sr.pdf?sequence=1.

Shaw, R. (2012). *The influence of organizational culture on employee attitudes towards information security policy*. [ProQuest Dissertations Publishing, Capella University]. https://www.proquest.com/openview/c47383be6d7e1aeed8d6889796516efd/1?pq-origsite=gscholar&cbl=18750.

Schelling, T. C. (1960). The Strategy of Conflict, 15. Auflage, Cambridge, MA.

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

Susanto, H. y Almunawar, M. N. (2012). Information Security Awareness Within Business Environment: An IT Review. Available at SSRN 2150821.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology. IJET Publications UK*, *2*(1). 67-75.

Trajtenberg, N., y Aloisio, C. (2009). La racionalidad en las teorías criminológicas Contemporáneas. Uruguay desde la sociología, 279-294.

Turban, E., Volonino, L., & Wood, G. (2013). *Information technology for management: Advancing sustainable profitable business growth* (9th ed.). NJ: John Wiley & Sons, Inc.

Tyler, T. R., Callahan, P. E., & Frost, J. (2007). Armed, and dangerous (?): Motivating rule adherence among agents of social control. *Law & Society Review*, 41(2), 457-492.

UANL. (2021). Universidad Autónoma de Nuevo León. De: https://www.uanl.mx/escuelas-y-facultades/. 23 abril 2021

Universidad de Guadalajara. (2021). *Red Universitaria de Jalisco*. En: https://www.udg.mx/es/directorio.

Ureña Centeno, F. J. (2015). Ciberataques, la mayor amenaza actual. *Instituto Español de Estudios Estratégicos, 1-12*.

Vance, A., Lowry, P. B., & Eggett, D. L. (2015). Increasing accountability through the user interface design artifacts: A new approach to addressing the problem of access-policy violations. *Mis Quarterly*, *39*(2), 345-366.

Vargas Salcedo, J. C. (2018). Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa. *Fundación Universidad Piloto de Colombia.* 1-12.

Viloria, O., & Blanco, W. (2009). Modelo sistémico de la seguridad de la información en las universidades. *Revista Venezolana de Análisis de Coyuntura*,*15*(1), 219-240.

Visauta B. y Martori J. C. (2005). *Análisis estadístico con SPSS para Windows*, Mc Graw Hill.

Wiesenfeld, B. M., Raghuram, S., & Garud, R. (1999). Communication patterns as determinants of organizational identification in a virtual organization. *Organization science*, *10*(6), 777-790.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 1-20

Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24(1), 1-32.

Yupanqui, J. R. A., & Oré, S. B. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, (25), 112-134.

Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2010). *Business research methods* (8th ed.). Cengage Learning.

ANEXOS

OPERALIZACIÓN DE LAS VARIABLES

Variable: X_1 Percepción y Participación de la Gerencia		
Definición conceptual: Hu et al, (2011) precisa que la equidad y la justicia implican que los empleados perciban que la gerencia practica justicia y equidad al establecer, definir y hacer cumplir las prácticas de seguridad de TI		
Instrumento: Encuesta		
Dimensiones	**Indicadores (Definición Operacional)**	**Ítems del instrumento**
Persepción de la Participación de la Gerencia	Likert	La gerencia de la institución de educación superior donde trabajo ha expresado interés por la seguridad de TI.
		La gerencia de la institución de educación superior donde trabajo ha establecido políticas de seguridad de TI.
		La gerencia de la institución de educación superior donde trabajo ha designado o debe designar a una persona a cargo de la seguridad de TI en toda la institución, tal como un Oficial de Seguridad de TI.
		La gerencia de la institución de educación superior donde trabajo modela con su comportamiento y aplica sanciones a todos los empleados, sin excepción; demostrando así su compromiso con las prácticas de TI.
Variable: X2 Concientización de la Seguridad de TI		
Definición conceptual: Son los conocimientos generales de un empleado sobre seguridad de la información y su conocimiento de las prácticas de seguridad de TI de su organización (Bulgurcu, et al 2010).		
Instrumento: Encuesta		
Dimensiones	**Indicadores (Definición Operacional)**	**Ítems del instrumento**

Concientización de la seguridad de TI	Likert	Estoy consciente de las posibles amenazas y riesgos relacionados a la seguridad de la información y sus consecuencias negativas
		Conozco y entiendo las normas y reglamentos establecidos por las prácticas de seguridad de TI de la institución de educación superior donde trabajo
		Conozco mis responsabilidades, según lo establecido por las prácticas de seguridad de TI en la institución de educación superior donde trabajo.
Variable: X3 Sanciones Formales de Disuasión		
Definición conceptual: Disuasión se refieren a la certeza y la gravedad percibidas por los empleados, de las sanciones impuestas por la organización por el mal uso, o uso no autorizado de las TI (D'Arcy & Herath, 2011).		
Instrumento: Encuesta		
Dimensiones	**Indicadores (Definición Operacional)**	**Ítems del instrumento**
Sanción Formal	Likert	Existe una alta probabilidad de que la institución de educación superior donde labora sancione a un usuario por acceder a la información de la computadora donde él no está autorizado
		Si se detecta en su institución de educación superior donde labora, que un usuario accedió a la computadora principal sin tener permisos, éste será severamente amonestado
		Existe una alta probabilidad de que la institución educativa sancione a un usuario por modificar los registros de nómina de horas trabajadas
		Si detectan que un usuario de la institución educativa donde labora altera los registros de horas trabajadas, este será severamente amonestado
Variable: X4 Sanciones Informales de Disuasión		

Definición conceptual: se refiere a los costos sociales y autoimpuestos por los empleados, tomados en consideración por estos antes de tomar decisiones de no cumplir con las prácticas de seguridad de TI (D'Arcy & Devaraj, 2012; Hu et al, 2012).		
Instrumento: Encuesta		
Dimensiones	**Indicadores (Definición Operacional)**	**Ítems del instrumento**
Sanción Informal de Disuasión	**Likert**	Considero que es necesario y beneficioso para una institución de educación superior establecer prácticas de seguridad de TI bien definidas
		Considero que es obligatorio para una institución de educación superior hacer cumplir las prácticas de seguridad de TI
		Las personas como mi supervisor y los compañeros de trabajo piensan que yo debería cumplir con las prácticas de seguridad de TI.
		Los miembros de mi familia piensan que yo debería cumplir con las prácticas de seguridad de TI.
		Los directivos de la institución educativa piensan que yo debería cumplir con las prácticas de seguridad de TI.
		Soy capaz de cumplir con las prácticas de seguridad de TI.
		Tengo las habilidades y destrezas adecuadas para cumplir con las prácticas de seguridad de TI.
Variable: X5 Contexto Laboral.		
Definición conceptual: se refiere al contexto inmediato de empleo y a las características del trabajo		
Instrumento: Encuesta		
Dimensiones	**Indicadores (Definición Operacional)**	**Ítems del instrumento**
Contexto Laboral	**Likert**	Mi puesto me exige conocer las políticas de seguridad de TI de mi institución
		En mi departamento (puesto) se aplican las políticas de seguridad de TI de mi institución

		Existe un responsable en mi institución que supervisa las políticas de TI tanto dentro como fuera de la institución
		Se aplican sanciones según el nivel de la falta cuando se labora dentro o la distancia de la institución
		La ética es un valor que se practica por los empleados de TI cuando se labora dentro a la distancia de la institución.
Variable: **Y** Empleados en cumplir con las prácticas de Seguridad de TI.		
Definición conceptual: El comportamiento de seguridad de la información conforme se refiere al conjunto de actividades de seguridad de la información centrales que los usuarios finales deben cumplir para mantener la seguridad de la información según lo definido por las políticas de la seguridad de la información (Ifinedo, 2016).		
Instrumento: Encuesta		
Dimensiones	**Indicadores (Definición Operacional)**	**Ítems del instrumento**
Intención	**Likert**	Generalmente aplico las prácticas de seguridad de TI en mi trabajo
		Por lo general utilizo aplicaciones, técnicas o mecanismos para proteger la información de mi trabajo
		Sigo las prácticas de seguridad de TI en cualquier lugar en donde yo utilice información de mi trabajo
		El personal que labora en el área de TI de la institución de educación superior sigue los lineamientos de seguridad de TI.
		Los sistemas y aplicaciones se realizan conforme a los requisitos de seguridad de la institución educativa en la que trabajo

UNIVERSIDAD DE SAN MARTÍN DE PORRES

La presente encuesta forma parte del proyecto de investigación titulado "**FACTORES QUE INCIDEN EN LOS EMPLEADOS EN CUMPLIR CON LAS PRÁCTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LAS TRES INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS MÁS GRANDES DE MÉXICO**", la *USMP*. Agradecemos la participación de administrativos, en el llenado de esta encuesta. La información es de carácter estrictamente confidencial; su uso será única y exclusivamente con propósitos de investigación científica. Su participación es completamente anónima.

I. PERFIL DEL ENCUESTADO

1.- Edad: _____21 a 30 años _____31 a 40 años _____41 a 50 años
_____51 a 60 años _____61 años o más

2.- Género:
( ) Masculino
( ) Femenino

3.- Escolaridad:
( ) Preparatoria
( ) Técnico superior
( ) Licenciatura
( ) Maestría
( ) Doctorado

4.- Estado civil
( ) Casado/a
( ) Soltero/a
( ) Divorciado/a
( ) **Otro:** _____

5.- Posición en la Institución de Educación Superior:
( ) Propietario
( ) Gerente/Director general
( ) Responsable del área de TI
( ) Empleado del área de TI

6- Indique los años que lleva trabajando en la institución de educación superior:

_____Menos de 1 año _____1 a 10 años _____11 a 20 años ____21 a 30 años
_____Más de 30 años.

7-. ¿Trabaja usted en alguno de los siguientes departamentos: ¿informática, sistemas de información o tecnologías de información?
_____Si _____No

II PREGUNTAS DE LAS VARIABLES

Indicaciones: Por favor lea las siguientes afirmaciones y *a partir de su experiencia y opinión* **indique el grado de acuerdo o desacuerdo** que Usted tiene respecto a cada una. No hay respuestas buenas ni malas, sólo queremos saber su opinión. Marque con una **X** el número que representa su opinión o respuesta. Considere lo siguiente:

Indicaciones: Seleccione de una escala del 1 al 5 a lo que más describa su situación.

1=Nunca 2=Casi nunca 3= Ocasionalmente 4= Casi siempre 5= Siempre

	Y. Intención de los empleados en cumplir con las prácticas de seguridad de TI	**1**	**2**	**3**	**4**	**5**
8.	Por lo general aplico las prácticas de seguridad de TI en mi trabajo.	( )	( )	( )	( )	( )
9.	Por lo general utilizo aplicaciones, técnicas o mecanismos para proteger la información de mi trabajo.	( )	( )	( )	( )	( )
10	Sigo las prácticas de seguridad de TI en cualquier lugar en donde yo utilice información de mi trabajo.	( )	( )	( )	( )	( )
11.	El personal que labora en el área de TI de la institución de educación superior sigue los lineamientos de seguridad de TI.	( )	( )	( )	( )	( )
12.	Utilizo los sistemas y aplicaciones conforme a los requisitos de seguridad de la institución educativa en la que trabajo.	( )	( )	( )	( )	( )
X1.	Percepción de la Participación de la Gerencia	**1**	**2**	**3**	**4**	**5**
13.	La gerencia de la institución de educación superior donde trabajo expresa su interés por la seguridad de TI	( )	( )	( )	( )	( )
14.	La gerencia de la institución de educación superior donde trabajo establece políticas de seguridad de TI	( )	( )	( )	( )	( )
15.	La gerencia de la institución de educación superior donde trabajo aplica las prácticas de seguridad de TI					
16.	La gerencia de la institución de educación superior donde trabajo asigna a una persona a cargo de la seguridad de TI en toda la institución, tal como un Oficial de Seguridad de TI	( )	( )	( )	( )	( )
17.	La gerencia de la institución de educación superior donde trabajo modela con su comportamiento y aplica sanciones a todos los empleados, sin excepción; demostrando así su compromiso con las prácticas de seguridad de TI.	( )	( )	( )	( )	( )
18.	La gerencia de la institución de educación superior donde trabajo sanciona a todos los empleados que no cumplen con las prácticas de seguridad de TI	( )	( )	( )	( )	( )
19.	La gerencia de la institución de educación superior donde trabajo da a conocer a los empleados, sin excepción, las sanciones por el incumplimiento de las prácticas de seguridad de TI	( )	( )	( )	( )	( )
X2.	Concientización de la seguridad de TI	**1**	**2**	**3**	**4**	**5**
20.	Estoy consciente de las posibles amenazas y riesgos relacionados a la seguridad de la información y sus consecuencias negativas	( )	( )	( )	( )	( )
21.	Conozco y entiendo las normas y reglamentos establecidos por las prácticas de seguridad de TI de la institución de educación superior donde trabajo.	( )	( )	( )	( )	( )
22.	Conozco mis responsabilidades, según lo establecido por las prácticas de seguridad de TI en la institución de educación superior donde trabajo.	( )	( )	( )	( )	( )

X3. Sanciones Formales de Disuasión		**1**	**2**	**3**	**4**	**5**
23.	La institución de educación superior donde labora sanciona a un usuario por acceder a la información de la computadora donde él no está autorizado.	( )	( )	( )	( )	( )
24.	Si la institución de educación superior donde labora detecta que un usuario accedió a la computadora principal sin tener permisos, éste es severamente sancionado.	( )	( )	( )	( )	( )
25.	La institución educativa donde labora sanciona a un usuario por modificar los registros de nómina de horas trabajadas.	( )	( )	( )	( )	( )
26.	Si detectan que un usuario de la institución educativa donde labora altera los registros de horas trabajadas, este es severamente sancionado.	( )	( )	( )	( )	( )
X4. Sanciones Informales de Disuasión.		**1**	**2**	**3**	**4**	**5**
27.	Considero que es necesario y beneficioso para una institución de educación superior en la que trabajo establecer prácticas de seguridad de TI bien definidas	( )	( )	( )	( )	( )
28.	Considero que la institución de educación superior donde trabajo debe hacer obligatorio el cumplir con las prácticas de seguridad de TI	( )	( )	( )	( )	( )
29.	Las personas como mi supervisor y los compañeros de trabajo piensan que yo debería cumplir con las prácticas de seguridad de TI.	( )	( )	( )	( )	( )
30.	Los miembros de mi familia piensan que yo debería cumplir con las prácticas de seguridad de TI.	( )	( )	( )	( )	( )
31.	Los directivos de la institución educativa piensan que yo debo cumplir con las prácticas de seguridad de TI.	( )	( )	( )	( )	( )
32.	Soy capaz de cumplir con las prácticas de seguridad de TI.	( )	( )	( )	( )	( )
33.	Tengo las habilidades y destrezas adecuadas para cumplir con las prácticas de seguridad de TI.	( )	( )	( )	( )	( )
X5. Contexto laboral		**1**	**2**	**3**	**4**	**5**
34.	El puesto en el que me desempeño me exige conocer las políticas de seguridad de TI de mi institución.	( )	( )	( )	( )	( )
35.	En mi departamento (puesto) se aplican las políticas de seguridad de TI de mi institución	( )	( )	( )	( )	( )
36.	Existe un responsable en mi institución que supervisa las políticas de TI tanto dentro como fuera de la institución.	( )	( )	( )	( )	( )
37.	Se aplican sanciones según el nivel de la falta cuando se labora dentro o la distancia de la institución.	( )	( )	( )	( )	( )
38.	La ética es un valor que se practica por los empleados de TI cuando se labora dentro a la distancia de la institución.	( )	( )	( )	( )	( )