UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTORA:

Ramirez Alva, Taina Licel (orcid.org/0000-0002-0488-6932)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (orcid.org/0000-0002-0024-668X)

CO-ASESOR:

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN:
Auditoria de sistemas y seguridad de la información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:
Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2023

Dedicatoria

Mi tesis se la dedico a mi querida madre Cecilia Alva que en todo momento es y ha sido mi soporte y me ha dado lo necesario para salir adelante en esta vida. A mis hermanos que sacan lo mejor de mí y me motivan a ser mejor cada día.

Agradecimiento

Agradezco a Dios por darme todo lo que tengo, por gozar de buena salud y tener todo lo necesario para salir adelante en esta vida. A los docentes de la Universidad César Vallejo por haber compartido sus conocimientos y haber ayudado en mi crecimiento profesional.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

La presente investigación fue realizada con la finalidad de Determinar la incidencia de la Ciberseguridad en la Gestión de tecnologías de Información en una empresa de Seguros, Lima 2022.

El tipo de investigación utilizada fue una investigación básica, así mismo se aplicó un diseño no experimental, de tipo transversal con un enfoque correlacional causal, también se aplicó el muestreo no probabilístico aleatorio simple, se consideró una muestra de 79 colaboradores de la empresa en la que se realizó la investigación, la información se recolectó a través de la técnica de investigación de la encuesta, realizándose un cuestionario.

Los resultados obtenidos al realizar el análisis estadístico en el cual me apoyé en el software SPSS que dio como resultado que el R^2 de Nagelkerke fue del 70.6%, este resultado indica que la variable Ciberseguridad posee un nivel considerable de incidencia; del mismo modo se alcanzó un valor de significancia de p= 0.000, siendo este inferior al 0.05, de tal modo que podemos determinar que si existe una incidencia de la variable Ciberseguridad en la variable Gestión de Tecnologías de información.

Palabras clave: Ciberseguridad, Gestión de Tecnologías de Información, ciberataque

Abstract

The present investigation was carried out with the purpose of determining the incidence of Cybersecurity in the Management of Information Technologies in an Insurance company, Lima 2022.

The type of research used was a basic research, likewise a non-experimental design was applied, cross-sectional with a causal correlational approach, simple random non-probabilistic sampling was also applied, a sample of 79 employees of the company was excluded in the that the investigation was carried out, the Information was collected through the survey research technique, doing a questionnaire.

The results obtained when carrying out the statistical analysis in which I relied on the SPSS software gave as a result that the R2 of Nagelkerke was 70.6%, this result indicates that the Cybersecurity variable has a considerable level of incidence; In the same way, a significance value of p= 0.000 was reached, this being less than 0.05, in such a way that we can determine if there is an incidence of the Cybersecurity variable in the Information Technology Management variable.

Keywords: Cybersecurity, Information Technology Management, cyberattack

I.INTRODUCCIÓN

Sabemos que la tecnología se encuentra en un crecimiento constante y acelerado, en esta nueva normalidad las personas hemos modificado nuestros hábitos de consumo, así como la manera en la que nos comunicamos, por su lado las organizaciones vienen adaptándose a nuevos modelos de negocios, debido a la competitividad que existe a nivel mundial de manera continua se vienen generando diferentes maneras de gestionar que en su mayoría se encuentran relacionadas a la innovación tecnológica.

A nivel internacional, Flores et al. (2019) indica que gestionar la innovación tecnológica impulsa la calidad del servicio y la competencia entre organizaciones, así mismo hace uso de la tecnología para aprovechar los bienes organizacionales de tal manera que estos beneficien a sus clientes, esta tecnología debe estar orientado a optimizar los recursos humanos, económicos y tecnológicos; planificar, ejecutar y controlar en base a las innovaciones tecnológicas vienen representando una gran reto para las empresas a nivel mundial; en Ecuador las organizaciones que integran la tecnología y el soporte a sus procesos buscan proporcionar a sus clientes un mejor servicio, sin embargo no incorporar la Gestión de Tecnologías de la Información viene ocasionando que los servicios que brindan no sean sobresalientes en el mercado, encontrándose que el 50% de las organizaciones evaluadas cuentan con una infraestructura tecnológica deficiente y que el 75% no incluye en sus presupuestos inversión tecnológica lo cual genera una gran desventaja que no permite mejorar los procesos, automatizarlos, implementar medidas de seguridad, proteger la información de sus clientes, convirtiéndolos en blanco fácil de los ciberdelincuentes, Check Point (2022) menciona en su reciente investigación que los ciberataques a las organizaciones a nivel mundial durante el 2021 ha aumentado en un 50% comparado a lo sucedido en el 2020, México es el primer país en Latinoamérica que sufre de intentos de ciberataques de lo que va de enero a junio del 2022 con un total de 85.000 millones, seguido de Brasil con un total de 31.500 millones de intentos de ciberataques en ese mismo período.

A nivel nacional, en un estudio realizado por el INEI (2020), menciona que las grandes empresas en Perú cuentan con mayor capacidad de inversión de manera que implementan diferentes tecnologías tanto de información como de comunicación mejorando así la Dirección en cuanto a sus tecnologías; en el caso de empresas pequeñas utilizan menos la tecnología, generando el aumento en sus costos, pérdidas de tiempo y clientes lo cual hace que sus ganancias se vean reducidas, aun así está poca o elevada inversión en tecnología no implica que no puedan ser víctimas de ciberdelincuentes, el Ministerio de la Producción (2022) indica que debido a la pandemia las organizaciones comprendieron que deberían de incorporar más herramientas digitales a sus actividades comerciales, lo que facilitó que nuestro país sufriera 11.5 mil millones de intentos de ciberataques durante el 2021. En el Perú se cuenta con algunas normas relacionadas con la ciberseguridad como son la Ley Nº 30999 de Ciberdefensa, Ley N° 27269 sobre los Certificados y Firmas Digitales; Ley N° 28493 sobre la regulación de correos spam; Ley N° 29733 de Protección de Datos Personales y algunas más; pese a ello según el Gerente de ESET Perú, nos define como un país que reacciona antes de ser uno que previene en cuanto a seguridad se refiere.

Por otro lado a nivel local se tiene que la SBS y AFP(2021) mediante Resolución N° 504-2021 para efectos de gestionar la seguridad de la información así como la seguridad cibernética, adoptaron el presente reglamento asumiendo que las organizaciones cuentan con un entorno seguro en el cual brindar productos y servicios a sus usuarios, de tal manera que puedan estar preparados ante los posibles riesgos que están asociados a la seguridad informática y seguridad en el espacio esto debido al avance tecnológico y el incremento de la interconectividad entre las organizaciones y la transformación digital. Según el diario el Comercio (2022) se tiene que casi un 75% de las empresas ha sido víctima de los ciberataques en el 2021, según un informe elaborado por la empresa de correduría de seguros y consultora de riesgos Marsh en conjunto con Microsoft se tiene que una de las consecuencias de la interrupción del trabajo presencial tras casi tres años producto de la pandemia es que las empresas desconfían de su capacidad para poder gestionar el riesgo en cuanto a ciberseguridad se refiere. Pero pese a esta

desconfianza poco a poco se viene implementando medidas y/o políticas de seguridad gracias a la gestión de las TI.

Bajo este contexto está empresa de seguros con su sede principal en Lima y en la que se realizará la presente investigación es consiente que el trabajo remoto y la digitalización los expone a más ciberataques y fugas de información, es por ello que actualmente se viene implementando el marco de seguridad FFIEC (Federal Financial Institutions Examination Council) se espera que estos controles se lleguen a implementar en su totalidad a finales del 2022, así mismo está empresa viene avanzando con la implementación de la norma SBS 504-2021 que es el reglamento que gestiona la seguridad informática y la seguridad en el espacio, así mismo esta ha incrementado en un 80% el personal experto en detección, respuesta, protección y recuperación de ciberataques.

Por lo antes expuesto se plantea como problema general ¿De qué manera la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?, también detallaremos problemas específicos: i) ¿De qué manera la dimensión prevención de la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?, ii) ¿De qué manera la dimensión detección de la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?, y iii) ¿De qué manera la dimensión recuperación de la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?

Así mismo se considera de suma importancia justificar está investigación, la misma que hace énfasis en cuatro ámbitos: tenemos la justificación epistemológica que se relaciona con este trabajo de investigación ya que se tendrá en cuenta cada una de la teorías y conceptos científicos válidos las mismas que serán usadas para poder formular de manera correcta el problema de investigación, así mismo tomando en cuenta las evidencias que se recogerán se podrá obtener las validaciones a las hipótesis que se definirán líneas abajo.

Cómo justificación teórica para el presente trabajo se buscará incrementar y generar información relacionada con la ciberseguridad, la gestión de tecnologías de

información, así como sus dimensiones respectivas, dichos nuevos conocimientos servirán como antecedentes y ayudarán a enriquecer el marco teórico a futuras investigaciones.

Así mismo tenemos la justificación práctica, la cual está enfocada en resolver la interrogante general que va a permitir a la empresa de seguros dónde se realiza la investigación si debe continuar adoptando y mejorando su ciberseguridad de tal modo que contribuya a una adecuada Gestión de TI.

En cuanto a la justificación metodológica nos enfocaremos en el diseño de tipo no experimental y emplearemos técnicas de investigación cuantitativa que en este caso será el cuestionario con los cuales se recolectaran datos que serán procesados de tal manera que nos permita validar nuestras hipótesis.

Por lo ya mencionado, se plantea como objetivo general: Determinar la incidencia de la Ciberseguridad en la Gestión de tecnologías de Información en una empresa de Seguros, Lima 2022, así mismo como objetivos específicos tenemos: i) Determinar la incidencia de la dimensión prevención de la Ciberseguridad en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022, ii) Determinar la incidencia de la dimensión detección de la Ciberseguridad en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022 y iii) Determinar la incidencia de la dimensión recuperación de la Ciberseguridad en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

Así mismo como hipótesis general tenemos lo siguiente: La Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022. Además como hipótesis específicas lo siguiente: i) La dimensión prevención de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022; ii) La dimensión detección de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022 y iii) La dimensión recuperación de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

II.MARCO TEÓRICO.

En esta investigación se están considerando algunos estudios previos como antecedentes nacionales e internacionales que respaldarán la investigación. Como trabajos previos nacionales tenemos a Mendoza et al. (2019) que en su investigación sobre las capacidades de detectar y dar respuesta a riesgos de ciberseguridad en una organización privada, tuvo como objetivo general identificar como la ciberseguridad está relacionada con la detección y respuesta a los eventos, los mismos que proponen un diseño de tipo no experimental y concluyen que está investigación será de apoyo a las empresas ya que les permitirá desarrollar un enfoque para mejorar sus capacidades de detección y respuesta a ataques cibernéticos, también concluyen que los riesgos principales de ciberseguridad encontrados fueron la intromisión de malware en sus servidores operacionales, la ausencia de procedimientos, personal especializado y el uso de medios de almacenamiento externo.

Así mismo se tiene que Bohórquez (2021) en el estudio que realizó sobre la Ciberseguridad y su relación con la Gestión de Tecnologías de Información (TI) en una empresa privada, se planteó como objetivo general la determinación del vínculo entre dichas variables, investigación de tipo no experimental, concluyéndose que la Ciberseguridad se relaciona de manera significativa con la Gestión de TI, así mismo concluye que las dimensiones prevención, detección y reacción de la variable independiente Ciberseguridad se relaciona de manera significativa con la variable dependiente Gestión de TI.

También tenemos a Huáman (2021) con su investigación sobre el análisis de las capacidades en ciberseguridad y ciberdefensa del ejército, cuyo objetivo general es explicar que la Ciberseguridad y la Ciberdefensa del Ejército brindan el soporte y apoyo y que también protegen la confiabilidad, la integridad y la disponibilidad de la información, la metodología utilizada fue la cualitativa con un enfoque teórico-empírico, el mismo que concluyó que las capacidades de ciberseguridad y ciberdefensa que brindan el soporte y apoyo a las diferentes Direcciones del ejército

todavía no son específicas, aunque el personal participe de seminarios, cursos, conferencias,etc., el proyecto que explica las capacidades aún se encuentra en proceso de implementación, así mismo también concluye que el uso de programas libres de licencia son las manera en que protegen la confiabilidad, la integridad y la disponibilidad de la información.

Del mismo modo tenemos que Moquillaza (2020) en su investigación sobre la Gestión de Tecnología de la Información y comunicación (TIC) y el nivel de servicio de diversos procesos de una Universidad Nacional, plantea como objetivo la de determinar la incidencia de la Gestión de TIC en la calidad de servicio, se utilizó un diseño de tipo no experimental, el mismo que concluye que el 53% de personas implicadas en el estudio, consideran que el proceso de Gestión de TIC incide en la importancia y la mejor de los servicios que se brinda, también se concluye que el 68% de los involucrados en está investigación, consideran que los objetivos y cualidades de la Gestión de TIC afectan el buen servicio que se prestan, el mismo que se refleja en los resultados, según evaluación realizada a los planes operativo y estratégico, así mismo el 51% de los implicados en la investigación consideran el Hardware y el Software utilizado como componente de las TIC's afecta el nivel de los servicios que se brinda.

Para los trabajos previos internacionales tenemos a Santos (2019) en su investigación titulada "O Fator Humano Da Cibersegurança Nas Organizações" del Instituto Superior de Economía y Gestión ubicado en Lisboa, Portugal, cuyo objetivo es comprender la influencia y transcendencia del factor humano en la ciberseguridad de las organizaciones, a través del cual se identifican comportamientos humanos, características que influyen y su impacto en los niveles de ciberseguridad alcanzados y las soluciones que permitan corregir estas situaciones, la metodología que se empleó fue la cualitativa de tipo no experimental, esta investigación concluye que el factor humano tiene una gran influencia en la ciberseguridad de las organizaciones y por lo tanto la solución que permite un cambio duradero es la creación de una sólida cultura de ciberseguridad a través de la sensibilización, educación y formación de los empleados.

Por otro lado Allauca (2022) en su investigación que hace referencia a una propuesta para mejorar las prácticas de Ciberseguridad a clientes de diversas corporaciones, Ecuador, en la misma que como objetivo general propone mejores prácticas de ciberseguridad en términos de la infraestructura de red de los clientes corporativos de un proveedor de servicio de internet, se emplea la metodología cualitativa de tipo experimental, finalmente se concluye que se logró identificar los problemas principales de Ciberseguridad que los clientes presentan, problemas que están relacionado con la infraestructura del proveedor de servicio de internet y con la ayuda de la norma ISO 27032, se obtiene las mejores prácticas de ciberseguridad, también el autor concluye que realizar este estudio comparativo en relación a los diversos ataques de ciberseguridad producidos, permitió conocer que el mayor ataque que se presenta a los clientes es mediante DoS y que mediante procedimientos aplicados se han logrado restablecer el servicio respectivo, posteriormente se les brindó recomendaciones de seguridad que deben ser aplicados en su equipos de red interna.

Así mismo Serna (2018) en su investigación realizó un análisis sobre la capacidad de la Ciberseguridad la misma que aplicó a la Dimensión Tecnológica, investigación realizada en Colombia, cuyo objetivo fue la de realizar un análisis de la capacidad de la ciberseguridad en la dimensión tecnológica en respuesta a diversos incidentes y a la protección de infraestructuras críticas, desde una perspectiva sistémica de la organización, para esta investigación se usó una metodología de simulación la cual parte de un Modelo de Madurez centrado en la competencia de la Ciberseguridad y teniendo en cuenta las buenas prácticas la misma que fue definida por el NIST y que obtuvo como conclusión que el nivel de riesgo organizacional representa un elemento evidente para la gestión de incidentes y la protección de infraestructuras, ya que va permitir dar la definición de lo que son estrategias en términos políticos, lineamientos del negocio, la parte tecnológica entre otros componentes que permitan enfrentar el peligro de la interconectividad, concluye también que el modelo ha permitido realizar la identificación de aspectos importantes, el mismo que evidencia la obligación de fortalecer el tiempo tanto de la detección, contención y erradicación de incidentes.

Tenemos también que Baquero (2018) en su investigación realizó un análisis sobre el uso de las tecnologías de información y comunicación (TIC) como sostén a la Gestión de empresas, investigación realizada en Ecuador, el mismo que tuvo como objetivo analizar cómo la Gestión de la TIC puede apoyar a aquellas empresas que directamente se orientan a ofrecer sus servicios en el campo del marketing digital, la metodología aplicada en este estudio fue cualitativa, la misma que concluye que esta empresa Ecuatoriana se orienta en temas operativos y en la resolución de conflictos diarios, debido a que no ha establecido de manera clara su visión, objetivos y estrategias, por lo que no cuenta con un parámetro que le permita Gestionar su TIC de manera correcta, también se concluye que está empresa cuenta con un manejo pobre de su marca, el mismo que no le permitido crecer y posicionarse en el mercado, el mismo que sugiere trabajar esta dificultar y resolverla los más antes posible.

Y como último antecedente internacional tenemos a Rodríguez (2018) con su investigación referente a la Gestión Tecnológica, que lo describe como un recurso de apoyo para la Auto-Sustentabilidad Económica y Competitividad, investigación realizada en México, cuyo objetivo fue adecuar un esquema de Gestión Tecnológica, basado en las necesidades del Parque Biotecnológico UAQ, para promover su autosostenibilidad económica y competitividad, la metodología usada fue la cualitativa, en dicha investigación se concluye que se debe proporcionar el conocimiento suficiente de los conceptos integrados en la Gestión de las Tecnologías, así mismo necesitan personal especializado, que permita lograr la autosostenibilidad en diversas áreas de trabajo que incluyen: Gerentes de Proyectos de Tecnología, Diseñadores de planes de negocios, profesionales de marketing y especialistas en propiedad intelectual, así mismo en este trabajo se concluye que los investigadores del Parque Biotecnológico deben generar más investigaciones enfocadas en la aplicación de procesos, se hace necesaria la inversión privada con la finalidad de desarrollar procesos y productos innovadores que fomenten la auto sustentabilidad del Parque Biotecnológico.

Con la finalidad de respaldar está investigación consideramos dos teorías, en primer lugar tenemos la Teoría General de Sistemas (TGS), dada por Ludwing Von Bertalanffy, al respecto Schuelter et al. (2005) manifiestan que la TGS se presenta como una forma de organización de sistemas complejos que puede ser representada como base para la unificación de diversos competencias científicas en los últimos tiempos, tiene como objetivo identificar los propiedades, principios y leyes característicos de los sistemas, en general, independientemente de cada uno, la naturaleza de los componentes que lo conforman y la relación entre ellos. Por otro lado, Pereira et al. (2016) indican que la TGS aplicada a la gestión busca establecer herramientas que teniendo en cuenta las complejidades organizativas específicas, así como la creación de instrumentos de análisis, facilita el desarrollo y mantenimiento de su procesos internos y externos, a través de medios que apoyen la calidad, la productividad, innovaciones tecnológicas y organizacionales, generando modelos de subsidios informacionales al procedimiento de toma de decisiones, conocimiento y agregación de valor a la modernidad, rentabilidad, competitividad y perpetuidad organizacional. Así mismo Marques et al. (2016) refieren que la TGS nos ayuda a comprender la interrelación entre los diversos sistemas que existen en la actualidad, y la complejidad de estas relaciones y que a través de los supuestos generales de esta teoría podemos estudiar la formación, organización, tendencias futuras, potencialidades de sistemas, entre otras cosas y por último en la TGS tenemos a Martínez et al. (2021) que manifiestan que los procesos de integración son el principal aspecto que diferencia a los sistemas de los agregados, la forma de cómo están organizados los componentes y las actividades de un sistema generan un sentido común o combinado, en otras palabras la coyuntura de las diversas autonomías vienen a determinar cuáles serán sus fines.

En referencia a la segunda teoría que respalda está investigación tenemos a la Teoría de la Administración planteada por Henry Fayol, al respecto Oliveira da Silva et al.(2018) mencionan que Fayol define a la administración como el acto de gobernar o administrar negocios públicos o privados, tratando de utilizar de la mejor manera el uso posible de todos aquellos recursos disponibles con el fin de poder

cumplir las metas de la organización, de manera genérica, la gestión pública y privada convergen en la medida en que necesitan planificación, organización, dirección y control de las acciones. Por su lado Matos et al. (2006) indican que Fayol planteó la simplificación de la distribución administrativa y de tal manera que la organización ahora se comprende como un resumen de los diferentes órganos que conforman su estructura, enfatizando las funciones y operaciones dentro de la empresa, así mismo implementó las bases de la administración, siendo su visión clásica las funciones del gerente: organizar, planificar, coordinar, mandar y controlar. Por otra parte, Velásquez (2002) manifiesta que en la teoría de la administración se definió las funciones básicas de la organización, así como el concepto de administración y sus principios generales, las mismas que pueden ser aplicadas a cualquier organización y/o empresa. Y por último tenemos a Espinoza (2009) en la que concuerda con que el autor de la teoría definió los principios generales de la administración, indicando que sin estos principios la función administrativa no contaría con una guía y estaría desorientada, en referencia a estos principios estos son flexibles y pueden adaptarse a diversas circunstancias y necesidades.

Para esta investigación hemos considerado dos variables las mismas que serán parte de este estudio, son la Ciberseguridad y la Gestión de Tecnologías de Información, para una mejor compresión se han recopilado varias definiciones de cada una de ellas, en primer lugar tenemos a la variable independiente, Leiva (2015) define a la Ciberseguridad como procedimientos de uso, procesos y las nuevas tecnologías que van a permitir la prevención, detección y recuperación de aquellos daños que se puedan provocar a la confidencialidad, integridad y disponibilidad de la información en el espacio cibernético. Así mismo Rauscher et al. (2011) definen a la Ciberseguridad como una característica del ciberespacio, cuya capacidad es la de resistir amenazas que tengan o no intención, de responder a ellas y recuperarse. Según el estándar técnico UIT-T X.1205 (2008) define a la ciberseguridad como una combinación de herramientas, diversas políticas, así como conceptos, dispositivos de seguridad, lineamientos, prácticas para gestionar riesgos, operaciones, capacitaciones, mejorar prácticas y herramientas de seguridad. La tecnología se

puede utilizar para poder proteger los diversos activos corporativos, así como de los usuarios que podemos encontrar en la red. ambiente. Por su lado Hurel (2021) la define como la agrupación de acciones encaminadas a la seguridad de las operaciones, con el fin de garantizar que los sistemas de información sean capaces de soportar eventos en el ciberespacio capaces de implicar la disponibilidad, integridad, confidencialidad, autenticidad de los datos que se han almacenado, procesado o transmitido, así como de los servicios que los sistemas ofrecen o permiten que sea accesible y por último de acuerdo al Decreto de Urgencia Nº 007-2020 (2020) dictaminada por el consejo de ministros; definen a la ciberseguridad como la capacidad tecnológica que garantizará el normal funcionamiento de las redes, recursos y sistemas informáticos, y los protegerá frente a amenazas y vulnerabilidades en el ciberespacio.

De acuerdo al concepto definido por Leiva (2015) tendremos como dimensiones de la Ciberseguridad a la prevención, detección y recuperación. Al respecto para la definición de la primera dimensión Romero et al. (2018) nos dice que la prevención hace referencia a diversas revisiones que se realizan de manera periódica, también a los cambios o mejoras que se puedan dar en diferentes aspectos como hardware, software o de cualquier otro elemento que esté involucrado con los softwares u procesos de la institución. Así mismo Cando et al. (2021) definen a la prevención como la alternativa que permite contrarrestar eventos de tipo maliciosos y que brinda a los usuarios diversas herramientas que nos van a otorgar confianza para la navegación en el ciberespacio. Por otro lado, Defaz et al. (2006) nos dice que la prevención es aquella que se encarga de preparar los equipos que puedan recibir posibles ataques, así mismo es aquella encargada de mantener buenas políticas de seguridad y de este modo reaccionar al momento y evitar un posible ataque. En cuanto a Miró (2011) indica que es la adopción de diferentes medidas que van a evitar realizar conductas que faciliten alguna ejecución de delito, consiste en capacitar a las posibles víctimas para que cuenten con una mejor autoprotección, adoptando diversas rutinas seguras, potenciando la utilización de sistemas en las que eviten riesgos que no sean deseados y como última definición Moreno et al.(2019) nos dice que la prevención es aquella que se anticipa a controlar los

posibles crímenes que se podrían generar por diversos medios digitales, para lo cual es muy indispensable contar con un marco de prevención la cual contenga varias capas para la realización de monitoreo, las mismas que son definidas por cada organización de acuerdo al tipo de negocio, requerimientos y/o transacción que está realiza.

Ahora en la dimensión segunda de nuestra variable Ciberseguridad Defaz et al. (2006) define a la detección como encargada de detectar los diversos ataques que en su momento se encuentren sucediendo, de tal modo que estos puedan ser contrarrestados de manera debida, una de sus principales funciones es la de identificar y eliminar las vulnerabilidades y ataques. Ahora para el Marco de Ciberseguridad del NIST (2018) menciona que la detección es aquella que desarrolla e implementa actividades necesarias que permiten identificar ocurrencias de un evento de seguridad cibernética, tales como anomalías y eventos, monitoreando de manera continua la seguridad y los procesos de detección. Para Wang et al. (2022) la detección es un enfoque proactivo que permite identificar diversas amenazas dentro de la red de una organización, ayudando así la reducción del tiempo entre la intrusión y el descubrimiento, de esta manera se mitiga los posibles daños causados por los atacantes. Ahora Liu et al. (2022) nos dicen que consiste en buscar agentes externos y/o intrusos que sean peligrosos en la red de la organización, esta búsqueda puede ejecutarse en diversos grados de automatización o también de manera manual y finalmente Kumar et al. (2021) nos dicen que la detección es aquella que permite reconocer, catalogar y calificar las vulnerabilidades tanto en las computadoras, la infraestructura de la red, el software y hardware.

Respecto a la tercera y última dimensión de la Ciberseguridad tenemos a Staves et al. (2022) que nos dicen que la recuperación es definida como la unión de diferentes técnicas y procedimientos empleados para extraer y acceder a información que se encuentre en un almacenamiento digital, que por diversos motivos estos se encuentren dañados o averiados y que no son accesibles de manera normal. Para Defaz et al. (2006) la recuperación sucede cuando todo el equipo vuelve al estado

de cómo se encontraba en un principio, borrando y/o eliminando el ataque de tal manera que permita a los usuarios continuar normalmente. En el caso de Kolosok et al. (2022) nos indican que son acciones realizadas ya sea por el sistema operativo, el personal o por un equipo especializado con la finalidad de restaurar los sistemas en condiciones que permitan retomar el trabajo después de ocurrido el fallo. Ahora el Marco de Ciberseguridad del NIST(2018) define a la recuperación como aquel procedimiento que permite fomentar e implantar actividades adecuadas para preservar los planes de resiliencia y para restablecer cualquier capacidad o servicio que se vio afectado debido a un incidente, mejorando así la posibilidad de recuperarse frente a la reincidencia de eventos y por último tenemos a Naseer et al. (2021) que nos dice que la recuperación es la fase donde se aplican mejoras en los planes de ciberseguridad, esto incluye las aplicaciones de parches y/o actualizaciones, cambio de contraseñas y finalmente el cierre de puntos de acceso, así mismo debe realizarse la redacción de la documentación de los incidentes ocurridos y exponer a los que se encargan de tomas decisiones en la organización.

En referencia a la variable dependiente también se cuenta con diversas definiciones que a continuación serán presentadas, Mendoza et al. (2014) definen a Gestión de Tecnologías de Información (TI) como esa unión entre tres niveles, haciendo referencia a la dirección estratégica, transferencia e innovación tecnológica esto permitirá organizar y dirigir racionalmente al capital humano y económico hacia un incremento de nuevos conocimientos, permitiendo generar infinidad de nuevas ideas técnicas, mediante las cuales se puedan elaborar productos, procesos y/o servicios o talvez incrementar los ya existentes. Por su lado De la Cruz (2021) definen a la Gestión de TI como la estructura de comunicaciones y procedimientos para orientar e inspeccionar a la organización camino al cumplimiento de sus objetivos agregando valor y/o tiempo, logrando un equilibrio entre riesgo y retorno de TI y sus procedimientos, constituye e integra las buenas prácticas que garantiza que las tecnologías en la organización apoye los objetivos comerciales, facilite a la organización utilizar la mayor información, maximizando beneficios, capitalizando oportunidades y obteniendo diversas ventajas competitivas. Así mismo Ramirez et al. (2019) explican que Gestión de TI es aquella que integra procesos, que cuentan

con características estratégicas, operativas y toma de decisiones de la organización, el mismo que representa un valor competitivo, formando parte del planteamiento estratégico, en las que se vincule las actividades de investigación, desarrollo, innovación, producción y administración estratégica. Fuenmayor et al.(2017) explican que la Gestión de TI es un procedimiento que necesita diversos recursos para poder transformarse y generar productos, dichos procesos operan según la naturaleza en que se encuentre cada contexto organizacional y por último tenemos a Senior et al. (2006) que conceptualizan a la Gestión de TI como un conjunto de actividades estratégicas de naturaleza técnica-gerencial, las que se implementan en una organización de tal forma que permitan manejar y controlar la variable tecnológica, mediante procesos y diversos métodos que servirán para mejorar la producción en una organización, logrando así maximizar sus resultados.

De acuerdo a la definición de Gestión de Tecnologías de Información conceptualizada por Mendoza et al. (2014), tendremos como dimensiones: la Dirección estratégica, Transferencia tecnológica y la Innovación tecnológica. Para la primera dimensión, Burbano (2017) nos dice que la Dirección estratégica consiste en formular estrategias que permitan el desarrollo de la organización, buscando de esta manera generar una mayor participación en el mercado y procurando siempre obtener mayores rendimientos. En el caso de Arano et al. (2011) la describe como un conjunto de compromisos, decisiones y acciones que van a permitir a una empresa distinguirse de otras de tal modo que está sea más competitiva, generando una mayor rentabilidad por encima de las empresas promedio. Para Peralta et al. (2020) nos dice que la Dirección estratégica es aquella que trabaja por integrar todos sus esfuerzos con los planes de actuación de cada área de la organización con diversos factores externos que convergen entre sí de tal manera que puedan obtener el éxito empresarial. Huerta et al. (2020) nos dice que la Dirección estratégica es un procedimiento en el que una organización tiene pensado lograr ventajas competitivas sostenibles que van a permitir lograr el éxito, lo que implica que se logre una afinidad entre los recursos y capacidades de la organización con los requerimientos del entorno y sector específico en el que opera y finalizando con las definiciones de esta dimensión tenemos a Armijos et al. (2020) que considera a

la Dirección estratégica como el norte empresarial, definido a través de estrategias centrales para gestionar la organización en períodos cortos, medianos y largos, logrando de esta manera posicionarse en el mercado asegurando así la sostenibilidad en el tiempo.

Respecto a la dimensión segunda de nuestra variable Gestión de Tecnologías de Información Conti et al. (2015) nos dicen que la Transferencia tecnológica se clasifica como un proceso que incluye los siguientes elementos: usuarios, proveedores, tecnología, comunicación, implementación y estructura u organización, definir la Transferencia tecnológica como un proceso significa que se compone de elementos interrelacionados que en última instancia tienen como objetivo cubrir las necesidades de los usuarios de esa manera poder levantar el nivel de vida. Sonmezturk et al. (2022) indican que la Transferencia tecnológica se puede definir como el traslado de conocimientos, de una institución a otra, en este caso, el flujo de conocimiento tecnológico es intencional y se materializa en mecanismos específicos de transferencia. Por su lado Mccormick et al. (2022) nos dicen que es el proceso de puesta en marcha e instalación de un nuevo producto o proceso en una planta de fabricación, la misma que implica la transferencia de conocimientos y experiencia documentados, acumulados durante el desarrollo y/o la producción a gran escala y requiere una demostración por parte de la instalación receptora de su capacidad para lograr todos los parámetros críticos del proceso. Para Macharia et al. (2019) es el proceso que se produce a través de un esfuerzo combinado para compartir habilidades, conocimientos, tecnologías, métodos de fabricación entre el agente de transferencia y el destinatario para garantizar que los desarrollos científicos y tecnológicos sean accesibles para el destinatario, que luego pueden hacer avanzar la tecnología mediante la producción de nuevos productos o servicios o procesos y procedimientos y finalmente Bozeman (2000) nos dice que la Transferencia tecnológica se ha utilizado para detallar y analizar una gama de interacciones organizacionales e institucionales que involucran alguna forma de intercambio relacionado con la tecnología.

Para la definición de la tercera dimensión de la Gestión de Tecnologías de Información encontramos que Estrada et al. (2019) definen que innovar tecnológicamente en las empresas no trata simplemente de aplicar exitosamente ideas nuevas de productos y/o servicios, en diferentes ocasiones estos van a requerir que se generen cambios a nivel organizacional así como de estrategias que lo soporten. Fuck et al. (2011) nos dicen que la Innovación tecnológica se caracteriza por ser un proceso multifacético que implica la integración de varias funciones de la empresa y actores externos, se basa fundamentalmente en actividades realizadas en la empresa, pública o privada, haciendo énfasis en el esfuerzo, desarrollo y contratación de personal calificado. Ahora Amponsah et al. (2022) la definen como la formación de nuevos productos y procesos dentro de las empresas, las innovaciones, ya sean tecnológicas o no tecnológicas, requieren el descubrimiento de nuevos conocimientos e ideas como ingredientes clave para el éxito y el mantenimiento, las fuentes de estas nuevas ideas y conocimientos se derivan principalmente de la investigación y el desarrollo. En el caso de Scherer (2002) la Innovación tecnológica tiene el propósito económico de incluir tecnologías emergentes tanto en la producción así como en el consumo, está misma debe reconocer nuevas posibilidades tecnológicas, organizar al capital humano y financiero indispensable para transformar en productos y procesos útiles y como última definición citamos a Yu et al. (2011) que nos dicen que la Innovación tecnológica es la forma en que una organización puede seleccionar, implementar y utilizar eficientemente una tecnología en comparación con un competidor, también se puede incluir el conocimiento profesional necesario para diseñar, fabricar y ensamblar un producto o la eficiencia del personal en el uso de las herramientas de producción.

III. METODOLOGÍA

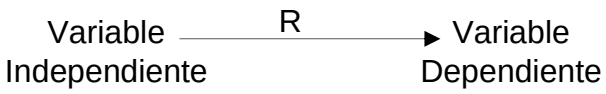
3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

Para este estudio aplicamos una investigación básica, al respecto Patel et al. (2019) nos indican que la definición de este tipo de investigación hace referencia a que investiga con la finalidad de mejorar el conocimiento, se realiza con la intención de superar hechos desconocidos, se preocupa por las leyes generales y también por formular una nueva teoría, puede o no producir soluciones o resultados al problema actual pero aporta conocimiento a la ciencia, así mismo tenemos la Ley Nº 31250:Ley del SINACTI (2021) en la que se dispone que la investigación básica está canalizado hacia un entendimiento más absoluto que permite comprender conocimientos y/o características fundamentales de los fenómenos, acontecimientos inspeccionables o las relaciones que establecen los entes.

3.1.2. Diseño de investigación

En la presente aplicamos un diseño no experimental, de tipo transversal con un enfoque correlacional causal, al respecto Hernández et. al (2018) mencionan que en este diseño lo que hacemos es mirar o cuantificar fenómenos y variables en su hábitat con la finalidad de poder analizarlos, es decir se analiza el efecto que genera la variable independiente sobre la dependiente; ahora bien al aplicar un diseño transversal significa que se recolectarán datos en un momento dado, así mismo el enfoque correlacional causal los mismos autores lo definen como un enfoque útil que nos permite establecer vínculos entre dos o más variables en un momento dado, a continuación se presenta el esquema correspondiente a este diseño:



Tenemos:

Variable Independiente: Ciberseguridad

Variable Dependiente: Gestión de Tecnologías de Información

R: Relación Causal

3.2. Variables y Operacionalización

Variable Independiente: Ciberseguridad

La Ciberseguridad hace referencia a una variable cualitativa de tipo categórica, Cienfuegos et al. (2016) define una variable cualitativa de tipo categórica como aquella que denota cualidad que no permiten operaciones aritméticas y están clasificados en números fijos categóricos manteniendo un orden y admitiendo la igualdad y desigualdad.

Definición Conceptual de la variable Ciberseguridad

Leiva (2015) define a la Ciberseguridad como procedimientos de uso, procesos y las nuevas tecnologías que van a permitir la prevención, detección y recuperación de aquellos daños que se puedan provocar a la confidencialidad, integridad y disponibilidad de la información en el espacio cibernético.

Definición Operacional de la variable Ciberseguridad

Se operacionalizó mediante 3 dimensiones: prevención, detección y recuperación, estás serán medidas mediante el cuestionario en la que se utilizará la escala de Likert, la misma que basamos en 5 categorías: (1) No tengo acceso, (2) Poco acceso, (3) Ni poco, ni mucho, (4) Tengo acceso, (5) Tengo acceso a todo (ver anexo 2).

Variable Dependiente: Gestión de Tecnologías de Información

Esta variable hace referencia a una cualitativa de tipo categórica, Cienfuegos et al. (2016) define una variable cualitativa de tipo categórica como aquella que denota

cualidad que no permiten operaciones aritméticas y están clasificados en números fijos categóricos manteniendo un orden y admitiendo la igualdad y desigualdad.

Definición Conceptual de la variable Gestión de Tecnologías de Información

Mendoza et al. (2014) definen a esta variable como esa unión entre tres niveles haciendo referencia a la dirección estratégica, transferencia e innovación tecnológica que permiten a la empresa y la gestión del capital humano y económico potenciar y generar muchos tipos de conocimiento, generando ideas técnicas que pueden ser utilizadas para obtener productos, procesos y servicios nuevos o aumentar los existentes y convertir estos ideales en prototipos.

Definición Operacional de la variable Gestión de Tecnologías de Información

Hemos operacionalizado mediante 3 dimensiones: dirección estratégica, transferencia e innovación tecnológica, estás serán medidas mediante el cuestionario en la que se utilizará la escala de Likert, la misma que basamos en 5 categorías: (1) No tengo acceso, (2) Poco acceso, (3) Ni poco, ni mucho, (4) Tengo acceso, (5) Tengo acceso a todo (ver anexo 2). (ver anexo 2).

3.3. Población, muestra y muestreo

3.3.1. Población

Para Villasís et al. (2016) la población de estudio es aquel conjunto de casos, que está definido, se encuentra accesible, es el referente para elegir nuestra muestra y que a su vez cumple con diversos criterios predeterminados, el mismo que no solo se refiere a humanos, sino que también corresponde por ejemplo animales, familias, objetos, etc. Para está investigación se ha tomado como población a 100 trabajadores de esta empresa de Seguros, se incluyen a los trabajadores que se encuentran laborando para diversas áreas de manera remota y presencial (modalidad híbrida) los mismos que corresponden a la sede principal ubicada en Lima, distrito de San Isidro.

Tabla 1

Detalle de la Población de la empresa de Seguros

Población	Cantidad
Gerentes	3
Subgerentes	3
Supervisores	9
Jefes de área	6
TI	15
Colaboradores	64
Total	100

Acotación: Información brindada por la División de GDH y Administración (2022)

3.3.2. Muestra

Hernández et al. (2018) nos dicen que viene a ser un subconjunto de la población o parte del universo que formar parte de nuestro interés, en la misma que recolectaremos los datos correspondientes y esta muestra deberá ser parte representativa de nuestra población. La muestra en el presente trabajo de

investigación corresponde a 79 trabajadores, el cual se calculó utilizando el programa Decision Analyst STATS™ 2.0, tomando en cuenta que se tendrá un porcentaje de error aceptable del 5% y un nivel de confianza del 95%.

Tabla 2

Detalle de la muestra poblacional

Población	Cantidad
Gerentes	1
Subgerentes	1
Supervisores	5
Jefes de área	3
TI	8
Colaboradores	61
Total	79

Acotación: Elaborado por autora

3.3.3. Muestreo

Aquí se usó un muestreo probabilístico cuyo tipo fue aleatorio simple, conforme mencionan Hernández et al. (2018) que este tipo corresponde a la muestra poblacional en el que la totalidad de involucrados tienen la misma probabilidad de ser elegidos, para obtener está muestra se definen peculiaridades de la población y así mismo el tamaño apropiado, mediante una elección aleatoria para nuestras unidades de muestreo.

3.3.4. Unidad de Análisis

En la presente investigación la unidad de análisis son los trabajadores de esta empresa de Seguros.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

La técnica que se utilizó fue la encuesta, al respecto Hernández et al. (2018) manifiestan que es una técnica que se emplea para reunir información de personas en lo que respecta a sus características, opiniones, creencias, expectativas, conocimiento, conducta actual y/o pasada, etc.

Instrumentos de recolección de datos

Se utilizó el cuestionario, Hernández et al. (2018) nos dicen que este es un conjunto de preguntas en referencia a las variables que se van a medir, utilizan encuestas de todo tipo, cuyo contenido de preguntas es muy variado, así como los aspectos que mide (ver anexo 3). En la siguiente tabla podemos ver a detalle de la ficha técnica de nuestro instrumento de medición:

Tabla 3

Ficha técnica del instrumento de medición

Nombre del Instrumento	Cuestionario para los trabajadores de la empresa de seguros		
Investigadora:	Taína Licel, Ramírez Alva		
Año:	2022		
Instrumento:	Cuestionario		
Fin:	Determinar la incidencia de la Ciberseguridad en la Gestión de tecnologías de Información en una empresa de Seguros, Lima 2022		
Población:	79 trabajadores		
Items:	Tenemos 36: VI(18) y VD(18)		
Aplicación:	En línea		
Tiempo utilizado:	3 minutos		
Escala	Likert: (1) No tengo acceso, (2) Poco acceso, (3) Ni poco, ni mucho, (4) Tengo acceso, (5) Tengo acceso a todo (ver anexo 2)..		
Niveles y rangos	Variable independiente: Ciberseguridad		
	Nivel	Valor	Rango
	Baja Prevalencia	1	18-42
	Media Prevalencia	2	43-67
	Alta Prevalencia	3	68-90
	Variable dependiente: Gestión de Tecnologías de Información		
	Nivel	Valor	Rango
	Nada Óptimo	1	18-42
	Regular	2	43-67
	Óptimo	3	68-90

Acotación: Elaborado por la autora

Validez

En lo que respecta a la corroboración del mecanismo se ha validado dicho instrumento con lo que conocemos juicio de expertos, para Hernández et al. (2018) la validación de expertos hace referencia al nivel en que el instrumentos mide la variable de interés, para nuestro caso en esta evaluación se ha tenido en cuenta la claridad, pertinencia y relevancia de los temas que se han planteado en el instrumento brindado frente a las dimensiones de cada variable mencionadas en el presente estudio (ver anexo 4). Para validar nuestro instrumento se ha contado con los profesionales siguientes:

Tabla 4

Validación de juicio de expertos

DNI	Experto	Procedencia	Calificación
09656793	Dr. Pedro Martín Lezama Gonzales	Univ. César Vallejo	Aplicable
41567782	Mg. Dino Michael Quinteros Navarro	Univ. César Vallejo	Aplicable
00865537	Dr. Carlos Enrique López Rodríguez	Univ. Nacional de San Martín-Tarapoto	Aplicable

Acotación: Elaborado por la autora

Confiabilidad

En lo que respecta a Hernández et al. (2018) para ellos la confiabilidad está definido como el grado en el que un instrumento producirá resultados que van a ser consistentes y coherentes en una muestra y/o instancia donde su interpretación se medirá con la misma consistencia interna que el alfa de Cronbach. Para calcular la confiabilidad de nuestro instrumento se realizó una prueba piloto en base a 10 encuestas, en las cuales se ha obtenido un valor en el canal alfa de Cronbach de 0.929, así mismo en la muestra total que fue aplicada a 79 encuestados se obtuvo una alfa de Cronbach de 0.830, de acuerdo a Hernández et al. (2018) el alfa de Cronbach oscila en una escala de 0 y 1, donde cero (0) equivale a una confiabilidad nula y uno (1) equivale al máximo grado de confiabilidad, es decir que mientras esté más próximo a 1 más consistentes serán nuestros ítems entre sí. A continuación, se muestra el detalle del resultado obtenido en el análisis de confiabilidad de esta investigación:

Tabla 5

Prueba de confiabilidad

Aplicación	Nº de encuestas	Nº de elementos	Alfa de Cronbach
Piloto	10	36	0.929
General	79	36	0.870

Acotación: Elaborado por la autora con apoyo de SPSS Statistics

3.5. Procedimientos.

Los procedimientos realizados para obtener resultados estadísticos en esta investigación se llevaron a cabo en las siguientes etapas: 1. Diseñar una herramienta de recolección de datos. 2.Validación de la herramienta mediante el juicio de expertos, para el caso se considerarán a 3 expertos que validaron la herramienta como aplicable. 3. Se usó una muestra de prueba con la finalidad de analizar la validez del instrumento, posterior a ello se aplicó a toda la muestra poblacional. 4. Con la información recolectada, se procedió a ingresar los resultados en un editor de hojas de cálculo denominado Excel, estos resultados y/o datos posteriormente fueron procesados utilizando el software SPSS, con lo que se obtuvo datos descriptivos e inferenciales que permitieron contrastar la hipótesis y el nivel de incidencia de ambas variables.

3.6. Método de análisis de datos

Ahora en esta investigación se realizó un análisis descriptivo e inferencial con todos nuestros indicadores, para eso nos apoyamos con los programas IBM SPSS Statistics versión 25.0.0 y Excel lo que nos permitió cargar y tabular los resultados obtenidos en las encuestas.

En el análisis descriptivo se utilizó tablas de contingencia cuyo resultado se presentará mediante tablas e histogramas lo cual será dirigido a un análisis bidimensional.

El análisis inferencial se ejecutó mediante un análisis estadístico no paramétrico utilizando un coeficiente de regresión logística ordinal con el cual justificaremos de manera adecuada el grado de incidencia existente entre la variable independiente y la dependiente.

3.7. Aspectos éticos

Teniendo la finalidad de respaldar la integridad científica y cumplir con las normas que van a regular las buenas prácticas se trabajó bajo los lineamientos del código

de ética aprobado mediante resolución de Consejo Universitario Nº 0262-2020/UCV de la universidad César Vallejo en las que se sustentan las bases éticas de la presente investigación las mismas que se describen a continuación:

Respeto a la propiedad intelectual, este principio se aplicó respetando la autoría de los investigadores, citando a cada autor del que pudimos tomar como referencia para la presente investigación para esto nos basamos en la normativa de citas de APA.

Libertad, porque se realizó una investigación de manera libre e independiente de aspectos económicos, políticos y/o religiosos, permitiendo así una investigación destinada netamente a la búsqueda de conocimiento de manera particular.

Transparencia, porque se está permitiendo que la presente investigación sea difundida y/o publicada y que a su vez sirva como generador de conocimientos que permitan a otros investigadores aplicar y/o tomar como referencia este estudio de investigación.

IV. RESULTADOS

Análisis descriptivos

Análisis descriptivo de la variable ciberseguridad y la variable Gestión de Tecnologías de Información

Tabla 6

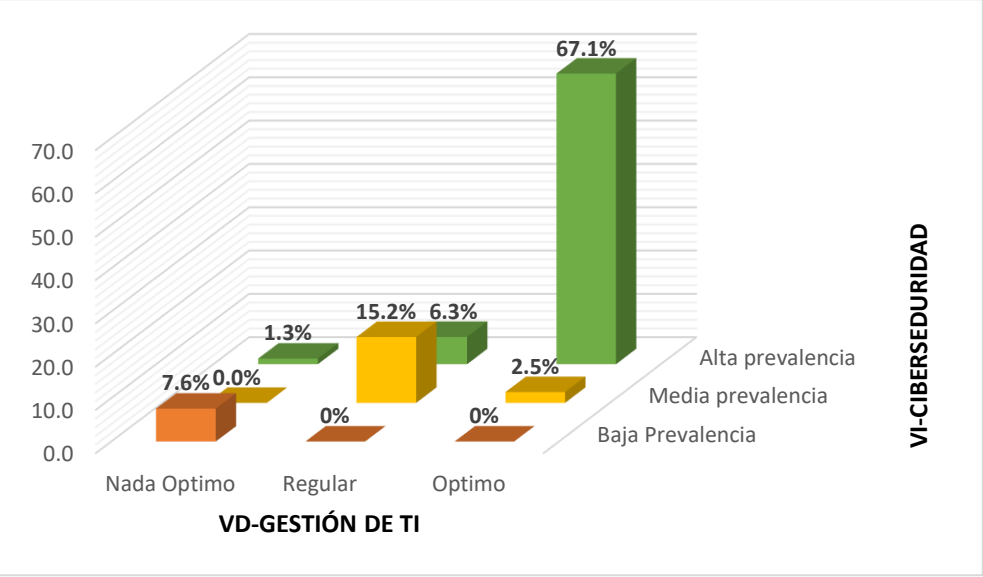
*Tabulación cruzada VI: Ciberseguridad * VD-Gestión de TI:*

		VD-Gestión de tecnologías de información			
		Nada Óptimo	Regular	Óptimo	Total
VI-Ciberseduridad	Baja Prevalencia	6 (7.6%)	0 (0.0%)	0(0.0%)	6 (7.6%)
	Media prevalencia	0 (0.0%)	12 (15.2%)	2 (2.5%)	14 (17.7%)
	Alta prevalencia	1 (1.3%)	5 (6.3%)	53 (67.1%)	59 (74.7%)
	Total	7 (8.9%)	17 (21.5%)	55 (69.6%)	79 (100.0%)

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel

Figura 1

*Histograma, VI-Ciberseguridad * VD-Gestión de TI:*



Acotación: Elaborado por la autora con apoyo de Excel

Con lo que respecta a la tabla 6, se pone en manifiesto que se obtiene mayor aceptación en el cruce de “Alta Prevalencia” de nuestra variable Ciberseguridad y “Óptimo” de nuestra variable Gestión de Tecnologías de Información conformado por un total de 53 contestaciones con una representación equivalente al 67.1% del total de encuestados; así mismo el menor índice se sitúa en el cruce de “Alta Prevalencia” de la variable Ciberseguridad y “Nada Óptimo” de la variable Gestión de Tecnologías de Información conformado por un total de 1 contestación el cual es equivalente al 1.3%. También tenemos cero contestaciones equivalentes al 0.0% en los niveles “Media Prevalencia” de nuestra variable Ciberseguridad y “Nada Óptimo” de nuestra variable Gestión de Tecnologías de Información y para finalizar podemos observar que el rango de mayor acogida es de 55 contestaciones el cual representa el 69.6% el mismo que corresponde a un nivel “Óptimo” de nuestra variable Gestión de Tecnologías de Información.

Análisis descriptivo de la dimensión Prevención de la variable Ciberseguridad y la variable Gestión de Tecnologías de Información

Tabla 7

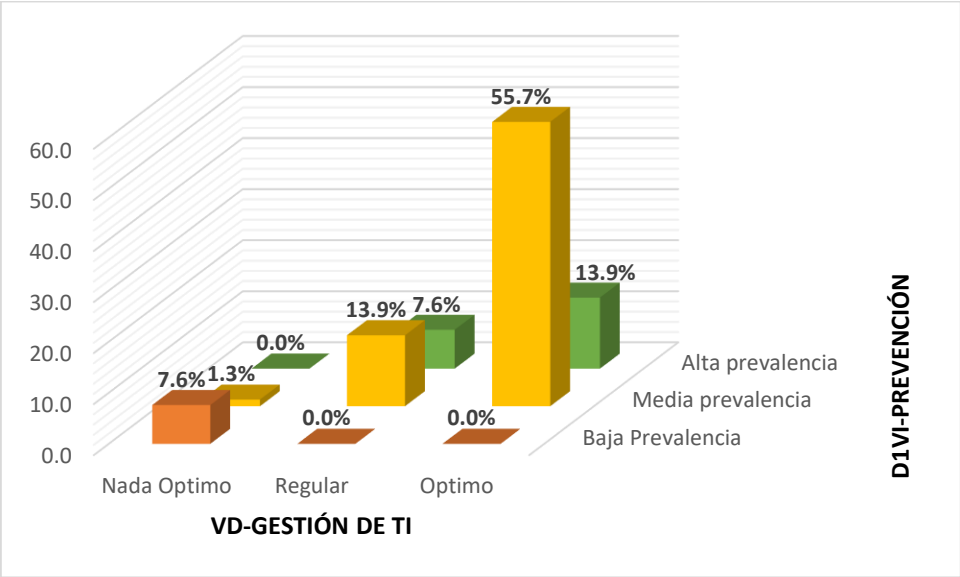
*Tabulación cruzada D1VI-Prevención de la Ciberseguridad * VD-Gestión TI:*

		VD-Gestión de tecnologías de información			
		Nada Óptimo	Regular	Óptimo	Total
D1VI-Prevención	Baja Prevalencia	6 (7.6%)	0 (0.0%)	0(0.0%)	6 (7.6%)
	Media prevalencia	1 (1.3%)	11 (13.9%)	44 (55.7%)	56 (70.9%)
	Alta prevalencia	0 (0.0%)	6 (7.6%)	11 (13.9%)	17 (21.5%)
	Total	7 (8.9%)	17 (21.5%)	55 (69.6%)	79 (100.0%)

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel

Figura 2

*Histograma, D1VI-Prevención de la Ciberseguridad * VD-Gestión TI:*



Acotación: Elaborado por la autora con apoyo de Excel

Para la tabla 7, se pone en manifiesto que se obtiene mayor aceptación en el cruce de “Media Prevalencia” de la dimensión Prevención de nuestra variable Ciberseguridad y “Óptimo” de nuestra variable Gestión de Tecnologías de Información con un total de 44 contestaciones con una representación equivalente al 55.7% del total de encuestados; así mismo el menor índice se sitúa en el cruce de “Media Prevalencia” de la dimensión Prevención de nuestra variable Ciberseguridad y “Nada Óptimo” de nuestra variable Gestión de Tecnologías de Información conformado un total de 1 contestación el cual es equivalente al 1.3%. También tenemos cero contestaciones equivalentes al 0.0% en los niveles “Alta Prevalencia” de la dimensión Prevención de la variable Ciberseguridad y “Nada Óptimo” de la variable Gestión de Tecnologías de Información y para finalizar podemos observar que el rango de mayor acogida es de 55 contestaciones el cual representa el 69.6% el mismo que corresponde al nivel “Óptimo” de nuestra variable Gestión de Tecnologías de Información.

Análisis descriptivo de la dimensión Detección de la variable Ciberseguridad y la variable Gestión de Tecnologías de Información

Tabla 8

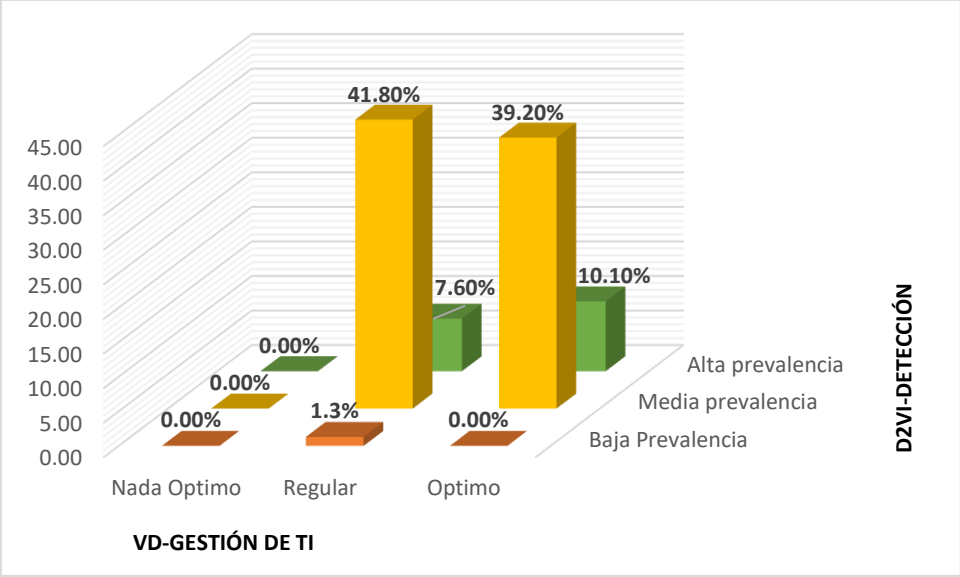
*Tabulación cruzada D2VI-Detección de la Ciberseguridad * VD-Gestión de TI:*

		VD-Gestión de tecnologías de información			
		Nada Óptimo	Regular	Óptimo	Total
D2VI-Detección	Baja Prevalencia	5 (6.3%)	1 (1.3%)	0 (0.0%)	6 (7.6%)
	Media prevalencia	2 (2.5%)	12 (15.2%)	29 (36.7%)	43 (54.4%)
	Alta prevalencia	0 (0.0%)	4 (5.1%)	26 (32.9%)	30 (38.0%)
	Total	7 (8.9%)	17 (21.5%)	55 (69.6%)	79 (100.0%)

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel

Figura 3

*Histograma, D2VI-Detección de la Ciberseguridad * VD-Gestión de TI:*



Acotación: Elaborado por la autora con apoyo de Excel

Con lo que respecta a la tabla 8, se pone en manifiesto que se obtiene mayor aceptación en el cruce de “Media Prevalencia” de la dimensión Detección de nuestra

variable Ciberseguridad y “Óptimo” de nuestra variable Gestión de Tecnologías de Información conformado por un total de 29 contestaciones con una representación equivalente al 36.7% del total de encuestados; así mismo el menor índice se sitúa en el cruce de “Baja Prevalencia” de la dimensión Detección de la variable Ciberseguridad y “Regular” de la variable Gestión de Tecnologías de Información conformado por un total de 1 contestación el cual es equivalente al 1.3%. También tenemos cero contestaciones equivalentes al 0.0% en los niveles “Alta Prevalencia” de la dimensión Detección de la variable Ciberseguridad y “Nada Óptimo” de la variable Gestión de Tecnologías de Información y para finalizar podemos observar que el rango de mayor acogida es de 55 contestaciones el cual representa el 69.6% el mismo que corresponde a un nivel “Óptimo” de nuestra variable Gestión de Tecnologías de Información.

Análisis descriptivo de la dimensión Recuperación de la variable Ciberseguridad y la variable Gestión de Tecnologías de Información

Tabla 9

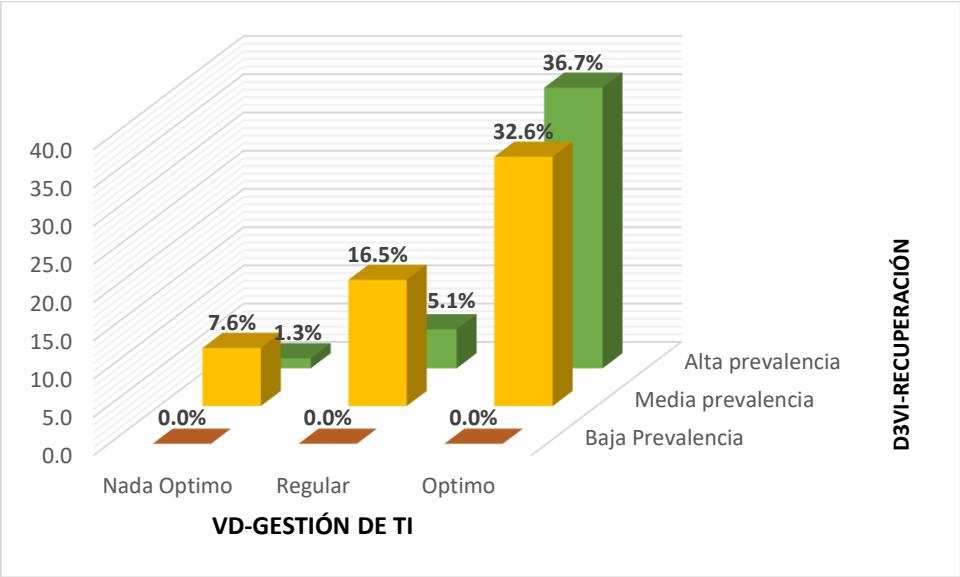
*Tabulación cruzada D3VI-Recuperación de la Ciberseguridad * VD-Gestión TI:*

		VD-Gestión de tecnologías de información			
		Nada Óptimo	Regular	Óptimo	Total
D3VI-Recuperación	Baja Prevalencia	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Media prevalencia	6 (7.6%)	13 (16.5%)	26 (32.6%)	45 (57.0%)
	Alta prevalencia	1 (1.3%)	4 (5.1%)	29 (36.7%)	34 (43.0%)
	Total	7 (8.9%)	17 (21.5%)	55 (69.6%)	79 (100.0%)

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel

Figura 4

*Histograma, D3VI-Recuperación de la Ciberseguridad * VD-Gestión de TI:*



Acotación: Elaborado por la autora con apoyo de Excel.

Ahora para la tabla 9, se pone en manifiesto que se obtiene mayor aceptación en el cruce de “Alta Prevalencia” de la dimensión Recuperación de nuestra variable Ciberseguridad y “Óptimo” de nuestra variable Gestión de Tecnologías de Información conformado por un total de 29 contestaciones con una representación equivalente al 36.7% del total de encuestados; así mismo el menor índice se sitúa en el cruce de “Baja Prevalencia” de la dimensión Recuperación de nuestra variable Ciberseguridad y “Óptimo” de nuestra variable Gestión de Tecnologías de Información conformado por un total de 1 contestación el cual es equivalente al 1.3%. También tenemos cero contestaciones equivalentes al 0.0% en los niveles “Baja Prevalencia” de la dimensión Recuperación de nuestra variable Ciberseguridad y “Nada Óptimo” de nuestra variable Gestión de Tecnologías de Información y para finalizar podemos observar que el rango de mayor acogida es de 55 contestaciones el cual representa el 69.6% el mismo que corresponde al nivel “Óptimo” de nuestra variable Gestión de Tecnologías de Información.

Análisis Inferencial

Para nuestro análisis se usó un análisis estadístico no paramétrico, para Hernández et al. (2018) el análisis inferencial nos permite realizar generalizaciones de la muestra a la población, usada con la finalidad de probar hipótesis y estimar parámetros, basado en el concepto de distribución muestral; en cuanto a las pruebas paramétricas está se usan con variables nominales u ordinales o relaciones no lineales. De acuerdo a las puntuaciones que se obtuvo para la interpretación del coeficiente R^2 la escala que usamos fue la siguiente: 0 a 0.25: relación escasa y/o nula; 0.26 a 0.50: relación débil; 0.51 a 0.75: relación entre moderada y fuerte y de 0.76 a 1.00: relación entre fuerte y perfecta.

Prueba de Hipótesis

A continuación, se formulan las siguientes hipótesis estadísticas:

H_0: La Ciberseguridad no incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

H_1: La Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

Contrastación de la hipótesis estadística general:

Tabla 10

Información de ajuste del modelo:

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	78,142			
Final	12,849	65,293	2	,000

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 10 podemos observar que hemos alcanzado un valor de p= 0.000, siendo este menor al 0.05, a lo que podemos interpretar que existe una incidencia significativa de la variable Ciberseguridad en la variable Gestión de Tecnologías de información.

Tabla 11

Bondad de ajuste:

	Chi-cuadrado	gl	Sig.
Pearson	9,073	2	,011
Desvianza	5,013	2	,082

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 11 de bondad de ajuste podemos visualizar que el Chi-cuadrado de Pearson ha obtenido un valor de 0.011, lo cual es menor a 0.05 por lo que se interpreta en cuanto a los datos que estuvieron en observación no son consecuentes con el modelo ajustado.

Tabla 12

Pseudo R cuadrado:

Coeficiente R^2	Valor
Cox y Snell	,562
Nagelkerke	,706
McFadden	,518

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

Para la tabla 12 observamos que de los 3 coeficientes de R^2 se escoge a Nagelkerke porque este representa un valor más acertado de 0.706 es decir del 70.6% ubicándose en la escala de moderada y fuerte, lo que representa la incidencia significativa de la variable Ciberseguridad en la variable Gestión de Tecnologías de Información.

Tabla 13

Estimación de parámetro:

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-6,331	1,222	26,833	1	,000	-8,726	-3,935
	[VD = 2]	-2,161	,428	25,529	1	,000	-3,000	-1,323
Ubicación	[VI=1]	-27,377	,000	.	1	.	-27,377	-27,377
	[VI=2]	-3,583	,791	20,512	1	,000	-5,133	-2,032
	[VI=3]	0[a]	.	.	0	.	.	.

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

Ahora tenemos la Tabla 13 en la que corroboramos que tenemos un coeficiente de estimación encontrado para la variable Ciberseguridad es -3,583, con un valor significativo p=0.000, con una relación (Wald) superior a 20. En conclusión, la regresión logística ordinal de valor p = 0,000 es menor a la estimación del error 0,05, el mismo que representa una existencia estadística pertinente para dar por descartado la hipótesis nula (H0) considerando la incidencia significativa de la variable Ciberseguridad en la variable Gestión de Tecnologías de Información (H1).

Prueba de Hipótesis específica 1:

H_0: La dimensión prevención de la Ciberseguridad no incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

H_1: La dimensión prevención de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

Tabla 14

Información de ajuste del modelo:

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	48,081			
Final	10,210	37,870	2	,000

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 14 podemos observar que hemos alcanzado un valor de p= 0.000, siendo este menor al 0.05, a lo que podemos interpretar que existe una incidencia significativa de la dimensión prevención de la Ciberseguridad en la variable Gestión de Tecnologías de información.

Tabla 15

Bondad de ajuste:

	Chi-cuadrado	gl	Sig.
Pearson	,642	2	,725
Desvianza	,972	2	,615

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 15 de bondad de ajuste podemos visualizar que el Chi-cuadrado de Pearson ha obtenido un valor de 0.725, siendo este mayor a 0.05 lo que indica que los datos observados son consistentes con el modelo ajustado.

Tabla 16

Pseudo R cuadrado:

Coeficiente R^2	Valor
Cox y Snell	,381
Nagelkerke	,478
McFadden	,301

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 16 se observa que de los 3 coeficientes de R^2 se escoge a Nagelkerke porque este representa un valor más acertado de 0.478 es decir del 47.8%, representando una incidencia significativa débil de la dimensión prevención de la Ciberseguridad en la variable Gestión de Tecnologías de Información.

Tabla 17

Estimación de parámetro:

			Desv.				Intervalo de confianza al 95%	
		Estimación	Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-3,822	1,086	12,392	1	,000	-5,949	-1,694
	[VD = 2]	-,639	,508	1,582	1	,208	-1,636	,357
Ubicación	[D1VI=1]	-24,879	,000	.	1	.	-24,879	-24,879
	[D1VI=2]	,651	,602	1,169	1	,280	-,529	1,832
	[D1VI=3]	0[a]	.	.	0	.	.	.

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 17 corroboramos que tenemos un coeficiente de estimación encontrado corroboramos para la dimensión prevención de la Ciberseguridad es 0.651, con un valor significativo p=0.280, con una relación (Wald) superior a 1,1. En conclusión, la regresión logística ordinal de valor p = 0,280 es superior a la estimación del error 0,05, el cual representa una existencia estadística pertinente para aceptar la hipótesis nula (H0).

Prueba de Hipótesis específica 2:

H_0: La dimensión detección de la Ciberseguridad no incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

H_1: La dimensión detección de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

Tabla 18

Información de ajuste del:

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	42,782			
Final	12,570	30,213	2	,000

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 18 podemos observar que hemos alcanzado un valor de p= 0.000, siendo este menor al 0.05, a lo que podemos interpretar que existe una incidencia

significativa de la dimensión detección de la Ciberseguridad en la variable Gestión de Tecnologías de información.

Tabla 19

Bondad de ajuste:

	Chi-cuadrado	gl	Sig.
Pearson	,637	2	,727
Desvianza	1,065	2	,587

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 19 de bondad de ajuste podemos visualizar observar que el Chi-cuadrado de Pearson ha obtenido un valor de 0.727, por lo que vemos que este es mayor a 0.05 lo que indica que los datos analizados son consistentes con el modelo ajustado.

Tabla 20

Pseudo R cuadrado:

Coeficiente R^2	Valor
Cox y Snell	,318
Nagelkerke	,399
McFadden	,240

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 20 se observa que de los 3 coeficientes de R^2 se escoge a Nagelkerke porque este representa un valor más acertado de 0.399 es decir del 39.9%, representando una incidencia significativa débil de la dimensión detección de la Ciberseguridad en la variable Gestión de Tecnologías de Información.

Tabla 21

Estimación de parámetro:

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-4,444	,871	26,053	1	,000	-6,150	-2,737
	[VD = 2]	-1,885	,539	12,216	1	,000	-2,942	-,828
Ubicación	[D2VI=1]	-6,071	1,397	18,876	1	,000	-8,810	-3,332
	[D2VI=2]	-1,172	,629	3,478	1	,062	-2,405	,060
	[D2VI=3]	0[a]	.	.	0	.	.	.

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 21 corroboramos que tenemos un coeficiente de estimación encontrado corroboramos para la dimensión detección de la Ciberseguridad es -1,172, con un valor significativo p=0.062, con una relación (Wald) superior a 3,4. En conclusión, la regresión logística ordinal de valor p = 0,062 es superior a la estimación del error 0,05, el cual representa una existencia estadística pertinente para aceptar la hipótesis nula (H0).

Prueba de Hipótesis específica 3:

H_0: La dimensión recuperación de la Ciberseguridad no incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.
H_1: La dimensión recuperación de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

Tabla 22

Información de ajuste del modelo:

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	20,241			
Final	12,669	7,572	1	,006

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 22 podemos observar que se alcanzó un valor de p= 0.006, siendo este inferior al 0.05, a lo que podemos interpretar que existe incidencia significativa de la dimensión recuperación de la Ciberseguridad en la variable Gestión de Tecnologías de información.

Tabla 23

Bondad de ajuste:

	Chi-cuadrado	gl	Sig.
Pearson	,033	1	,855
Desvianza	,034	1	,854

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 23 de bondad de ajuste podemos visualizar observar que el Chi-cuadrado de Pearson ha obtenido el valor de 0.855, siendo mayor a 0.05 lo que se interpreta que los datos analizados son coherentes con el modelo ajustado.

Tabla 24

Pseudo R cuadrado:

Coeficiente R^2	Valor
Cox y Snell	,091
Nagelkerke	,115
McFadden	,060

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la tabla 24 podemos observar que de los 3 coeficientes de R^2 se escoge a Nagelkerke porque este representa un valor más acertado de 0.115 es decir del 11.5%, representando una incidencia significativa débil de la dimensión recuperación de la Ciberseguridad en la variable Gestión de Tecnologías de Información.

Tabla 25

Estimación de parámetro:

			Desv.				Intervalo de confianza al 95%	
		Estimación	Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-3,353	,600	31,286	1	,000	-4,528	-2,178
	[VD = 2]	-1,763	,484	13,256	1	,000	-2,712	-,814
Ubicación	[D3VI=2]	-1,455	,568	6,567	1	,010	-2,569	-,342
	[D3VI=3]	0[a]	.	.	0	.	.	.

Acotación: Elaborado por la autora con apoyo de SPSS Statistics y Excel.

En la Tabla 25 validamos el coeficiente de estimación que hemos encontrado para la dimensión recuperación de la Ciberseguridad el mismo que tiene el valor de -1,455, con un valor significativo p=0.010, con una relación (Wald) superior a 6,5. En conclusión, la regresión logística ordinal de valor p = 0,010 es inferior a la estimación del error 0,05, el cual representa una existencia estadística pertinente para aceptar la hipótesis alterna (H_1).

V. DISCUSIÓN

Con lo que respecta al objetivo general los resultados que se han obtenido en el análisis descriptivo se demuestra que el indicador que cuenta con una alta aceptación está ubicado en el cruce de “Alta Prevalencia” de nuestra variable Ciberseguridad y “Óptimo” de nuestra variable Gestión de Tecnologías de Información con un total de 53 contestaciones con una representación equivalente al 67.1% del total de encuestados; así mismo el menor índice de aceptación se sitúa en el cruce de “Alta Prevalencia” de nuestra variable Ciberseguridad y “Nada Óptimo” de nuestra variable Gestión de Tecnologías de Información con un total de 1 contestación el cual es equivalente al 1.3%.

Ahora con lo que respecta al análisis inferencial se ha obtenido como resultado que el R^2 de Nagelkerke es de 0.706 es decir del 70.6%, este resultado indica que la variable Ciberseguridad posee un nivel considerable de incidencia en la variable Gestión de Tecnologías de Información. Del mismo modo alcanzó un valor de significancia de p= 0.000, siendo este inferior al 0.05, de tal modo que podemos determinar que si existe una incidencia de la variable Ciberseguridad en la variable Gestión de Tecnologías de información.

Según el resultado obtenido este guarda concordancia con los que obtuvo Bohórquez (2021) quien determinó la relación de la Ciberseguridad y la Gestión de Tecnologías de Información (TI) en una empresa privada, en su análisis inferencial ha logrado demostrar una correlación existente, teniendo que el coeficiente Rho de Spearman ha resultado con una equivalencia de 0.832 demostrando una correlación muy fuerte ya que se encuentra en el rango de 0.81 a 1.00. En cuanto a su significancia este fue igual a 0.00 y es inferior a 0.05 obteniendo que la relación entre las variables es estadísticamente significativa. Además concuerda con Baquero (2018) que en su investigación analizó el uso de las tecnologías de información y comunicación (TIC) como soporte a la Gestión de empresas, el mismo que tuvo como objetivo analizar cómo la Gestión de la TIC puede apoyar a las

organizaciones o empresas que están dedicadas a ofrecer servicios digitales, la metodología aplicada en este estudio fue cualitativa, la misma que concluye que esta empresa Ecuatoriana se orienta en temas de operaciones y en la resolución de conflictos diarios, debido a que no ha establecido de manera clara su visión, objetivos y estrategias, por lo que no cuenta con un parámetro que le permita Gestionar su TIC de manera correcta. Así mismo concuerda con Santos (2019) que en su pesquisa investigativa tuvo como objetivo comprender la influencia e importancia del factor humano en la ciberseguridad de las organizaciones, a través del cual se identificaron comportamientos humanos, características que influyen y su impacto en los niveles de ciberseguridad alcanzados y las soluciones que permitan corregir estas situaciones, la metodología que se empleó fue la cualitativa de tipo no experimental, esta investigación concluye que el factor humano tiene una gran influencia en la ciberseguridad de las organizaciones y por lo tanto la solución que permite un cambio duradero es la creación de una sólida cultura de ciberseguridad a través de la sensibilización, educación y formación de los empleados.

Con relación al concepto de variable independiente Ciberseguridad Leiva (2015) la define como procedimientos de uso, procesos y las nuevas tecnologías que van a permitir la prevención, detección y recuperación de aquellos daños que se puedan provocar a la confidencialidad, integridad y disponibilidad de la información en el espacio cibernético. Para la variable dependiente Mendoza et al. (2014) la definen como la unión de tres niveles que son la dirección estratégica, transferencia e innovación tecnológica que van a permitir poder gestionar y direccionar los recursos humanos y económicos con la finalidad de poner en aumento nuevos conocimientos y por último De la Cruz (2021) definen a la Gestión de TI como la estructura de comunicaciones y procedimientos para orientar e inspeccionar a la empresa camino a cumplir sus objetivos agregando valor y tiempo, logrando así el equilibrio entre riesgo y retorno de TI y sus procedimientos.

Ahora bien para el objetivo específico número 1 se ha obtenido que el análisis descriptivo demuestra que el indicador que cuenta con una alta aceptación está

ubicado en el cruce de “Media Prevalencia” de la dimensión Prevención de variable Ciberseguridad y “Óptimo” de la variable Gestión de Tecnologías de Información con un total de 44 contestaciones con una representación equivalente al 55.7% del total de encuestados; así mismo el menor índice se sitúa en el cruce de “Media Prevalencia” de la dimensión Prevención de la variable Ciberseguridad y “Nada Óptimo” de la variable Gestión de Tecnologías de Información con un total de 1 contestación el cual es equivalente al 1.3%.

Así mismo con lo que respecta al análisis inferencial como resultado se ha obtenido que el R^2 de Nagelkerke es 0.478 el cual equivale al 47.8%, representando una incidencia significativa débil de la dimensión prevención de la Ciberseguridad en la variable Gestión de Tecnologías de Información; por otro lado se alcanzó un valor de significancia de p= 0.000, siendo este inferior al 0.05, de tal modo que podemos interpretar que si existe una incidencia significativa de la dimensión prevención de la Ciberseguridad en la variable Gestión de Tecnologías de información.

Estos resultados guardan concordancia con los obtenidos por Bohórquez (2021) que obtuvo como resultado que la dimensión prevención de la ciberseguridad se relaciona de manera significativa con la gestión de tecnologías de información en un nivel moderado.

Con lo que respecta a la dimensión de prevención, Romero et. Al (2018) logra definirla como la secuencia de revisiones realizadas de manera periódica, estos pueden ser de múltiples formas como el hardware, software o de cualquier componente que involucren a los sistemas y procesos, por tal motivo es que las diferentes revisiones dependen de los procedimientos de la empresa y cada una tiene sus propios procesos. Por otro lado, Defaz et al. (2006) nos dice que la prevención es aquella que se encarga de preparar los equipos que puedan recibir posibles ataques, así mismo es aquella encargada de mantener buenas políticas de seguridad y de este modo reaccionar al momento y evitar un posible ataque.

Ahora para el objetivo específico número 2 se ha obtenido que en el análisis descriptivo se demuestra que el indicador que cuenta con una alta aceptación está ubicado en el cruce de “Media Prevalencia” de la dimensión Detección de la variable Ciberseguridad y “Óptimo” de la variable Gestión de Tecnologías de Información con un total de 29 contestaciones con una representación equivalente al 36.7% del total de encuestados; así mismo el menor índice se sitúa en la intersección de “Baja Prevalencia” de la dimensión Detección de la variable Ciberseguridad y “Regular” de la variable Gestión de Tecnologías de Información con un total de 1 contestación el cual es equivalente al 1.3%.

Así mismo con lo que respecta al análisis inferencial se ha obtenido que el R^2 de Nagelkerke es 0.399 es decir del 39.9%, representando una incidencia significativa débil de la dimensión detección de la Ciberseguridad en la variable Gestión de Tecnologías de Información, tenemos también que se alcanzó un valor de significancia de p= 0.000, siendo este inferior al 0.05, de tal modo que podemos interpretar que si existe una incidencia significativa de la dimensión detección de la Ciberseguridad en la variable Gestión de Tecnologías de información

Estos resultados que se mencionan concuerdan con los obtenidos por Serna (2018) quien obtuvo como conclusión que el nivel de riesgo de una empresa equivale a un componente evidente necesario en la gestión de incidentes y la protección de infraestructuras, ya que va permitir establecer la definición de todas las habilidades en términos políticos, lineamientos del negocio, la parte tecnológica entre otros componentes que permitan enfrentar el peligro de las amenazas, concluye también que el modelo ha permitido realizar la identificación de aspectos importantes, el mismo que evidencia la obligación de fortalecer el tiempo tanto de la detección, contención y erradicación de incidentes.

Para la definición de la dimensión detección Defaz et al. (2006) nos dicen que es aquella encargada de identificar aquellos ataques realizados en el momento y así poder combatirlos debidamente, una de las principales funciones de la seguridad es identificar y eliminar las vulnerabilidades y los ataques; así mismo Kumar et al (2021) nos dicen que la detección es aquella que permite reconocer, catalogar y

calificar las vulnerabilidades tanto en las computadoras, la infraestructura de la red, el software y hardware.

Y finalmente para el objetivo específico número 3 tenemos como resultado que en el análisis descriptivo se demuestra que el indicador que cuenta con una alta aceptación está ubicado en el cruce de “Alta Prevalencia” de la dimensión Recuperación de la variable Ciberseguridad y “Óptimo” de la variable Gestión de Tecnologías de Información con un total de 29 contestaciones con una representación equivalente al 36.7% del total de encuestados; así mismo el menor índice se sitúa en la intersección de “Baja Prevalencia” de la dimensión Recuperación de la variable Ciberseguridad y “Óptimo” de la variable Gestión de Tecnologías de Información con un total de 1 contestación el cual es equivalente al 1.3%.

Así mismo con lo que respecta al análisis inferencial se ha obtenido que el R^2 de Nagelkerke es de 0.115 es decir del 11.5%, representando una incidencia significativa débil de la dimensión recuperación de la Ciberseguridad en la variable Gestión de Tecnologías de Información; también tenemos que se alcanzó un valor de significancia de p= 0.006, siendo este inferior al 0.05, de tal modo que podemos interpretar que si existe una incidencia significativa de la dimensión recuperación de la Ciberseguridad en la variable Gestión de Tecnologías de información. Así mismo Allauca (2022) propone mejorar las prácticas de Ciberseguridad a clientes de diversas corporaciones, concluye que se logró identificar los problemas principales de Ciberseguridad que los clientes presentan, problemas que están relacionado con la infraestructura del proveedor de servicio de internet y con la ayuda de la norma ISO 27032, se obtiene las mejores prácticas de ciberseguridad, posteriormente se les brindó recomendaciones de seguridad y recuperación que deben ser aplicados en su equipos de red interna.

Con respecto a la dimensión recuperación Defaz et al. (2006) mencionaron que la recuperación es la parte más importante porque el ataque es inevitable, todo el equipo debe restaurar al original, eliminar el ataque para continuar normalmente.;

de tal modo para Staves et al. (2022) la recuperación es definida como la unión de diferentes técnicas y procedimientos empleados para extraer y acceder a información que se encuentre en un almacenamiento digital, que por diversos motivos estos se encuentren dañados o averiados y que no son accesibles de manera normal.

La metodología usada para esta investigación me ha dado la posibilidad de recolectar información en una empresa de Seguros y su Gestión de Tecnologías de Información, así mismo hemos determinado el grado de incidencia de la variable Ciberseguridad en la variable Gestión de Tecnologías de Información apoyándonos del software SPSS para la realización de nuestro análisis estadístico, así mismo hemos podido mostrar los beneficios de los estudios básicos, los mismos que dejan valiosos aportes para futuras investigaciones de tal modo que está investigación pueda ser tomada como referencia; también en esta investigación hemos podido tomar como evidencia una de sus debilidades, ya que al recolectar los datos mediante el cuestionario estamos expuestos a diversos estados de ánimos de los encuestados por lo que algunas respuestas dependiendo del ánimo de las personas estos podrían variar, pero sabemos que esto es parte del método científico realizado.

VI. CONCLUSIONES

Primera La variable Ciberseguridad presenta incidencia en la variable Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022, como resultado se ha obtenido un valor de R^2 de Nagelkerke de 70.6%, dicho resultado señala la existencia de un nivel considerable de incidencias entre ambas variables.

Segunda La dimensión prevención de la Ciberseguridad presenta una incidencia significativa débil sobre la variable Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022, como resultado se ha obtenido un valor de R^2 de Nagelkerke de 47.8%, lo que representa esa incidencia significativa débil de la dimensión uno de la variable independiente hacía la dependiente.

Tercera La dimensión detección de la Ciberseguridad presenta una incidencia significativa débil sobre la variable Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022, como resultado se ha obtenido un valor de R^2 de Nagelkerke es de 39.9%, lo que representa una incidencia significativa débil de la dimensión dos de la variable independiente hacía la dependiente.

Cuarta La dimensión recuperación de la Ciberseguridad presenta una incidencia significativa débil sobre la variable Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022, como resultado se ha obtenido un valor de R^2 de Nagelkerke es de 11.5%, representando una incidencia significativa débil de la tercera dimensión de la variable independiente hacía la dependiente.

VII. RECOMENDACIONES

Primera Para mejorar del nivel considerable a un nivel fuerte la incidencia de la variable Ciberseguridad en la variable Gestión de Tecnologías de Información en una empresa de Seguros, se recomienda a la Gerencia de Infraestructura y soporte TI retomar su programa de capacitaciones que se realizaba de manera trimestral en beneficio del personal que pertenece a esa gerencia (Soporte, seguridad de la información, infraestructura, etc.) y que posteriormente puedan aplicar los conocimientos adquiridos en los diversos procesos en los que están inmersos.

Segunda Con el propósito de poder mejorar e incrementar el nivel débil de la incidencia de la dimensión prevención de la Ciberseguridad en la variable Gestión de Tecnologías de Información en una empresa de Seguros, se recomienda a la Gerencia de Infraestructura y soporte TI y a la Gerencia de Administración realizar programas de capacitación constantes en beneficio del personal que pertenece al área de TI, así como de las áreas administrativas con la finalidad de inculcarles la importancia de la prevención en cuanto a ciberseguridad se refiere.

Tercera Con el propósito de poder mejorar e incrementar el nivel débil de la incidencia de la dimensión detección de la Ciberseguridad en la variable Gestión de Tecnologías de Información en una empresa de Seguros, se recomienda a la Gerencia de Infraestructura y soporte TI y a la Gerencia de Administración realizar programas de capacitación constantes en beneficio del personal que pertenece al área de TI, así como de las áreas administrativas con la finalidad de inculcarles la importancia de la detección en cuanto a ciberseguridad se refiere (fraudes, delitos informáticos, phishing, etc.).

Cuarta Con el propósito de poder mejorar e incrementar el nivel débil de la incidencia de la dimensión recuperación de la Ciberseguridad en la

variable Gestión de Tecnologías de Información en una empresa de Seguros, se recomienda a la Gerencia de Infraestructura y soporte TI y a la Gerencia de Administración realizar programas de capacitación constantes en beneficio del personal que pertenece al área de TI, así como de las áreas administrativas con la finalidad de inculcarles la importancia del proceso de recuperación en cuanto a ciberseguridad se refiere (recuperación de información, cuentas hackeadas, etc.).

REFERENCIAS

Allauca Carrillo., E.F. (2022). Propuesta de Mejores Prácticas de Ciberseguridad para la Comunicación en Redes de Clientes Corporativos. Pontificia Universidad Católica del Ecuador.https://repositorio.pucesa.edu.ec/bitstream/123456789/3779/1/78213.pdf

Amponsah Odei, S., & Karikari Appiah, M. (2022). Unravelling the Drivers of Technological Innovations in the Czech Republic: Do International Technological Linkages Matter? International Journal of Innovation Studies, Volume 7, Issue 1, Pages 32-46. https://doi.org/10.1016/j.ijis.2022.09.002

Arano Chávez, R. M., Espinosa Mejía, F. y Arroyo Grant G. (2011). El rol de la dirección estratégica en las empresas. Ciencia Administrativa 2011-1, 29-31 https://www.uv.mx/iiesca/files/2012/11/005direccion2011-1.pdf

Armijos Robles, L., Campos Carrillo, A., & Hidalgo-Luzuriaga, Y. (2020). Estudio del Direccionamiento Estratégico en el Desarrollo Organizacional en Latinoamérica: Una Revisión de Literatura (2009-2018). Economía Y Negocios, 11(1), 104-117. https://doi.org/10.29019/eyn.v11i1.695

Baquero Vallejos, C. E. (2018). Análisis sobre el uso de las tecnologías de información y comunicación como soporte de la gestión de empresas dedicadas a la oferta de servicios de marketing digital, Caso: Addconsulta del Ecuador S.A.https://repositorio.uasb.edu.ec/bitstream/10644/6000/1/T2493-MAE-Baquero-Analisis.pdf

Bohórquez Salcedo, A. I. (2021). Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020.https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/63128/Bohorquez_SAI-SD.pdf?sequence=1&isAllowed=y

Bozeman, B. (2000). Technology transfer and public policy: a review of research and theory. Research Policy, Volume 29, Issues 4–5, Pages 627-655. https://doi.org/10.1016/S0048-7333(99)00093-1

Burbano Pérez, A. B. (2017). Importancia de la dirección estratégica para el desarrollo empresarial. Revista científica Dominio de las ciencias, Vol. 3,19-28. https://dialnet.unirioja.es/descarga/articulo/6093283.pdf

Cando Segovia, M. R. y Medina Chicaiza, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10(1), 17-41. https://doi.org/10.17993/3ctic.2021.101.17-41

Check Point (2022). Midyear trends report. https://pages.checkpoint.com/cyber-security-report-2022-spanish.html?utm_source=eblast&utm_medium=email&utm_campaign=fm_eb_22q1_latam_es_security_report

Cienfuegos Velasco, M. A., Cienfuegos Velasco, A. (2016). Lo cuantitativo y cualitativo en la investigación. Un apoyo a su enseñanza. Revista Iberoamericana para la Investigación y el Desarrollo Educativo, Vol. 7, Núm. 13, 1-22. https://www.scielo.org.mx/pdf/ride/v7n13/2007-7467-ride-7-13-00015.pdf

Conti Montero, G. P. y Briseño Diaz, F. A. (2015). Transferencia tecnológica. Aspectos a seguir para controlar el activo tecnológico en empresas del sector petrolero. Prospect, Vol 13, N° 2, 110-117.https://doi.org/10.15665/rp.v13i2.493

De la Cruz Vêlez de Villa, P. E. (2021). Intellectual Capital, Knowledge Management in the Interaction of Government and Management of Information Technologies from COBIT 5 Perspective. Journal of Applied Business & Economics, 23(1), 258–276. https://doi.org/10.33423/jabe.v23i1.4068

Decreto de Urgencia Nº 007-2020.Decreto de Urgencia que Aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento.09 de enero del 2020.Diario Oficial el Peruano.https://cdn.www.gob.pe/uploads/document/file/2790485/Decreto%20de%20Urgencia%20N%C2%BA%20007-2020.pdf?v=1643322610

Defaz Toapanta, X. E., Yanchapaxi Barragán, R. O. (2006). Análisis de la aplicación metodológica para el estudio de riesgos y vulnerabilidades en la Universidad de Pinar del Río: Propuesta de Perfeccionamiento. Universidad de Pinar del Río. Cuba. 96 p. http://repositorio.utc.edu.ec/handle/27000/536

Diario el comercio (2022). Ransomware:75% de las empresas víctima de un ciberataque 2021.https://elcomercio.pe/tecnologia/empresas/ransomware-75-de-las-empresas-victima-de-un-ciberataque-2021-ciberseguridad-ciberdelincuentes-noticia/?ref=ecr

Espinoza Sotomayor, R. (2009). El fayolismo y la organización contemporánea. Visión Gerencial, (1),53-62. ISSN: 1317-8822.https://www.redalyc.org/articulo.oa?id=465545880010

Flores Ccanto, F., Ramos Vera, P. P., Ramos Vera, F., & Ramos Vera, A. M. (2019). Gestión de innovación tecnológica y globalización como factores impulsadores de la calidad de servicio y competitividad. Revista Venezolana De Gerencia, 24(88). https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083571700&partnerID=40&md5=0659636ff58565f3abf1d2a166ec16be

Fuck, M. P., Morales Vilha, A. (2011). Inovação Tecnológica: da definição à ação. Revista de Artes e Humanidades contemporâneos, 1-21. https://revistacontemporaneos.com.br/n9/dossie/inovacao-tecnologica.pdf

Fuenmayor Sandrea, A. Dadul Barrios, Y. & Gutiérrez, J. (2017). Gestión tecnológica de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia. Revista de la Universidad del Zulia 3a época Ciencias del Agro, Ingeniería y Tecnología.08(20),83 - 96. https://produccioncientificaluz.org/index.php/rluz/article/view/30878/31913

Hernández Sampieri, R. & Mendoza Torres, C. P. (2018). Metodología de la Investigación: Las Rutas Cuantitativa, Cualitativa y Mixta.McGraw-HILL Interamericana Editores, S.A. de C. V.

Huaman Baltazar, J. L. (2021). Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática Del Ejército, Lima,

2020
http://repositorio.esge.edu.pe/bitstream/handle/ESGEEPG/692/TESIS%20DE%20GRADO%20MY%20HUAM%C3%81N%20B.%20.pdf?sequence=1&isAllowed=y

Huerta Riveros, P. C., Gaete Feres, H. G., & Pedraja Rejas, L. M. (2020). Dirección estratégica, sistema de información y calidad. El caso de una universidad estatal chilena. Información tecnológica, 31(2), 253-266. https://dx.doi.org/10.4067/S0718-07642020000200253

Hurel, L. M. (2021). Cibersegurança no Brasil: uma Análise da Estratégia Nacional. Revista Instituto Igarapé, ISSN 2359-0998, 1-45. https://www.researchgate.net/publication/351098187

Instituto Nacional de Estadística e Informática (2020). Perú: Tecnologías de Información y Comunicación en las Empresas, 2017. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1719/libro.pdf

Kolosok, I., Gurina, L. (2022). Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems, IFAC-PapersOnLine, Volume 55, 485-490.https://doi.org/10.1016/j.ifacol.2022.07.084"

Kumar, P., Gupta, G., Tripathi, R. (2021). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Computer Communications, Volume 166,110-124.https://doi.org/10.1016/j.comcom.2020.12.003.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local Revista Latinoamericana de Ingeniería de Software, 3(4),161-176. https://doi.org/10.18294/relais.2015.161-176

Ley N° 31250 de 2021.Ley del Sistema Nacional de Ciencia, Tecnología e Innovación (Sinacti). 2 de Julio de 2021.Diario Oficial El Peruano Nº 1968664-

1. https://busquedas.elperuano.pe/download/full/3b3WpD0VKIw902-VvFdP1O

Liu, X., Chang, P., Wu, Z., Jiang, M., Sun, Q. (2022). Malicious data injection attacks risk mitigation strategy of cyber–physical power system based on hybrid measurements attack detection and risk propagation. International Journal of Electrical Power & Energy Systems, Volume 142, Part A, 108241. https://doi.org/10.1016/j.ijepes.2022.108241.

Macharia Chege, S., Wang, D., Leparan Suntu, S., Kyetuza Bishoge, O. (2019). Influence of technology transfer on performance and sustainability of standard gauge railway in developing countries. Technology in Society, Volume 56, 79-92. https://doi.org/10.1016/j.techsoc.2018.09.007

Marques de Araújo, A. C. (2016). Uma Revisão Sobre os Princípios da Teoria Geral Dos Sistemas. Revista Estação Científica, num 16, 1-14. https://portal.estacio.br/media/3727396/uma-revis%C3%A3o-sobre-os-princ%C3%ADpios-da-teoria-geral-dos-sistemas.pdf

Martínez Romero, E. y Esparza Olguín, L. G. (2021). Teorías de Sistemas Complejos: marco epistémico para abordar la complejidad socioambiental. Intersticios sociales, (21), 373-398. Epub 30 de agosto de 2021. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-49642021000100373&lng=es&tlng=es.

Matos, E., & Pires, D. (2006). Teorias administrativas e organização do trabalho: de Taylor aos dias atuais, influências no setor saúde e na enfermagem. Texto Contexto Enferm, Florianópolis,15(3),508-514 https://doi.org/10.1590/S0104-07072006000300017

Mccormick, K., Sanders, J. H. (2022). Chapter 11 - Technology transfer. Quality (Second Edition), Butterworth-Heinemann, Pages 243-261. https://doi.org/10.1016/B978-0-323-90815-3.00005-0.

Mendoza León, J. G. y Valenzuela Valenzuela, A. (2014). Aprendizaje, innovación y gestión tecnológica en la pequeña empresa-Un estudio de las industrias

metalmecánica y de tecnologías de información en Sonora. Contaduría y Administración 59 (4),253-284.https://www.scielo.org.mx/pdf/cya/v59n4/v59n4a11.pdf

Mendoza Silva, L. y Vega Gallegos, G. (2019). Evaluación de la Capacidad de Detección y Respuesta a Riesgos de Ciberseguridad, Caso de la Empresa SISC. https://repositorio.up.edu.pe/bitstream/handle/11354/2250/Luis_Tesis_Maestria_2019.pdf?sequence=1&isAllowed=y

Ministerio de la Producción (Produce) (2022). Produce ayuda a empresas a protegerse de ciberataques. https://www.gob.pe/institucion/produce/noticias/598609-produce-ayuda-a-empresas-a-protegerse-de-ciberataques

Miró Llinares, F. (2011). La Oportunidad Criminal en el Ciberespacio- Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología,13(07), 1-55. http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Moquillaza Mayuri, R. N. (2020). Gestión de la Tecnología de la Información y Comunicación (Tic) y la Calidad de Servicio de La Oficina General de Matricula, Registro y Estadística de la Universidad Nacional San Luis Gonzaga, Años 2018 - 2019.https://bit.ly/3RBU5Pr

Moreno, J., Sánchez, C. M. S., Salavarrieta, J., & Vargas, L. (2019). Soluciones Tecnológicas para la Prevención de Fraude y diseño de un Modelo de Prevención del Riesgo Transaccional para el Botón de Pago. Entre Ciencia E Ingeniería, 13(26), 36-42. https://doi.org/10.31908/19098367.1154

Naseer, A., Naseer, H., Ahmad, A., Sean, B. M., Adil Masood, S. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. International Journal of Information Management, Volume 59, 102334, ISSN 0268-4012. https://doi.org/10.1016/j.ijinfomgt.2021.102334.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

Oliveira da Silva Araújo, R. C., & Alves de Souza Filho, T. (2018). Da teoria clássica à administração moderna: os 14 princípios gerais de Fayol comparados à administração pública brasileira. Revista Reflexões Econômicas, Ilhéus (BA). n.3. v.1.,78-91. https://periodicos.uesc.br/index.php/reflexoeseconomicas/article/view/1324/1493

Patel, M., & Patel, N. (2019). Exploring Research Methodology: Review Article. International Journal of Research & Review, 6(3),48-55. https://www.ijrrjournal.com/IJRR_Vol.6_Issue.3_March2019/IJRR0011.pdf

Peralta Miranda, P., Cervantes Atia, V., Salgado Herrera, R., & Espinoza Pérez, A. (2020). Dirección estratégica para la innovación en pequeñas y medianas empresas de la ciudad de Barranquilla –Colombia. Revista Venezolana De Gerencia, 25(89), 229-243. https://doi.org/10.37960/revista.v25i89.31380

Pereira da Silva, A., Dos Santos, J. C., & Konrad, M. R. (2016). Teoria Geral Dos Sistemas: Diferencial Organizacional que viabiliza o Pleno Entendimento da Empresa. Revista da Faculdade Eça de Queirós, 6(22), 1-12. http://uniesp.edu.br/sites/_biblioteca/revistas/20170509162834.pdf

Ramírez Molina, R. I., Royero Orozco, G.A., Janbeih, Omar Nabih El Kadi (2019). Gestión tecnológica como factor clave de éxito en universidades privadas. Telos, 21 (1),10-32. https://www.redalyc.org/articulo.oa?id=99357718023

Rauscher, K.F. y Yashenko, V. (2011). The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2. EastWest Institute and the Information Security Institute of Moscow State University. https://www.files.ethz.ch/isn/178418/terminology2.pdf

Rodríguez Cano, F. (2018). Gestión Tecnológica, un Recurso para Lograr la Auto-Sustentabilidad Económica y Competitividad en un Parque Biotecnológico.http://ring.uaq.mx/bitstream/123456789/1236/1/RI007864.pdf

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D.S., Álava Cruzatty, J.E., Parrales Anzúles, G. B., Álava Mero, C.J., Murillo Quimiz, A.L. y Castillo Merino, M. A. (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L., 1-121.http://dx.doi.org/10.17993/IngyTec.2018.46

Santos Gonçalves, R. (2019). O Fator Humano da Cibersegurança nas Organizações.https://www.repository.utl.pt/bitstream/10400.5/19248/1/DM-RSG-2019.pdf

Scherer, F. M. (2001). Innovation and Technological Change, Economics.International Encyclopedia of the Social & Behavioral Sciences, Pergamon, Pages 7530-7536. https://doi.org/10.1016/B0-08-043076-7/02308-1

Schuelter, G., Bosco da Mota Alves, J., Milano Falcão Vieira, E., & Medina Kern, V. (2005). A Teoria Geral de Sistemas, Gestão do Conhecimento e Educação a Distância: Revisão e integração dos temas dentro das organizações. Revista de Ciências da Administração, 7(14),1-13. ISSN: 1516-3865. https://www.redalyc.org/articulo.oa?id=273520153003

Senior, A., Narváez, M. & Fernández, G. (2006). Una aproximación a la gestión de ciencia y tecnologíaen las PYME's. Multiciencias, 6(2),194-201. https://www.redalyc.org/articulo.oa?id=90460214

Serna Patiño, A. M. (2018). Análisis de la Capacidad de Ciberseguridad para la Dimensión Tecnológica en Colombia: Una Mirada Sistémica Desde la Organización.https://repository.upb.edu.co/bitstream/handle/20.500.11912/4152/AN%c3%81LISIS%20DE%20LA%20CAPACIDAD%20DE%20CIBERSEGURIDAD%20PARA.pdf?sequence=1&isAllowed=y

Sonmezturk Bolatan, G. I., Giadedi, A., & Daim, T. (2022). Innovation leadership through technology transfer: Case of Turkish industry. Technology in Society, Volume 68,101909. https://doi.org/10.1016/j.techsoc.2022.101909

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., Hutchison, D. (2022). A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. International Journal of Critical Infrastructure Protection, Volume 37,100505. https://doi.org/10.1016/j.ijcip.2021.100505.

Superintendencia de Banca, Seguros y AFP (2021). Seguridad de la información y ciberseguridad: nuevo reglamento para promover un entorno seguro y confiable en beneficio de los usuarios de los sistemas supervisados. https://bit.ly/3CDVhxI

Unión Internacional de Telecomunicaciones (2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad, Recomendación UIT-T X.1205.Sector de Normalización de las Telecomunicaciones de la UIT. https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-S&type=items

Velásquez Vásquez, F. (2002). Escuelas e Interpretaciones del Pensamiento Administrativo. Universidad ICESI, 31-55. http://www.scielo.org.co/pdf/eg/v18n83/v18n83a02.pdf

Villasís Keever, M. A., Arias Gómez, J., & Miranda Novales, M. G. (2016). El protocolo de investigación III: la población de estudio. Revista Alergia México, 63 (2),201-206. https://www.redalyc.org/articulo.oa?id=486755023011

Wang, W., Harrou, F., Bouyeddou, B., Senouci, S., Sun, Y. (2022). Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. International Journal of Critical Infrastructure Protection, Volume 38,100542. https://doi.org/10.1016/j.ijcip.2022.100542

Yu Cheng H. & Shun Hsing, Ch. (2011). An Empirical Study of Technological Innovation, Organizational Structure and New Product Development of the

High-tech Industry. Information Technology Journal, 10 : 1484-1497. https://scialert.net/abstract/?doi=itj.2011.1484.1497

ANEXOS

Anexo 1 : Matriz de Consistencia

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES

Problema principal:

¿De qué manera la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?

Problemas específicos:

PE1: ¿De qué manera la dimensión prevención de la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?

PE2: ¿De qué manera la dimensión detección de la Ciberseguridad incide en la Gestión de

Objetivo principal:

Determinar la incidencia de la Ciberseguridad en la Gestión de tecnologías de Información en una empresa de Seguros, Lima 2022.

Objetivos específicos:

OE1: Determinar la incidencia de la dimensión prevención de la Ciberseguridad en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

OE2: Determinar la incidencia de la dimensión detección de la Ciberseguridad en la

Hipótesis principal:

La Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

Hipótesis específicas:

HE1: La dimensión prevención de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.

HE2: La dimensión detección de la Ciberseguridad incide significativamente en la

Variable - 1: Ciberseguridad

Dimensiones	Indicadores	Ítems	Niveles
Prevención	Control	1-2	
	Conocimiento	3-4	
	Confiabilidad	5-6	
Detección	Control	7-8	
	Monitoreo	9-10	
	Conocimiento	11-12	
Recuperación	Proceso	13-14	
	Documentación	15-16	
	Difusión	17-18	

Variable - 2: Gestión de Tecnología de Información

Dimensiones	Indicadores	Ítems	Niveles
Dirección Estratégica	Participación	19-20	
	Uso	21-22	

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
Tecnologías de Información en una empresa de Seguros, Lima 2022? PE3: ¿De qué manera la dimensión recuperación de la Ciberseguridad incide en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022?	Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022. OE3: Determinar la incidencia de la dimensión recuperación de la Ciberseguridad en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.	Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022. HE3: La dimensión recuperación de la Ciberseguridad incide significativamente en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022.		Confiabilidad	23-24	
			Transferencia Tecnológica	Conocimiento	25-26	
				Intercambio	27-28	
				Planificación	29-30	
			Innovación Tecnológica	Sensibilización	31-32	
				Accesibilidad	33-34	
				Ejecución	35-36	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Investigación Básica. **Diseño:** No experimental Del tipo transversal con un enfoque correlacional causal.	**Población:** 100 Trabajadores **Tamaño de muestra:** 79 trabajadores **Muestreo:** **Probabilístico de tipo aleatorio simple**	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** En el análisis descriptivo se utilizará tablas de contingencia cuyo resultado se presentará mediante tablas e histogramas lo cual será dirigido a un análisis bidimensional. **Inferencial:** Se ejecutará mediante un análisis estadístico no paramétrico utilizando un coeficiente de regresión logística ordinal con el cual justificaremos de manera adecuada el grado de incidencia existente entre la variable independiente y la dependiente.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable Independiente: Ciberseguridad Leiva (2015) define a la Ciberseguridad como procedimientos de uso, procesos y las nuevas tecnologías que van a permitir la prevención, detección y recuperación de aquellos daños que se puedan provocar a la confidencialidad, integridad y disponibilidad de la información en el espacio cibernético.	**Prevención** Según Romero et. Al (2018) consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es por lo que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos	Control	1	¿Consideras que los controles de acceso a su laptop y/o PC son suficientes para evitar ser víctima de delincuentes cibernéticos?	
			2	¿Consideras necesario el bloqueo de puertos USB de tú laptop y/o PC?	
		Conocimiento	3	¿Conoce si su empresa cuenta con algún plan de capacitación para evitar ser víctimas de ataques cibernéticos?	
			4	¿Conoce sobre algún programa de concientización sobre ciberseguridad que su empresa haya realizado?	
		Confiabilidad	5	¿Confías que el área de Soporte TI cuenta con personal capacitado que realiza revisiones de manera correcta que eviten en un futuro ataques cibernéticos?	
			6	¿Confías que las políticas de ciberseguridad establecidas en la empresa han ayudado hasta el momento en la prevención de ataques cibernéticos?	
		Control	7	¿Sabe qué medidas de control debe tomar en caso detecte actividades poco inusuales en algunos de los dispositivos electrónicos que la empresa le asignó?	

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Detección Según Defaz & Yanchapaxi (2006) es aquella que se encarga de detectar los ataques en el momento que se están realizando, y así poder contrarrestarlos debidamente, una de las principales funciones de la seguridad es identificar y eliminar las vulnerabilidades y los ataques.		8	¿Conoce que herramientas de control se utilizan para la detección de ataques cibernéticos en la empresa?	
		Monitoreo	9	¿Está de acuerdo con que el área de TI monitoree de manera constante actividades que usted realiza cuando se conecta a la red de la empresa?	
			10	¿Sabe si la empresa cuenta con un plan y herramientas de detección que permita anticipar un ataque cibernético?	
		Conocimiento	11	¿Conoce cuáles son los controles con los que se cuenta para ingresar a la empresa?	
			12	¿Conoce si la empresa cuenta con un plan que permita mejorar la detección de ataques cibernéticos?	
	Recuperación Según Defaz & Yanchapaxi (2006) la recuperación es la parte más crítica, ya que no se ha logrado evitar el ataque se debe recuperar todo el equipo como lo teníamos en un inicio borrando el ataque para poder continuar normalmente.	Proceso	13	¿Sabe cuál es el proceso de recuperación que el área de TI pone en marcha después de un ataque y/o evento cibernético?	
			14	¿Sabe cuán importante es que la empresa cuente con un Plan de Contingencia y Continuidad de Negocio?	
			15	¿En referencia a las políticas de seguridad de la empresa, usted tiene acceso a la documentación respectiva?	
				¿Sabe si la empresa cuenta con algún repositorio dónde usted pueda acceder e informarse sobre	

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
		Documentación	16	los tipos de ataques cibernéticos, suplantaciones de identidad (phishing), etc.?	
		Difusión	17	¿La empresa cuenta con un plan de difusión sobre qué medidas debe tomar en cuenta para evitar ser víctimas de ataques cibernéticos?	
			18	¿Conoce que canales digitales utiliza la empresa para difundir información sobre como evitar ser víctima de ataques cibernéticos?	
Variable Dependiente: Gestión de Tecnologías de Información Mendoza & Valenzuela (2014) definen a la Gestión de Tecnologías de Información como la unión de tres niveles que son la dirección estratégica, transferencia e innovación tecnológica que permiten organizar y direccionar los recursos humanos y económicos con la finalidad de aumentar nuevos conocimientos, generar	**Dirección estratégica** Burbano (2017) nos dice que la Dirección estratégica consiste en formular estrategias que permitan el desarrollo de la organización, buscando de esta manera generar una mayor participación en el mercado y procurando siempre obtener mayores rendimientos.	Participación	19	¿En su empresa ha sido participe de talleres, dónde se le ha capacitado sobre Phishing, virus informático, etc.?	
			20	¿Ha recibido capacitaciones por parte de la empresa sobre cómo actuar frente a un posible ataque cibernético?	
		Uso	21	¿Usted tiene acceso a los diferentes sistemas y/o aplicaciones con los que cuenta la empresa?	
			22	¿Está de acuerdo que solo se le permita el acceso a los sistemas y/o aplicaciones de acuerdo a su perfil (jefe, asesor, ejecutivo de ventas, etc.)?	
		Confiabilidad	23	¿Confía en el servicio que brinda el área de soporte y operaciones TI?	
			24	¿Si un día pierde información de su PC y/o laptop asignados por la empresa, estará confiado porque la empresa realiza backups de manera constante y podrá recuperarla?	

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
ideas técnicas con las que se pueden obtener nuevos productos, procesos y servicios o mejorar las que ya existen, así como el desarrollo de estas ideas en prototipos de trabajo y su transferencia.	**Transferencia tecnológica** Sonmezturk et al. (2022) indican que la Transferencia tecnológica se puede definir como el traslado de conocimientos, de una institución a otra, en este caso, el flujo de conocimiento tecnológico es intencional y se materializa en mecanismos específicos de transferencia.	Conocimiento	25	¿Conoce usted de algún programa (Capacitaciones, talleres, etc.) que permita al área de soporte y operaciones TI compartir sus conocimientos con sus proveedores de servicios?	
			26	¿Conoce usted que los diferentes procesos con las que cuenta el área de soporte y operaciones TI son atendidos por distintos proveedores?	
		Intercambio	27	¿Conoce usted si la empresa intercambia conocimientos con sus proveedores de servicios?	
			28	¿Cree usted que intercambiar conocimientos tecnológicos sea beneficioso para la mejora del servicio que brinda el área de soporte y operaciones TI?	
		Planificación	29	¿Para usted es importante que la empresa planifique capacitaciones que permitan el intercambio y/o actualización de conocimientos a sus proveedores de servicios?	
			30	¿Está de acuerdo con que la implementación de planes de capacitación incrementa las habilidades técnicas y mejora el desempeño del personal de TI?	
	Innovación tecnológica Yu-Cheng & Shun-Hsing (2011) que nos dicen que la Innovación tecnológica es la forma en que	Sensibilización	31	¿Está de acuerdo con las innovaciones tecnológicas que viene implementando su empresa (centros compartidos, impresión vía wifi por ejemplo)?	

TÍTULO: La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022

AUTOR: Taína Licel Ramírez Alva

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	una organización puede seleccionar, implementar y utilizar eficientemente una tecnología en comparación con un competidor, también se puede incluir el conocimiento profesional necesario para diseñar, fabricar y ensamblar un producto o la eficiencia del personal en el uso de las herramientas de producción.		32	¿En referencia a las innovaciones tecnológicas, se le ha informado sobre cambios que realizará o viene realizando su empresa?	
		Accesibilidad	33	¿Tiene acceso a las innovaciones tecnológicas que actualmente su empresa viene implementando?	
			34	¿Cree que el acceso a la tecnología mejora su productividad dentro de la empresa?	
		Ejecución	35	¿Conoce usted que proyectos de innovación tecnológica viene actualmente ejecutando su empresa?	
			36	¿Considera importante que su empresa estimule la innovación mediante la ejecución de proyectos tecnológicos?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para trabajadores de una empresa de Seguros.

Fecha: [/ /] **Edad:** [ ]

Sexo: Femenino[ ] Masculino[ ]

Ocupación: Gerente [ ] Subgerente[ ] Supervisor[ ] Jefe de área [ ] Personal TI [ ] Colaborador(a) [ ]

Grado de estudio: Superior Técnica [ ] Superior Universitaria[ ]

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente **ejemplo**: (1) No es importante, (2) Poco importante, (3) Ni poco ni mucho, (4) Importante, (5) Muy importante.

No	Pregunta	Valoración				
		1	2	3	4	5
	Sobre Ciberseguridad					
1	¿Consideras que los controles de acceso a su laptop y/o PC son suficientes para evitar ser víctima de delincuentes cibernéticos?	Nada suficiente	Poco suficiente	Ni poco, ni mucho	Suficiente	Muy suficiente
2	¿Consideras necesario el bloqueo de puertos USB de tú laptop y/o PC?	Nada necesario	Poco necesario	Ni poco, ni mucho	Necesario	Muy necesario
3	¿Conoce si su empresa cuenta con algún plan de capacitación para evitar ser víctimas de ataques cibernéticos?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
4	¿Conoce sobre algún programa de concientización sobre ciberseguridad que su empresa haya realizado?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
5	¿Confías que el área de Soporte TI cuenta con personal capacitado que realiza revisiones de manera correcta que eviten en un futuro ataques cibernéticos?	No confío	Confío poco	Ni poco, ni mucho	Confío	Confió mucho
6	¿Confías que las políticas de ciberseguridad establecidas en la empresa han ayudado hasta el momento en la prevención de ataques cibernéticos?	No confío	Confío poco	Ni poco, ni mucho	Confío	Confío mucho
7	¿Sabe qué medidas de control debe tomar en caso detecte actividades poco inusuales en algunos de los dispositivos electrónicos que la empresa le asignó?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
8	¿Conoce que herramientas de control se utilizan para la detección de ataques cibernéticos en la empresa?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho

No	Pregunta	Valoración				
		1	2	3	4	5
9	¿Está de acuerdo con que el área de TI monitoree de manera constante actividades que usted realiza cuando se conecta a la red de la empresa?	Totalmente en desacuerdo	En Desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
10	¿Sabe si la empresa cuenta con un plan y herramientas de detección que permita anticipar un ataque cibernético?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
11	¿Conoce cuáles son los controles con los que se cuenta para ingresar a la empresa?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
12	¿Conoce si la empresa cuenta con un plan que permita mejorar la detección de ataques cibernéticos?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
13	¿Sabe cuál es el proceso de recuperación que el área de TI pone en marcha después de un ataque y/o evento cibernético?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
14	¿Sabe cuán importante es que la empresa cuente con un Plan de Contingencia y Continuidad de Negocio?	No es importante	Poco importante	Ni poco, ni mucho	Importante	Muy importante
15	¿En referencia a las políticas de seguridad de la empresa, usted tiene acceso a la documentación respectiva?	No tengo acceso	Poco acceso	Ni poco, ni mucho	Tengo acceso	Tengo acceso a todo
16	¿Sabe si la empresa cuenta con algún repositorio dónde usted pueda acceder e informarse sobre los tipos de ataques cibernéticos, suplantaciones de identidad (phishing), etc?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
17	¿La empresa cuenta con un plan de difusión sobre qué medidas debe tomar en cuenta para evitar ser víctimas de ataques cibernéticos?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
18	¿Conoce que canales digitales utiliza la empresa para difundir información sobre como evitar ser víctima de ataques cibernéticos?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
19	¿En su empresa ha sido participe de talleres, dónde se le ha capacitado sobre Phishing, virus informático, etc?	Ninguna Participación	Poca Participación	Ni poca, ni mucha	Varias Participaciones	Muchas Participaciones
20	¿Ha recibido capacitaciones por parte de la empresa sobre cómo actuar frente a un posible ataque cibernético?	Ninguna Capacitación	Poca capacitación	Ni poca, ni mucha	Varias capacitaciones	Muchas capacitaciones

No	Pregunta	Valoración				
		1	2	3	4	5
21	¿Usted tiene acceso a los diferentes sistemas y/o aplicaciones con los que cuenta la empresa?	No tengo acceso	Poco acceso	Ni poco, ni mucho	Tengo acceso	Tengo acceso a todo
22	¿Está de acuerdo que solo se le permita el acceso a los sistemas y/o aplicaciones de acuerdo a su perfil (Jefe, asesor, ejecutivo de ventas, etc.)?	Totalmente en desacuerdo	En Desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
23	¿Confía en el servicio que brinda el área de soporte y operaciones TI?	No confío	Confío poco	Ni poco, ni mucho	Confío	Confío mucho
24	¿Si un día pierde información de su PC y/o laptop asignados por la empresa, estará confiado porque la empresa realiza backups de manera constante y podrá recuperarla?	No confío	Confío poco	Ni poco, ni mucho	Confío	Confío mucho
25	¿Conoce usted de algún programa (Capacitaciones, talleres, etc.) que permita al área de soporte y operaciones TI compartir sus conocimientos con sus proveedores de servicios?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
26	¿Conoce usted que los diferentes procesos con las que cuenta el área de soporte y operaciones TI son atendidos por distintos proveedores?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
27	¿Conoce usted si la empresa intercambia conocimientos con sus proveedores de servicios?	No conozco	Conozco poco	Ni poco, ni mucho	Conozco	Conozco mucho
28	¿Cree usted que intercambiar conocimientos tecnológicos sea beneficioso para la mejora del servicio que brinda el área de soporte y operaciones TI?	No creo	Creo poco	Ni poco, ni mucho	Creo	Creo mucho
29	¿Para usted es importante que la empresa planifique capacitaciones que permitan el intercambio y/o actualización de conocimientos a sus proveedores de servicios?	No es importante	Poco importante	Ni poco, ni mucho	Importante	Muy importante
30	¿Está de acuerdo con que la implementación de planes de capacitación incrementa las habilidades técnicas y mejora el desempeño del personal de TI?	Totalmente en desacuerdo	En Desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
31	¿Está de acuerdo con las innovaciones tecnológicas que viene implementando su empresa (centros compartidos, impresión vía wifi por ejemplo)?	Totalmente en desacuerdo	En Desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
32	¿En referencia a las innovaciones tecnológicas, se le ha informado sobre cambios que realizará o viene realizando su empresa?	Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre

No	Pregunta	Valoración				
		1	2	3	4	5
33	¿Tiene acceso a las innovaciones tecnológicas que actualmente su empresa viene implementando?	No tengo	Tengo poco	Ni poco, ni mucho	Tengo	Tengo mucho
34	¿Cree que el acceso a la tecnología mejora su productividad dentro de la empresa?	No creo	Creo poco	Ni poco, ni mucho	Creo	Creo mucho
35	¿Conoce usted que proyectos de innovación tecnológica viene actualmente ejecutando su empresa?	No conozco	Conozco algo	Ni poco, ni mucho	Conozco	Conozco bastante
36	¿Considera importante que su empresa estimule la innovación mediante la ejecución de proyectos tecnológicos?	No es importante	Poco importante	Ni poco, ni mucho	Importante	Muy importante

¡Gracias por su tiempo!

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1

VARIABLE: Ciberseguridad

N°	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PREVENCIÓN	Si	No	Si	No	Si	No	
1	¿Consideras que los controles de acceso a su laptop y/o PC son suficientes para evitar ser víctima de delincuentes cibernéticos?	X		X		X		
2	¿Consideras necesario el bloqueo de puertos USB de tú laptop y/o PC?	X		X		X		
3	¿Conoce si su empresa cuenta con algún plan de capacitación para evitar ser víctimas de ataques cibernéticos?	X		X		X		
4	¿Conoce sobre algún programa de concientización sobre ciberseguridad que su empresa haya realizado?	X		X		X		
5	¿Confías que el área de Soporte TI cuenta con personal capacitado que realiza revisiones de manera correcta que eviten en un futuro ataques cibernéticos?	X		X		X		
6	¿Confías que las políticas de ciberseguridad establecidas en la empresa han ayudado hasta el momento en la prevención de ataques cibernéticos?	X		X		X		
	DETECCIÓN	Si	No	Si	No	Si	No	
7	¿Sabe qué medidas de control debe tomar en caso detecte actividades poco inusuales en algunos de los dispositivos electrónicos que la empresa le asignó?	X		X		X		
8	¿Conoce que herramientas de control se utilizan para la detección de ataques cibernéticos en la empresa?	X		X		X		
9	¿Está de acuerdo con que el área de TI monitoree de manera constante actividades que usted realiza cuando se conecta a la red de la empresa?	X		X		X		
10	¿Sabe si la empresa cuenta con un plan y herramientas de detección que permita anticipar un ataque cibernético?	X		X		X		
11	¿Conoce cuáles son los controles con los que se cuenta para ingresar a la empresa?	X		X		X		
12	¿Conoce si la empresa cuenta con un plan que permita mejorar la detección de ataques cibernéticos?	X		X		X		
	RECUPERACIÓN	Si	No	Si	No	Si	No	
13	¿Sabe cuál es el proceso de recuperación que el área de TI pone en marcha después de un ataque y/o evento cibernético?	X		X		X		
14	¿Sabe cuán importante es que la empresa cuente con un Plan de Contingencia y Continuidad de Negocio?	X		X		X		
15	¿En referencia a las políticas de seguridad de la empresa, usted tiene acceso a la documentación respectiva?	X		X		X		
16	¿Sabe si la empresa cuenta con algún repositorio dónde usted pueda acceder e informarse sobre los tipos de ataques cibernéticos, suplantaciones de identidad (phishing), etc?	X		X		X		

N°	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
17	¿La empresa cuenta con un plan de difusión sobre qué medidas debe tomar en cuenta para evitar ser víctimas de ataques cibernéticos?	X		X		X		
18	¿Conoce que canales digitales utiliza la empresa para difundir información sobre cómo evitar ser víctima de ataques cibernéticos?	X		X		X		

VARIABLE: Gestión de Tecnologías de Información

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	DIRECCIÓN ESTRATÉGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿En su empresa ha sido partícipe de talleres, dónde se le ha capacitado sobre Phishing, virus informático, etc?	X		X		X		
20	¿Ha recibido capacitaciones por parte de la empresa sobre cómo actuar frente a un posible ataque cibernético?	X		X		X		
21	¿Usted tiene acceso a los diferentes sistemas y/o aplicaciones con los que cuenta la empresa?	X		X		X		
22	¿Está de acuerdo que solo se le permita el acceso a los sistemas y/o aplicaciones de acuerdo a su perfil (Jefe, asesor, ejecutivo de ventas,etc.)?	X		X		X		
23	¿Confía en el servicio que brinda el área de soporte y operaciones TI?	X		X		X		
24	¿Si un día pierde información de su PC y/o laptop asignados por la empresa, estará confiado porque la empresa realiza backups de manera constante y podrá recuperarla?	X		X		X		
	TRANSFERENCIA TECNOLÓGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Conoce usted de algún programa (Capacitaciones, talleres, etc.) que permita al área de soporte y operaciones TI compartir sus conocimientos con sus proveedores de servicios?	X		X		X		
26	¿Conoce usted que los diferentes procesos con las que cuenta el área de soporte y operaciones TI son atendidos por distintos proveedores?	X		X		X		
27	¿Conoce usted si la empresa intercambia conocimientos con sus proveedores de servicios?	X		X		X		
28	¿Cree usted que intercambiar conocimientos tecnológicos sea beneficioso para la mejora del servicio que brinda el área de soporte y operaciones TI?	X		X		X		
29	¿Para usted es importante que la empresa planifique capacitaciones que permitan el intercambio y/o actualización de conocimientos a sus proveedores de servicios?	X		X		X		

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
30	¿Está de acuerdo con que la implementación de planes de capacitación incrementa las habilidades técnicas y mejora el desempeño del personal de TI?	X		X		X		
	INNOVACIÓN TECNOLÓGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Está de acuerdo con las innovaciones tecnológicas que viene implementando su empresa (centros compartidos, impresión vía wifi por ejemplo)?	X		X		X		
32	¿En referencia a las innovaciones tecnológicas, se le ha informado sobre cambios que realizará o viene realizando su empresa?	X		X		X		
33	¿Tiene acceso a las innovaciones tecnológicas que actualmente su empresa viene implementando?	X		X		X		
34	¿Cree que el acceso a la tecnología mejora su productividad dentro de la empresa?	X		X		X		
35	¿Conoce usted que proyectos de innovación tecnológica viene actualmente ejecutando su empresa?	X		X		X		
36	¿Considera importante que su empresa estimule la innovación mediante la ejecución de proyectos tecnológicos?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

14 de octubre del 2022

Apellidos y nombre s del juez evaluador: LEZAMA GONZALES PEDRO MARTIN DNI: 09656793

Especialista: Metodólogo [X] Temático [X]

Grado: Maestro [ ] Doctor [X]

Firma del Experto Informante

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Validación del Experto N°2

VARIABLE: Ciberseguridad

N°	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PREVENCIÓN	Si	No	Si	No	Si	No	
1	¿Consideras que los controles de acceso a su laptop y/o PC son suficientes para evitar ser víctima de delincuentes cibernéticos?	X		X		X		
2	¿Consideras necesario el bloqueo de puertos USB de tú laptop y/o PC?	X		X		X		
3	¿Conoce si su empresa cuenta con algún plan de capacitación para evitar ser víctimas de ataques cibernéticos?	X		X		X		
4	¿Conoce sobre algún programa de concientización sobre ciberseguridad que su empresa haya realizado?	X		X		X		
5	¿Confías que el área de Soporte TI cuenta con personal capacitado que realiza revisiones de manera correcta que eviten en un futuro ataques cibernéticos?	X		X		X		
6	¿Confías que las políticas de ciberseguridad establecidas en la empresa han ayudado hasta el momento en la prevención de ataques cibernéticos?	X		X		X		
	DETECCIÓN	Si	No	Si	No	Si	No	
7	¿Sabe qué medidas de control debe tomar en caso detecte actividades poco inusuales en algunos de los dispositivos electrónicos que la empresa le asignó?	X		X		X		
8	¿Conoce que herramientas de control se utilizan para la detección de ataques cibernéticos en la empresa?	X		X		X		
9	¿Está de acuerdo con que el área de TI monitoree de manera constante actividades que usted realiza cuando se conecta a la red de la empresa?	X		X		X		
10	¿Sabe si la empresa cuenta con un plan y herramientas de detección que permita anticipar un ataque cibernético?	X		X		X		
11	¿Conoce cuáles son los controles con los que se cuenta para ingresar a la empresa?	X		X		X		
12	¿Conoce si la empresa cuenta con un plan que permita mejorar la detección de ataques cibernéticos?	X		X		X		
	RECUPERACIÓN	Si	No	Si	No	Si	No	
13	¿Sabe cuál es el proceso de recuperación que el área de TI pone en marcha después de un ataque y/o evento cibernético?	X		X		X		
14	¿Sabe cuán importante es que la empresa cuente con un Plan de Contingencia y Continuidad de Negocio?	X		X		X		
15	¿En referencia a las políticas de seguridad de la empresa, usted tiene acceso a la documentación respectiva?	X		X		X		
16	¿Sabe si la empresa cuenta con algún repositorio dónde usted pueda acceder e informarse sobre los tipos de ataques cibernéticos, suplantaciones de identidad (phishing), etc?	X		X		X		

N°	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
17	¿La empresa cuenta con un plan de difusión sobre qué medidas debe tomar en cuenta para evitar ser víctimas de ataques cibernéticos?	X		X		X		
18	¿Conoce que canales digitales utiliza la empresa para difundir información sobre cómo evitar ser víctima de ataques cibernéticos?	X		X		X		

VARIABLE: Gestión de Tecnologías de Información

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	DIRECCIÓN ESTRATÉGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿En su empresa ha sido participe de talleres, dónde se le ha capacitado sobre Phishing, virus informático, etc?	X		X		X		
20	¿Ha recibido capacitaciones por parte de la empresa sobre cómo actuar frente a un posible ataque cibernético?	X		X		X		
21	¿Usted tiene acceso a los diferentes sistemas y/o aplicaciones con los que cuenta la empresa?	X		X		X		
22	¿Está de acuerdo que solo se le permita el acceso a los sistemas y/o aplicaciones de acuerdo a su perfil (Jefe, asesor, ejecutivo de ventas,etc.)?	X		X		X		
23	¿Confía en el servicio que brinda el área de soporte y operaciones TI?	X		X		X		
24	¿Si un día pierde información de su PC y/o laptop asignados por la empresa, estará confiado porque la empresa realiza backups de manera constante y podrá recuperarla?	X		X		X		
	TRANSFERENCIA TECNOLÓGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Conoce usted de algún programa (Capacitaciones, talleres, etc.) que permita al área de soporte y operaciones TI compartir sus conocimientos con sus proveedores de servicios?	X		X		X		
26	¿Conoce usted que los diferentes procesos con las que cuenta el área de soporte y operaciones TI son atendidos por distintos proveedores?	X		X		X		
27	¿Conoce usted si la empresa intercambia conocimientos con sus proveedores de servicios?	X		X		X		
28	¿Cree usted que intercambiar conocimientos tecnológicos sea beneficioso para la mejora del servicio que brinda el área de soporte y operaciones TI?	X		X		X		
29	¿Para usted es importante que la empresa planifique capacitaciones que permitan el intercambio y/o actualización de conocimientos a sus proveedores de servicios?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
30	¿Está de acuerdo con que la implementación de planes de capacitación incrementa las habilidades técnicas y mejora el desempeño del personal de TI?	X		X		X		
	INNOVACIÓN TECNOLÓGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Está de acuerdo con las innovaciones tecnológicas que viene implementando su empresa (centros compartidos, impresión vía wifi por ejemplo)?	X		X		X		
32	¿En referencia a las innovaciones tecnológicas, se le ha informado sobre cambios que realizará o viene realizando su empresa?	X		X		X		
33	¿Tiene acceso a las innovaciones tecnológicas que actualmente su empresa viene implementando?	X		X		X		
34	¿Cree que el acceso a la tecnología mejora su productividad dentro de la empresa?	X		X		X		
35	¿Conoce usted que proyectos de innovación tecnológica viene actualmente ejecutando su empresa?	X		X		X		
36	¿Considera importante que su empresa estimule la innovación mediante la ejecución de proyectos tecnológicos?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

14 de octubre del 2022

Apellidos y nombre s del juez evaluador: Quinteros Navarro Dino Michael DNI: 41567782

Especialista: Metodólogo [X] Temático [X]

Grado: Maestro [X] Doctor [ ]

Firma del Experto Informante

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Validación del Experto N°3

VARIABLE: Ciberseguridad

N°	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PREVENCIÓN	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Consideras que los controles de acceso a su laptop y/o PC son suficientes para evitar ser víctima de delincuentes cibernéticos?	X		X		X		
2	¿Consideras necesario el bloqueo de puertos USB de tú laptop y/o PC?	X		X		X		
3	¿Conoce si su empresa cuenta con algún plan de capacitación para evitar ser víctimas de ataques cibernéticos?	X		X		X		
4	¿Conoce sobre algún programa de concientización sobre ciberseguridad que su empresa haya realizado?	X		X		X		
5	¿Confías que el área de Soporte TI cuenta con personal capacitado que realiza revisiones de manera correcta que eviten en un futuro ataques cibernéticos?	X		X		X		
6	¿Confías que las políticas de ciberseguridad establecidas en la empresa han ayudado hasta el momento en la prevención de ataques cibernéticos?	X		X		X		
	DETECCIÓN	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Sabe qué medidas de control debe tomar en caso detecte actividades poco inusuales en algunos de los dispositivos electrónicos que la empresa le asignó?	X		X		X		
8	¿Conoce que herramientas de control se utilizan para la detección de ataques cibernéticos en la empresa?	X		X		X		
9	¿Está de acuerdo con que el área de TI monitoree de manera constante actividades que usted realiza cuando se conecta a la red de la empresa?	X		X		X		
10	¿Sabe si la empresa cuenta con un plan y herramientas de detección que permita anticipar un ataque cibernético?	X		X		X		
11	¿Conoce cuáles son los controles con los que se cuenta para ingresar a la empresa?	X		X		X		
12	¿Conoce si la empresa cuenta con un plan que permita mejorar la detección de ataques cibernéticos?	X		X		X		
	RECUPERACIÓN	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Sabe cuál es el proceso de recuperación que el área de TI pone en marcha después de un ataque y/o evento cibernético?	X		X		X		
14	¿Sabe cuán importante es que la empresa cuente con un Plan de Contingencia y Continuidad de Negocio?	X		X		X		
15	¿En referencia a las políticas de seguridad de la empresa, usted tiene acceso a la documentación respectiva?	X		X		X		
16	¿Sabe si la empresa cuenta con algún repositorio dónde usted pueda acceder e informarse sobre los tipos de ataques cibernéticos, suplantaciones de identidad (phishing), etc?	X		X		X		

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
17	¿La empresa cuenta con un plan de difusión sobre qué medidas debe tomar en cuenta para evitar ser víctimas de ataques cibernéticos?	X		X		X		
18	¿Conoce que canales digitales utiliza la empresa para difundir información sobre cómo evitar ser víctima de ataques cibernéticos?	X		X		X		

VARIABLE: Gestión de Tecnologías de Información

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	DIRECCIÓN ESTRATÉGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿En su empresa ha sido partícipe de talleres, dónde se le ha capacitado sobre Phishing, virus informático, etc?	X		X		X		
20	¿Ha recibido capacitaciones por parte de la empresa sobre cómo actuar frente a un posible ataque cibernético?	X		X		X		
21	¿Usted tiene acceso a los diferentes sistemas y/o aplicaciones con los que cuenta la empresa?	X		X		X		
22	¿Está de acuerdo que solo se le permita el acceso a los sistemas y/o aplicaciones de acuerdo a su perfil (Jefe, asesor, ejecutivo de ventas,etc.)?	X		X		X		
23	¿Confía en el servicio que brinda el área de soporte y operaciones TI?	X		X		X		
24	¿Si un día pierde información de su PC y/o laptop asignados por la empresa, estará confiado porque la empresa realiza backups de manera constante y podrá recuperarla?	X		X		X		
	TRANSFERENCIA TECNOLÓGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Conoce usted de algún programa (Capacitaciones, talleres, etc.) que permita al área de soporte y operaciones TI compartir sus conocimientos con sus proveedores de servicios?	X		X		X		
26	¿Conoce usted que los diferentes procesos con las que cuenta el área de soporte y operaciones TI son atendidos por distintos proveedores?	X		X		X		
27	¿Conoce usted si la empresa intercambia conocimientos con sus proveedores de servicios?	X		X		X		
28	¿Cree usted que intercambiar conocimientos tecnológicos sea beneficioso para la mejora del servicio que brinda el área de soporte y operaciones TI?	X		X		X		
29	¿Para usted es importante que la empresa planifique capacitaciones que permitan el intercambio y/o actualización de conocimientos a sus proveedores de servicios?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
30	¿Está de acuerdo con que la implementación de planes de capacitación incrementa las habilidades técnicas y mejora el desempeño del personal de TI?	X		X		X		
	INNOVACIÓN TECNOLÓGICA	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Está de acuerdo con las innovaciones tecnológicas que viene implementando su empresa (centros compartidos, impresión vía wifi por ejemplo)?	X		X		X		
32	¿En referencia a las innovaciones tecnológicas, se le ha informado sobre cambios que realizará o viene realizando su empresa?	X		X		X		
33	¿Tiene acceso a las innovaciones tecnológicas que actualmente su empresa viene implementando?	X		X		X		
34	¿Cree que el acceso a la tecnología mejora su productividad dentro de la empresa?	X		X		X		
35	¿Conoce usted que proyectos de innovación tecnológica viene actualmente ejecutando su empresa?	X		X		X		
36	¿Considera importante que su empresa estimule la innovación mediante la ejecución de proyectos tecnológicos?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

17 de octubre del 2022

Apellidos y nombre s del juez evaluador: CARLOS ENRIQUE LÒPEZ RODRÌGUEZ DNI: 00865537

Especialista: Metodólogo [X] Temático [X]

Grado: Maestro [ ] Doctor [X]

Firma del Experto Informante

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Anexo 5: Base de datos de la aplicación

Encuesta	Sexo	V1																		V2																	
		D1						D2						D3						D1						D2						D3					
		I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	2	4	3	2	4	5	3	4	3	2	1	4	3	2	3	3	4	4	3	4	3	4	5	4	4	3	4	4	4	4	4	4	4	4	5	4	4
2	2	4	2	4	2	4	5	3	3	2	3	4	4	2	3	4	3	3	4	4	4	3	4	5	4	4	3	3	4	5	4	4	4	4	4	5	4
3	1	2	4	5	2	3	2	2	2	3	3	5	4	3	4	2	4	4	3	3	3	4	3	4	3	3	4	4	4	4	3	3	4	4	5	3	5
4	1	4	4	4	3	3	3	3	3	4	4	3	4	4	5	5	5	3	4	2	3	5	4	4	3	3	4	5	4	5	2	5	4	4	4	3	4
5	1	1	3	4	3	4	3	5	3	4	4	5	4	5	5	3	5	3	4	4	5	4	4	3	4	3	5	4	5	4	3	3	4	5	5	4	3
6	1	2	5	2	3	5	3	2	5	3	5	3	3	4	5	4	5	4	5	1	3	4	3	4	3	5	4	4	4	3	5	4	5	3	3	5	4
7	1	2	3	3	3	3	3	3	3	5	4	5	5	4	5	3	4	5	5	4	5	4	4	5	4	4	5	4	3	4	2	3	3	3	3	3	5
8	1	1	2	3	1	2	3	2	2	3	2	3	1	3	2	3	1	2	4	1	2	2	1	1	2	1	2	1	2	1	2	3	4	5	5	4	3
9	2	3	5	2	4	2	4	2	4	3	5	3	5	4	5	5	5	2	5	4	4	5	4	4	3	3	5	4	5	4	3	5	4	4	4	3	4
10	1	3	4	3	4	3	4	3	4	2	4	4	4	4	4	5	5	4	4	3	5	5	5	4	5	5	5	4	4	5	4	2	3	3	2	2	2
11	2	1	5	4	4	4	5	2	4	3	4	5	3	4	4	4	4	4	4	4	4	5	4	4	3	3	5	4	5	4	3	5	4	4	4	3	4
12	1	2	5	3	5	4	4	5	4	3	4	5	4	4	5	2	4	2	3	3	5	4	5	2	5	2	4	2	5	2	5	5	4	3	5	4	3
13	1	5	5	4	5	5	4	5	4	3	4	2	4	2	5	2	3	2	3	5	4	4	4	3	4	4	5	4	4	5	5	1	2	2	3	2	3
14	1	4	3	5	4	3	4	5	4	3	4	3	4	5	4	2	4	2	4	3	2	3	2	2	2	3	3	5	4	5	5	1	4	5	5	5	4
15	2	3	5	3	5	4	5	5	5	3	5	2	4	4	4	2	3	2	4	5	4	5	4	4	3	3	5	4	5	4	3	5	4	4	4	3	4
16	2	4	3	2	4	3	4	2	4	3	4	4	4	5	4	5	4	5	4	3	4	4	5	5	4	4	3	4	2	3	2	4	4	5	3	4	5
17	1	1	2	3	4	5	3	4	4	5	4	5	3	4	4	4	4	5	4	4	4	5	4	4	3	3	5	4	5	4	3	5	4	4	4	3	4
18	2	1	5	5	4	3	4	4	3	4	4	4	4	4	4	4	3	4	4	4	4	5	4	4	3	4	5	3	5	4	3	5	4	4	4	3	4
19	1	4	3	5	3	2	3	3	3	4	4	3	4	5	4	4	5	3	4	1	3	3	2	5	3	2	4	5	4	5	4	4	3	5	5	4	3
20	1	1	2	1	3	5	4	4	4	4	4	5	4	5	5	4	5	4	4	2	5	3	2	2	4	4	5	4	5	4	3	4	5	5	4	3	4
21	1	3	5	2	3	5	3	2	3	3	5	4	3	4	5	4	5	4	5	3	5	5	4	3	4	4	5	4	5	3	3	4	4	3	4	4	5
22	2	2	5	4	4	3	4	5	4	3	4	3	4	2	4	4	4	5	4	5	4	5	4	5	4	4	3	4	4	3	4	3	2	4	3	3	4
23	1	1	4	5	5	2	3	5	3	3	4	5	4	3	5	3	3	5	4	3	4	3	4	4	2	1	1	3	1	3	1	1	2	2	3	2	3

Encuesta	Sexo	V1																		V2																	
		D1						D2						D3						D1						D2						D3					
		I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
24	2	1	5	2	5	3	4	5	4	5	4	3	4	2	4	5	4	5	4	5	5	5	4	4	5	5	5	4	4	4	5	2	2	1	3	1	4
25	2	3	4	3	4	3	4	3	4	4	4	5	4	3	5	4	3	5	3	3	4	3	5	4	5	3	4	5	5	3	4	4	5	5	3	5	2
26	1	2	5	5	3	3	2	5	2	3	3	4	3	5	5	5	4	5	4	4	4	5	4	5	2	4	4	3	4	5	4	4	4	4	3	5	4
27	1	3	5	4	5	3	5	3	4	3	4	2	4	3	5	4	4	3	4	5	4	4	2	5	4	3	5	3	2	3	4	2	5	4	5	3	5
28	2	1	5	3	4	3	3	3	5	2	5	4	5	4	5	4	4	4	4	3	3	5	2	5	3	4	4	3	5	3	4	4	5	2	5	5	3
29	1	4	5	4	5	1	4	5	4	1	4	3	4	5	4	5	4	2	4	2	5	4	4	4	5	2	3	5	3	4	3	3	4	4	5	4	4
30	1	1	5	4	5	3	5	3	5	3	5	4	4	3	4	3	3	4	4	3	4	3	5	5	4	3	5	4	4	3	5	2	4	4	5	5	4
31	1	1	5	3	4	3	3	3	5	2	5	4	5	4	5	4	4	4	4	4	4	5	4	4	3	2	4	5	4	5	4	5	4	4	4	3	4
32	1	1	2	1	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	4	5	3	3	5	2	4	5	5	5	3	2	2	4	4	5	5	4
33	1	4	4	4	4	3	4	5	3	4	3	4	3	4	5	4	3	4	3	4	4	5	4	4	3	3	4	5	4	4	4	5	4	4	4	3	4
34	1	4	3	2	3	2	3	3	3	4	4	3	4	2	4	2	5	3	4	3	3	5	4	5	4	1	2	3	4	3	2	5	4	4	4	3	4
35	2	2	4	4	3	2	3	5	3	4	4	5	4	5	5	3	5	3	4	4	5	3	3	2	4	3	4	5	4	3	5	5	4	2	5	3	5
36	1	2	2	4	3	5	3	5	3	3	5	3	3	4	5	4	5	4	5	4	4	5	4	4	3	3	2	3	4	3	4	4	4	4	4	4	5
37	2	3	5	5	3	5	5	3	5	2	4	3	3	3	5	3	3	2	5	4	5	4	3	5	3	2	3	3	2	3	2	3	5	4	3	4	5
38	2	1	4	5	4	2	5	5	3	3	4	3	4	3	5	3	3	5	4	4	3	5	5	5	2	2	2	1	2	3	2	4	4	5	4	3	4
39	1	3	5	2	4	2	4	2	4	3	5	3	5	4	5	3	5	4	5	3	5	4	5	2	5	1	5	4	2	5	5	3	5	5	2	5	3
40	1	4	5	3	2	3	1	3	2	2	1	4	2	3	4	3	5	3	4	3	3	2	3	2	1	3	2	3	2	3	3	2	2	3	2	1	3
41	1	3	5	5	4	3	5	5	3	3	4	2	3	5	2	5	4	2	4	4	5	5	2	4	4	2	3	2	4	1	2	5	4	4	4	3	4
42	1	4	5	4	5	4	5	4	4	4	4	3	4	1	5	2	4	2	4	4	4	3	5	4	4	4	5	3	5	3	4	3	5	2	5	5	4
43	2	4	5	4	5	2	4	5	4	3	4	5	4	3	5	2	3	2	3	4	4	5	4	4	3	1	4	3	2	3	4	3	4	5	4	4	4
44	2	2	3	1	4	5	3	4	4	5	4	5	3	4	4	4	4	5	4	5	3	3	4	3	3	2	5	5	2	5	5	3	4	4	5	4	4
45	2	4	4	5	5	4	5	3	5	3	5	4	4	2	4	2	3	2	4	4	3	3	5	2	4	4	5	3	4	4	4	3	3	4	5	4	5
46	1	1	5	3	4	3	4	4	4	3	4	3	4	2	4	5	4	4	4	3	2	4	2	1	2	2	2	1	2	1	1	5	5	2	5	3	4
47	2	1	3	4	4	5	3	4	4	5	4	5	3	4	2	4	4	5	4	4	4	5	4	4	3	3	4	5	4	4	4	5	4	4	4	3	4

Encuesta	Sexo	V1																		V2																	
		D1						D2						D3						D1						D2						D3					
		I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
48	2	5	4	4	4	3	4	4	3	4	3	4	4	5	2	3	5	4	3	2	4	5	4	5	4	3	4	5	5	4	3	3	4	5	5	4	3
49	1	2	4	3	4	3	4	5	3	4	5	3	4	3	5	4	4	5	4	4	5	3	4	3	5	4	4	5	2	5	4	5	2	5	5	4	3
50	1	2	5	3	3	3	2	4	5	5	3	4	5	3	4	3	5	4	5	4	4	5	4	4	3	2	4	5	4	5	4	5	4	4	4	3	4
51	1	3	5	2	5	5	5	5	5	3	4	2	4	2	4	4	3	4	3	4	2	3	4	5	4	4	5	4	5	5	4	5	4	3	2	2	3
52	1	3	4	2	5	4	5	4	5	4	4	3	4	5	3	2	4	3	4	3	2	4	5	2	4	4	3	4	5	4	4	4	4	4	4	4	4
53	1	3	3	5	4	5	3	4	4	5	4	5	3	3	4	3	4	3	3	3	4	5	4	4	4	5	3	3	5	3	5	5	4	4	4	3	4
54	1	5	4	5	4	3	4	4	3	4	3	5	3	4	3	4	3	4	3	4	5	4	3	4	4	2	5	3	5	5	4	5	3	4	5	3	4
55	2	2	5	2	5	5	5	5	5	3	4	2	4	2	4	4	4	4	3	5	4	4	3	5	3	4	4	4	5	3	4	4	5	5	4	3	3
56	1	1	4	4	3	4	3	5	3	4	4	5	4	5	5	3	5	3	4	3	2	4	4	3	4	3	4	5	4	5	4	5	4	5	3	5	4
57	2	3	4	2	3	5	3	4	3	3	5	4	4	4	5	5	4	4	3	3	4	4	4	4	5	2	3	2	3	4	3	5	4	5	5	5	3
58	2	4	5	3	4	3	3	3	5	2	5	4	5	4	4	4	3	4	3	3	5	3	4	4	5	2	5	4	4	5	4	2	4	5	3	5	5
59	2	2	2	2	3	2	3	1	2	2	2	3	1	2	2	3	3	5	2	1	2	4	3	2	2	3	2	2	1	2	3	1	2	1	2	1	2
60	1	2	5	3	4	3	2	3	5	2	5	4	5	4	5	4	4	4	4	5	4	2	4	5	4	5	5	5	3	2	4	5	2	4	5	4	4
61	2	3	5	3	4	5	2	3	5	2	5	4	5	4	4	3	4	4	3	3	4	4	3	5	5	5	4	3	4	4	4	4	4	4	5	4	3
62	1	3	4	4	5	4	5	4	3	2	4	2	5	5	2	4	4	5	3	5	4	4	3	3	5	2	4	3	5	5	5	4	5	4	4	5	2
63	2	3	4	4	5	4	3	5	2	5	4	3	5	4	2	3	5	3	4	1	4	5	5	4	5	3	3	4	5	4	5	4	3	5	3	5	4
64	1	1	2	1	3	2	1	2	3	1	5	2	3	3	3	3	2	3	2	1	2	3	4	2	2	1	2	2	3	3	2	2	3	3	2	2	3
65	1	3	4	5	2	5	2	1	2	5	5	5	4	5	4	5	4	5	2	4	4	5	4	3	4	2	4	5	5	5	3	5	3	4	3	5	4
66	2	2	4	4	5	4	5	4	3	4	2	4	4	5	4	4	2	4	4	4	5	4	4	3	4	4	5	4	5	4	3	3	5	3	5	4	4
67	1	2	2	4	2	5	5	4	4	5	5	2	5	2	5	4	5	2	5	3	5	5	4	3	4	4	5	4	4	3	4	5	3	4	4	3	5
68	2	3	3	4	3	3	2	3	4	3	4	5	4	5	5	4	4	4	5	4	5	4	3	4	4	4	4	5	4	5	4	4	3	2	3	4	2
69	1	3	3	2	1	2	3	1	3	2	1	3	1	3	3	3	3	2	3	3	3	5	4	4	5	1	1	1	2	1	3	1	1	2	1	1	2
70	2	2	3	2	3	2	1	2	2	1	3	2	3	2	3	2	3	2	4	2	3	2	1	3	2	4	2	3	2	2	3	2	1	3	3	2	2
71	2	3	4	3	4	4	2	5	2	3	5	4	3	3	5	4	5	5	4	2	1	3	2	2	1	2	3	1	2	1	3	3	2	2	3	4	2

Encuesta	Sexo	V1																		V2																	
		D1						D2						D3						D1						D2						D3					
		I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
72	2	2	4	5	4	5	5	4	4	5	4	3	5	2	5	3	2	3	3	2	4	5	5	5	3	2	4	3	2	2	2	4	3	5	4	3	5
73	1	4	2	2	3	5	5	5	3	4	3	4	3	5	3	4	4	4	5	3	5	3	4	4	5	4	4	2	2	1	2	3	3	2	2	3	2
74	1	1	2	2	3	2	1	2	3	2	1	2	2	2	3	2	2	4	5	3	1	2	2	3	3	2	3	2	1	2	3	2	3	2	2	2	4
75	1	2	2	3	3	5	4	3	5	2	4	2	5	5	4	5	4	5	5	4	4	5	4	4	4	3	4	5	4	5	3	3	4	2	3	3	4
76	1	3	4	5	4	5	5	5	5	4	3	2	4	2	3	4	3	3	4	5	5	5	4	2	4	4	4	3	4	4	5	3	4	4	5	4	5
77	2	4	4	4	5	5	4	4	4	2	4	5	3	4	3	4	4	3	3	1	2	4	3	3	4	3	4	3	4	3	4	1	3	3	5	5	5
78	1	2	3	4	4	4	4	5	4	3	4	5	4	4	4	5	5	4	4	4	4	5	4	4	1	3	4	3	4	4	4	4	3	4	4	2	3
79	2	4	2	4	3	5	4	3	3	1	5	5	4	4	3	5	5	4	4	5	5	2	4	5	4	4	5	3	4	4	2	3	4	3	4	3	4

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, VISURRAGA AGUERO JOEL MARTIN, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "La Ciberseguridad y su incidencia en la Gestión de Tecnologías de Información en una empresa de Seguros, Lima 2022", cuyo autor es RAMIREZ ALVA TAINA LICEL, constato que la investigación tiene un índice de similitud de 20.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 07 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
VISURRAGA AGUERO JOEL MARTIN **DNI:** 10192325 **ORCID:** 0000-0002-0024-668X	Firmado electrónicamente por: JMVISURRAGA el 11-01-2023 20:55:02

Código documento Trilce: TRI - 0513120

INVESTIGA UCV