ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERIA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE INFORMACIÓN

Ciberseguridad y su incidencia en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Mallqui Mallqui, Ampelio Juan de Mata (orcid.org/0000-0002-4930-5038)

ASESOR:

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

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2022

Dedicatoria

El presente trabajo de investigación está dedicado a mi familia y en especial a mi querido hijo Kael, por ser motivo de superación personal y profesional.

Agradecimiento

Agradezco a mi madre por haberme inculcado la perseverancia para logar mis objetivos. Asimismo, agradecer a los docentes de la Universidad Cesar Vallejo por contribuir en mi formación profesional.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

La presente investigación tiene como objetivo determinar la incidencia de la ciberseguridad en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022. Para ello, se desarrolló una investigación de tipo básica, con un diseño no experimental y clasificado como un estudio transversal de nivel correlacional-causal.

Asimismo, en la investigación se consideró una población de 321 servidores públicos de una Institución Administradora de Fondos de Aseguramiento en Salud – IAFAS de las sedes de Lima y Callao; en la cual se determinó a través de un muestreo probabilístico simple el tamaño muestral de 175 servidores. Para la recolección de datos de información se utilizó la técnica de encuesta y como instrumento cuestionario, la cual fue valido por juicio de expertos. De igual forma, para el análisis estadístico descriptivo se utilizaron tablas cruzadas e histogramas y para el análisis inferencial se utilizó pruebas paramétricas, aplicando el coeficiente de regresión ordinal.

Los resultados obtenidos permiten concluir que la variable ciberseguridad incide significativamente con un 53.7%, este valor indica que existe una correlación positiva considerable con la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

Palabras clave: Ciberseguridad, gestión de tecnologías de información, seguridad de sistemas de información

Abstract

The objective of this research is to determine the incidence of cybersecurity in the management of information technologies in an institution that administers health insurance funds, Lima 2022. For this, a basic type of research was developed, with a non-experimental and non-experimental design. Classified as a cross-sectional study of correlational-causal level.

Likewise, the research considered a population of 321 public servants from an Institution for the Administration of Health Insurance Funds - IAFAS from the Lima and Callao offices; in which the sample size of 175 servers was determined through a simple probabilistic sampling. For the collection of information data, the survey technique was used and as a questionnaire instrument, which was validated by expert judgment. Similarly, cross-tables and histograms were used for the descriptive statistical analysis, and parametric tests were used for the inferential analysis, applying the ordinal regression coefficient.

The results obtained allow us to conclude that the cybersecurity variable has a significant impact with 53.7%, this value indicates that there is a considerable positive correlation with the information technology management variable in an institution that administers health insurance funds, Lima 2022.

Keywords: Cybersecurity, information technology management, information systems security

I. INTRODUCCIÓN

La convergencia tecnológica en una sociedad cada vez más digital y tecnológicamente modificada, se establecen nuevos escenarios con mayor complejidad que exigen un análisis de negocio, enfocados en una vista holística a la ciberseguridad y la gestión de tecnologías de información (Gestión de TI). En ese contexto, surge el ciberespacio como una nueva dimensión de interacción social, que integra todo un conjunto de tecnologías de información e innovación, donde ya no es suficiente conocer y entender las amenazas, sino generar propuestas novedosas que permitan evaluar, detectar, prevenir y responder a las ciberamenazas actuales.

A nivel internacional, las instituciones públicas y privadas se han propuesto incrementar sus presupuestos a fin de proteger sus activos de información contra la ciberdelincuencia. En relación a ello, la revista IT Reseller (2022) menciona que, tres de cada 10 empresas españolas han sufrido ciberataques en el último año, la cual indica que, el 29% de las compañías en España afirmaron que tuvieron uno o más ciberataques con éxito y un 18% indica haber experimentado más de siete ciberataques en un mismo periodo. El elevado índice de amenazas a nivel mundial, ocasionado por los ataques de ransomware, phishing o ingeniería social, la vulneración de dispositivos NAS y la denegación de servicio (DoS), es motivo de preocupación ya que conlleva a la pérdida de información, el daño de equipos, la contratación de consultores expertos con un costo elevado y la pérdida de clientes.

Por otro lado, a nivel nacional, según la empresa EY Global, dedicada a la auditoría seguridad informática, Mishima (2021), menciona lo siguiente: el 51% de las empresas en el Perú han tenido ciberataques altamente efectivos desde 2020, el 63% de las empresas presentan una elevada preocupación por la poca capacidad de respuesta para gestionar una amenaza cibernética, el 42% de las empresas en el Perú están dispuestos a invertir en data y la adquisición de nuevas tecnologías

de seguridad, y el 45% se proyecta en la transformación digital en miras del ciberespacio.

Por consiguiente, en el Perú, se aprueba NTP ISO/IEC 27001:2014 que tiene en sus principales ejes y objetivos, implementar las políticas de sistema de gestión de seguridad de la información; asimismo, deberá ser aplicada bajo los nuevos enfoques de ciberseguridad ISO 27032, donde se pueda abordar riesgos y amenazas sobre los accesos no autorizados a los sistemas, ataques de software malicioso como el spyware, malware y ransomware.

Ante esta coyuntura muchas organizaciones a nivel nacional, se han visto con la necesidad de implementar nuevas herramientas tecnológicas, donde no sólo es suficiente adquirir o tener implementado los servicios de gestión de tecnología de información, sino que debe cumplir con los estándares de seguridad con enfoques holísticos y sistemáticos. La Institución Administradora de Fondos de Aseguramiento en Salud - IAFAS no es ajena a este problema, debido a que, en la institución se ha presentado ataques de ciberseguridad y pérdida de información en una de las sedes desconcentradas de la institución. Esto debido al ataque del software ransomware, donde se perdieron toda la información administrativa de muchos años, también se tuvo una disrupción en la operatividad de servicios a nivel de base de datos y sistemas. Razón por el cual, en el proyecto de investigación se propone evaluar la incidencia que tiene la ciberseguridad en la gestión de TI en una IAFAS, también denominada institución aseguradora de salud.

En ese sentido, se estableció el siguiente problema general: ¿De qué manera la ciberseguridad incide en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022?; asimismo, se consideró los siguientes problemas específicos: (a) ¿De qué manera la dimensión estrategias de seguridad de la ciberseguridad incide en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022?, (b) ¿De qué manera la dimensión protección de infraestructura critica

de la ciberseguridad incide en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022?, (c) ¿De qué manera la dimensión control técnico de seguridad de la ciberseguridad incide en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022?.

Por otro lado, la presente investigación se fundamenta con las siguientes justificaciones: La justificación epistemológica, donde se intenta evaluar la incidencia que tiene la ciberseguridad en la gestión de TI en una institución aseguradora de salud. En la cual, se utilizó un análisis de los valores implicados en la investigación, para transmitir un nuevo conocimiento e interpretación de los resultados a través de teorías, conceptos y métodos científicos. En cuanto, a la justificación teórica, permitirá establecer conocimientos fundamentales sobre la ciberseguridad y la gestión de TI, la cual permitirá un aporte de conocimientos para futuros investigadores. Asimismo, los resultados de la investigación brindarán una información valiosa a la institución para incorporar nuevos criterios y/o políticas de seguridad para una adecuada gestión de TI. De la misma forma, la investigación se apoya con la teoría general de sistemas y la teoría de las restricciones. En relación a la justificación práctica, la investigación permitirá contribuir a la institución, para enfocarse en la ciberseguridad, establecer nuevas políticas y de esta manera lograr una significativa incidencia en la gestión de TI y finamente la justificación metodológica, se realiza tomando en cuenta una investigación científica de diseño no experimental, para determinar un nivel correlación-causal entre las variables, cuyos resultados se obtendrán de la recopilación de datos de información haciendo uso de instrumentos validados por juicio de expertos.

Asimismo, como objetivo general se propone: Determinar la incidencia de la ciberseguridad en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022. Asimismo, se consideró los siguientes objetivos específicos: (a) Determinar la incidencia de la dimensión estrategias de seguridad de la ciberseguridad en la gestión de

tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022, (b) Determinar la incidencia de la dimensión protección de infraestructura crítica de la ciberseguridad en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022, (c) Determinar la incidencia de la dimensión control técnico de seguridad de la ciberseguridad en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

Por consiguiente, se estableció la hipótesis general: La ciberseguridad incide significativamente en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022. Asimismo, se establecen las hipótesis específicas: (a) La dimensión estrategias de seguridad de la ciberseguridad incide significativamente en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022, (b) La dimensión protección de infraestructura critica de la ciberseguridad incide significativamente en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022, (c) La dimensión control técnico de seguridad de la ciberseguridad incide significativamente en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

II. MARCO TEÓRICO.

Referente a los trabajos de investigación precedentes, que están vinculados con las variables de ciberseguridad y la gestión de TI, se mencionan los siguientes:

En el ámbito internacional, tenemos a Gumucio (2021), en su investigación titulada "Guía de implementación de un programa de gestión de riesgos de ciberseguridad en entidades de intermediación financiera", realizado en la Universidad de Chile, Chile, como objetivo determinó la evolución y estrategias de ciberseguridad para gestionar los posibles riesgos en una entidad financiera, aplicando el marco de buenas prácticas para la evaluación de riesgo NIST (National Institute of Standards and Technology); utilizó la metodología cuantitativa, llegando a la conclusión, que existe una brecha marcada entre los países de Latinoamérica, para la evaluación y regulación de la ciberseguridad. Asimismo, mencionó que la concientización a los líderes sobre la ciberseguridad, traerá beneficios a las entidades financieras, donde se puedan establecer marcos de riesgos de ciberseguridad a nivel sistemático, para asegurar los derechos y la confidencialidad de información de los cibernautas.

Asimismo, Vosikas (2021), en su investigación denominada "Cybersecurity in Internet of Medical Things. Risks and Challenges", de la universidad de ciencias aplicadas de XAMK, Finlandia, como objetivo determinó la exposición que presenta el internet de las cosas en los dispositivos IoMT, que vienen a ser conjunto de dispositivos y aplicaciones médicas que se interconectan con los sistemas TI. Asimismo, presentó una investigación cuantitativa - no experimental, se utilizaron entrevistas semiestructuradas y cuestionarios. En las conclusiones indicó que existen amenazas externas como los ataques de ransomware y buzz, que constituyen una amenaza en las tecnologías 5G, así también carece de una adecuada regulación y vigilancia de accesos a los dispositivos IoMT. Por lo que se planteó la implementación de buenas practica de TI y un plan de ciberseguridad.

Igualmente, Xiaoyan (2020), en su investigación denominada “Diseño de un sistema de gestión de la seguridad de la información en una empresa de recursos humanos”, en la Universidad de Alcalá, España. Como objetivo estableció la ejecución de un sistema de TI para el área de RRHH de una organización, basándose en el estándar de seguridad de buenas prácticas ISO 27001:2013; determinó una investigación cuantitativa de diseño no experimental. Con respecto a las conclusiones mencionó que el nivel de cumplimiento es de 48% posterior a la implementación de políticas de seguridad con el ISO 27001, esto debido a la falta de mecanismo de supervisión por la alta dirección. Asimismo, se consideró como baja el grado de cumplimiento de la política implementada en la organización.

De la misma forma, Avellán y Zambrano (2019), en su investigación denominada “Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí”, realizado en la Escuela Superior Politécnica Agropecuaria de Manabí, Ecuador. Como objetivo determinaron el estado de desempeño de la ciberseguridad mediante el ISO 27032-2012, a fin de establecer mecanismo para minimizar vulnerabilidades y/o amenazas que tienen los sistemas propios de la institución educativa; para ello, se aplicó una investigación cuantitativa. Como conclusiones destacaron la evaluación e identificación de riesgos con la matriz de análisis modal que denominaron AMFE; asimismo, precisaron que existe un riesgo crítico en los diferentes dominios de seguridad de las plataformas de sistemas que dispone la institución, cuyos resultados de vulnerabilidad se obtuvieron: 50% de nivel crítico en seguridad de información, 7.14% de nivel crítico en seguridad de las App y 12.5% en seguridad en redes. Asimismo, establecieron un plan de acción para mitigar riesgos.

Finalmente, Rajamäki (2021), en su investigación denominada “Industrial control systems’ integrations to Operation Technology and Information Technology Security Operation Center”, realizado en la Universidad de Ciencias aplicadas de XAMK, Finlandia, cuyo objetivo fue, determinar los requisitos para proporcionar supervisión de seguridad gestionada en TI, para ello realizó la integración de un sistemas de

control industrial y como fuente de información proveniente de tecnología operativa, sistema de información para eventos de seguridad - SIEM y el Centro de Operaciones de Seguridad – SOC; los cuales sirvieron para mantener y poner en ejecución un sistema de registros y operación de TI. Utilizó una investigación cuantitativa del tipo no experimental. Con respecto a las conclusiones, mencionó que las capacidades de detección de amenazas y riesgos del sistema control ICS, requieren soporte con nuevos controles de políticas para la tecnología operativa. Además, la ciberseguridad y las habilidades TI, son necesarias para trabajar con la gestión de riesgos de ICS.

Por otro lado, en el ámbito nacional, Mendoza y Vega (2019), en su investigación denominada “Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la Empresa SISC”, realizado en Universidad del Pacifico, como objetivo principal determinaron la identificación de brechas aplicados a la ciberseguridad, para determinar respuestas a eventos que se susciten ante un ciberataque; asimismo, establecieron los controles para su implementación en la organización, aplicando el desarrollado con el marco NIST; utilizaron la metodología de investigación cualitativa, de tipo exploratorio. Como conclusiones, precisaron que los principales riesgos en la empresa SISC, es la poca capacidad de respuesta ante la presencia del malware, por falta de tratamiento de políticas y procedimientos para su acción inmediata. Además, se buscó proteger y detectar posibles incidentes de ciberseguridad con herramientas poco efectivas, para ello se estableció el marco NIST para brindar un análisis y evaluación de riesgos en la organización.

Asimismo, Cruzado y Rodríguez (2022), en su investigación denominada “Marco de referencia “HOGO” para ciberseguridad en Pymes basado en ISO 27002 y 27032” realizado en la Universidad Peruana Unión, cuyo objetivo principal fue, minimizar los posibles riesgos de ciberseguridad que afectan a las Pymes, las cuales son contextualizadas con la integración del ISO 27002 y el ISO 27032 para mantener y brindar mayor seguridad en las transacciones online, transferencias de información financiera, buena imagen frente a los clientes y proveedores de las Pymes. Para

ello, se tomó en consideración a las pymes que cuenten entre 10 y 250 colaboradores. Se estableció una investigación de diseño no experimental, del tipo aplicada. Donde se comprobó que, la implementación del modelo de ciberseguridad presenta una brecha de 25% de incumplimiento de los controles aplicados. Asimismo, los controles de seguridad implementadas en las pymes, brindarán mayor seguridad en las redes de internet, información e infraestructura crítica.

Igualmente, Salinas (2020), en su investigación denominada "Modelo de ciberseguridad para cajas municipales en tiempos de transformación digital – un nuevo enfoque", realizado en Universidad Privada del Norte, propone un plan piloto de ciberseguridad enfocado en la transformación digital para las cajas municipales, donde puede existir una integración de plataformas tecnológicas y una información protegida para los servicios financieros que brindan las cajas municipales en las regiones y capitales de la nación. En relación a la investigación es de un diseño no experimental, cuyo estudio es descriptivo. Como conclusión, se implementó un nuevo diseño de arquitectura para la ciberseguridad, aplicando 20 controles enfocados en la seguridad y protección de información. Asimismo, se desarrolló un marco NIST para gestión de riesgos de los servicios financieros de las cajas municipales.

De la misma forma, Manrique (2022) en su investigación denominada "Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público" realizada en la Universidad Cesar Vallejo; determinó como objetivo realizar una guía de ciberseguridad para optimizar en la gestión de TI, aplicando controles de seguridad y mecanismos de análisis de riesgo con el ISO 27032, utilizó un diseño de investigación - acción y de tipo aplicada. De la misma forma, utilizó la entrevista semiestructurada como técnica para seleccionar información en un instituto superior; donde determinó que una implementación de ciberseguridad optimizará eficientemente en la seguridad del ciberespacio y disminuirá los peligros de los activos de la organización a través de la aplicación de

un plan de ciberseguridad, que servirá para optimizar los procesos con controles y políticas en la red de campus de la institución.

Finalmente, Ormachea (2019), en su investigación denominada “Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional”, realizado en Centro de Altos Estudios Nacionales - CAEN, determinó como objetivo establecer estrategias de ciberseguridad para el desarrollo de fortalecimiento en seguridad nacional en el Perú, esto a fin de mejorar las brechas que existe frente a las amenazas del ciberespacio en el estado peruano. Como metodología aplicó un diseño no experimental, tipo descriptivo; entre sus conclusiones refirió que, las estrategias conjuntas de ciberseguridad serán más eficientes con la implantación de políticas de seguridad a nivel nacional; además, con la identificación de las limitaciones y brechas que se tienen para el desarrollo, evaluación y actualización de estrategias de ciberseguridad, permitirá reforzar convenios internacionales en materia de ciberseguridad.

Por otro lado, esta investigación se respaldó con las teorías enunciadas a continuación: La Teoría General de Sistemas - TGS, establecido por Ludwig Von Bertalanffy. En relación a ello Maldonado (2017), menciona que la TGS está conformada por métodos para facilitar una visión general del universo, en términos sencillos, permite una dinámica en la generación de ideas. Asimismo, Sagasti y Mitroff (1973) y Kish et al. (2021), mencionan que un sistema se tiene que analizar en forma holística, donde se integre todos los componentes y esta conllevará a una interrelación propia del sistema. Por su parte, Seising (2010), menciona que TGS, es una multidisciplina de sistemas teológicos y epistemológicos que busca generar una retroalimentación continua que asegure la perdurabilidad de los procesos integrantes a razón de la homeostasis y finalmente, Domínguez y López (2019), mencionaron que un sistema es una interdependencia o interrelación de diversos elementos que buscan un determinado propósito en un bien común.

De manera similar, se tiene la teoría de restricciones - TOC, establecido por Elyahu Goldratt, en relación a ello, Hernández et al. (2020), manifiestan que la TOC, está basado en un pensamiento sistemático que aborda la identificación de restricciones para aumentar la productividad y mejorar los objetivos. Asimismo, Penagos et al. (2012), mencionan que la teoría de restricciones son elementos de apoyo a la gerencia y esto conllevará a un buen manejo de procesos en la organización con parámetros de aplicación y gestión de manera personalizada. De la misma forma, Horna (2020) define que un TOC, es una restricción optimizada de los procesos del negocio que permitirá determinar una mezcla óptima de producción, cuyo objetivo será generar mayor utilidad y la fluidez de información para una adecuada gestión y la toma de decisiones. Concordante a ello, Marín (2013) y Jiang y Wu (2013), indican que la teoría de restricciones permite administrar de manera efectiva las operaciones de producción enfocados para detectar, definir capacidad y considerar la variabilidad de elementos que componen un sistema.

De manera similar, se tiene las definiciones de la variable independiente denominada ciberseguridad, Reta et al. (2019), menciona que la ciberseguridad es un conjunto de acciones ejecutadas para mitigar los riesgos en el ciberespacio, a fin de pronosticar la probabilidad de un ciberataque; asimismo, Carrillo et al. (2020), mencionan que la ciberseguridad es un conjunto de directrices, políticas y métodos para la gestión de riesgos que se usan para resguardar los activos de una organización y la información privada de los usuarios de un entorno de ciberespacio. Por otro lado, Cornejo (2019), define que la ciberseguridad es un conjunto de métodos que persigue la protección integral de la información que se encuentra en el ciberespacio. De la misma forma, Romero (2018), indica que la ciberseguridad es está compuesto por políticas y directrices con métodos de gestión de riesgos que se utilizan para proteger la información almacenada en ciberentorno. Finalmente, tenemos a Moreno et al. (2020), donde mencionan que la ciberseguridad en la actualidad, son de alta prioridad para salvaguardar los derechos de privacidad de información de los ciudadanos en un ámbito digital, cuya base fundamental es incrementar la confianza de los usuarios en las tecnologías digitales, donde a través

del estudio de la madurez de la ciberseguridad, desarrollado en los países de Latinoamérica, definieron las siguientes dimensiones: Estrategias de seguridad, Protección de infraestructura crítica y Control técnico de seguridad.

De esta forma, se procederá a definir las dimensiones de la variable independiente ciberseguridad mencionados en el párrafo anterior. Como primera dimensión se tiene estrategias de seguridad, donde Aguilar (2019), define que las estrategias de seguridad permitirán avances tecnológicos para consolidar una política de ciberseguridad, que formarán parte de una tendencia para prevenir posibles ciberamenazas. Asimismo, Leyva (2021), menciona que una estrategia de seguridad busca responder las nuevas necesidades de seguridad y confianza en el ciberespacio, las cuales deberán establecerse con los principios y políticas nacionales. Por su parte, Díaz (2021), refiere que una estrategia de seguridad busca variables de análisis para asignar prioridades y recursos, de manera que los esfuerzos posteriores estén alineados a las estrategias de prevención y elaboración de un plan para la ciberseguridad. Por otro lado, Hernández (2022), define que todo proceso de cambio tecnológico, traerá consigo mayor nivel de conocimiento y confianza en el entorno digital, para ello se debe implementar estrategias de seguridad que ayuden a profundizar el uso de servicios digitales y finalmente Aguilar (2021), menciona que los ejes de un marco legal para la ciberseguridad y el cibercrimen, deben estar establecidos como estrategias de seguridad vinculados a los objetivos principales de la seguridad nacional, securitización del internet y la ciberseguridad.

Asimismo, se define la segunda dimensión de la variable ciberseguridad, protección de infraestructura crítica, para ello citamos a López et al. (2021), donde indican que la protección de una infraestructura crítica es clave para una adecuada estrategia nacional de ciberseguridad, la cual debe ser explorado para determinar directrices y dicho desarrollo que involucre a la sociedad como medida de seguridad de entorno. Asimismo, Sánchez, A. (2020) menciona que son marcos o líneas de acción estratégicas para garantizar la protección de los servicios de tecnologías de

información como los sistemas físicos y virtuales que facilitan servicios esenciales a nivel social, económico, político y medioambiental. Por otro lado, Zuluaga (2020), menciona que la protección de infraestructura crítica presta un servicio esencial y fundamental en nuestra sociedad dada la presencia del ciberespacio en nuestras actividades cotidianas, para ello se tiene que establecer un plan de protección y defensa a nivel de ciberseguridad. De la misma forma, Kulugh et al. (2022), mencionan que la protección de una infraestructura critica apoya a la sociedad moderna a enfrentar las amenazas inherentes a los ciberataques, que pueden tener un impacto debilitante si no se prepara para asegurar la disponibilidad continua de los servicios tecnológicos y finalmente Malatji et al. (2022), definen que una protección de infraestructura crítica responde a una dirección encaminada a la eficiencia de los servicios de TI, que se materializan con la transformación digital y la interoperabilidad de personas, procesos y datos. Por ello es necesario identificar y fortalecer las capacidades de respuesta ante un ciberataque.

De la misma forma, se define la tercera dimensión de la variable ciberseguridad control técnico la seguridad, para ello citamos a Sabillón y Cano (2019), que definen que un control técnico de seguridad permitirá materializar un programa de ciberseguridad y desarrollar un marco de trabajo para realizar auditorías y concientizar en seguridad de la información basado en los objetivos de la empresa. Asimismo, Criollo et al. (2020) mencionan que, establecer un control técnico de seguridad permitirá a la organización centralizar procesos, personas y tecnología con el propósito de brindar capacidades de mejora para prevenir, detectar y asegurar las incidencias de ciberseguridad. De igual forma. Gutiérrez (2020) menciona que establecer los controles de seguridad permitirá a las organizaciones a centrarse y mejorar el despliegue de estándares de seguridad cibernética a fin de aminorar los ciberataques. Igualmente, Jara y Jorquera (2021) indican que, como principio de control de seguridad, es un instrumento para lograr un adecuado funcionamiento de servicios tecnológicos en las organizaciones con la finalidad de implementar, gestionar y realizar seguimiento de políticas de privacidad y protección ante un ciberataque, y finalmente Zekos (2022) menciona que el control de

seguridad es un programa de ciberseguridad para proteger la información valiosa de manera confidencial y asegurar la evaluación efectiva de ciberseguridad.

En relación a la definición de la variable dependiente denominada gestión de tecnologías de información, Díaz et al. (2022), mencionan que la gestión de TI, es el grado de sinergia que tiene la gerencia o área de TI, para desarrollar una planificación de TI alineados a las estrategias de servicio, a fin de optimizar los procesos, generar valor y capacidad de respuesta a las incidencias a nivel operativo y gerencial. Asimismo, Bermeo et al. (2020), consideran que la gestión de TI, son técnicas de apoyo para la realización y ejecución de actividades de interacción con las TIC, cuyas herramientas permiten una transición para la mejora en los procesos relacionados con la informática, internet e infraestructura tecnológica. De igual forma, Villarreal et al. (2021), definen que la gestión de TI es el proceso de transformación de los activos de información a través de la creación de servicios innovadores o la implementación de políticas de TI, para lograr una vista holística de un entorno gestionado. Igualmente, Casanova y Calderón (2019), indican que gestión de TI es un proceso de transformación estratégica para mejorar los procesos de negocio, reducir costos de operación e innovación, garantizando el cumplimiento de objetivos como organización. Finalmente, Sánchez y Valles (2021) mencionan que, el enfoque de gestión de TI, es un marco de mejoras prácticas de servicio de TI, que detecta cuellos de botella y genera valor agregado en los servicios de TI, de esta manera se establecen las siguientes dimensiones: Estrategia de servicio, operación de servicio y continuidad de servicio.

De igual forma, se procederá a definir las dimensiones de la variable dependiente gestión de TI, mencionados en el párrafo anterior. Como primera dimensión se tiene estrategia de servicio, definido por Vásquez et al. (2019), una estrategia de servicio en el marco de buenas prácticas, determina la calidad de servicio con la que el área de TI ofrece a sus clientes – usuarios para gestionar los recursos de TI, con el objetivo de establecer planes de mejora continua de la organización. Asimismo, Quintero y Peña (2017), indican que la estrategia de servicio es un componente

fundamental para proveer la gestión de TI, donde pueda incluir políticas y marcos de trabajo segmentados por proceso para hacer efectiva su gestión e implementación. De igual manera, Casanova y Calderón (2020), definen que la estrategia de servicio de TI, es un conjunto de directrices que permiten una óptima planificación de las necesidades de la organización, contextualizadas en políticas automatizables y no automatizables, las cuales son enfocadas para la estimación de impacto en los servicios de TI. Igualmente, Galeano y González (2021), definen que una estrategia de servicio de TI, está enfocado en la necesidad y demanda de los servicios de tecnología de información; de tal manera, se deben alinear a los indicadores de gestión organizacional, para asegurar la continuidad de los servicios y mitigar riesgos en el ciclo de operación. Finalmente, Meléndez y Dávila (2018), mencionan que la estrategia de servicio es determinar un conjunto de directrices para cada ciclo de proceso de gestión de TI, para planificar, ejecutar y revisar la necesidad del usuario final.

Asimismo, se define la segunda dimensión de la variable gestión de TI operación de servicio, Cuesta (2020), menciona que la operación de servicio es una práctica de gestión de TI, basado en la generación de valor y control de eventos críticos en relación a los temas de prestación de servicio de tecnología la cual permitirá implementar un modelo adecuado para la gestión de servicios a nivel gerencial. Asimismo, Astudillo y Encalada (2019), indican que, el proceso de operación de servicio, consiste en que los servicios TI cumplan de manera eficiente todos los requerimientos de los usuarios finales, cuya ejecución debe desarrollarse con una planificación y asistencia en el proceso de transición. De manera similar, Muhamet et al. (2018), definen que la operación de servicio contribuye al desarrollo y ejecución del proceso de gestión de TI, a través de subprocesos que monitorean y gestionan los problemas que se suscitan en los servicios de operación de tecnologías de información. En relación a ello, Tining (2019), indica que la operación de servicio es parte del proceso de mejora y eficiencia de calidad de los servicios, que apoya el nivel de preparación del diseño y mejora en la madurez de los servicios de TI y para finalizar, Pérez et al. (2021), mencionan que la operación de servicio

de gestión de TI, son mecanismos de gobernanza y deben garantizar que los servicios de TI cumplan con los procesos comerciales y la finalidad de la organización. Para ello, es necesario que los procesos se correlacionen en los distintos niveles de estructura, procedimiento y actividades a desarrollarse con un fin común.

De la misma forma, se define la tercera dimensión de la variable gestión de TI denominada continuidad de servicio, Moudoubah et al. (2021), indican que la continuidad de servicio proporciona un marco integral de los servicios de TI y puede mejorar el rendimiento de las organizaciones en la dirección y uso adecuado de recursos implementados en la gestión de TI, a través de métodos para su administración y regulación sobre el uso de los sistemas de información. Asimismo, Piñuela y Quito (2020), consideran que la continuidad de servicio es un proceso fundamental para alcanzar un alto nivel de eficiencia y mejorar la productividad en la organización. De manera similar, Andrade (2021), menciona que la continuidad de servicio es un método gerencial que permite realizar una adecuada gestión de servicios de TI, cuyo objetivo es mejorar los resultados esperados y en este proceso se debe realizar una planificación, evaluación y generar controles correctivos. En relación a ello, Nina y Vera (2021), mencionan que la continuidad de servicio busca mejorar las operaciones de los servicios de TI, con prácticas estandarizadas para optimizar el flujo de procesos operativos, para que estos sean más productivos y eficientes de acuerdo a los objetivos y prioridades de un líder de negocio, y para finalizar, Gómez y Valencia (2021), mencionan que una continuidad de servicio permite formular una planificación acorde a la situación para optimizar procesos que conllevan mayor tiempo de respuesta y determinar controles con parámetros de medición ante cualquier riesgo de los servicios de TI.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

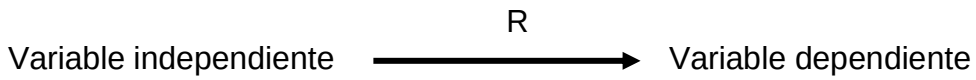
La investigación planteada es tipo básica. Baena (2017), menciona que la investigación fundamental o básica, es la aplicación de conocimientos a través métodos científicos a un problema específico para obtener una información relevante. Asimismo, Hernández y Mendoza (2018), menciona que la aplicación de un estudio básico de las variables tiene una relación directa para brindar una respuesta, a fin de describir cualidades de los elementos de estudio.

Diseño de investigación

La investigación planteada es de diseño no experimental, Hernández y Mendoza (2018), conceptualizan que una investigación no experimental, describe variables correlacionadas que no tienen alteración y la recopilación de datos se ejecuta en un periodo determinado por el investigador. Asimismo, la investigación se clasificó de estudio transversal con un nivel correlacional - causal, debido a que se establecen una correlación de dos variables.

A nivel correlacional-causal, se pretende un estudio de correspondencia de las variables ciberseguridad y gestión de TI, representado de la siguiente manera:

Esquema:



Dónde:

Variable independiente: Ciberseguridad

R: Relación causal

Variable dependiente: Gestión de tecnologías de información.

3.2. Variables y Operacionalización

Variable independiente: Ciberseguridad

Ciberseguridad es una variable cualitativa de tipo ordinal. Según Ñaupas et al. (2018), esta variable señala cualidades que se pueden observar y medir de forma numérica, debido a que tiene jerarquía de nivel y puede expresar un orden.

Definición conceptual de la variable ciberseguridad

Moreno et al. (2020), menciona que la ciberseguridad, es conjunto de procedimientos y herramientas que se determinan mediante las siguientes dimensiones: Estrategias de seguridad, protección de infraestructura crítica y control técnico de seguridad, para salvaguardar la información y la privacidad del mismo en un ambiente digital o ciberespacio.

Definición operacional de la variable ciberseguridad

Ciberseguridad, se consideró operacionalizar en tres dimensiones: Estrategias de seguridad, protección de infraestructura crítica y control técnico de seguridad; asimismo, la información obtenida será analizada mediante escala Likert en 5 valores: Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5); de manera similar se aplicó mediante 3 niveles: No óptimo con un rango de 18 a 42, Moderado con un rango de 43 a 67 y el nivel Óptimo con un rango de 68 a 90, ver Anexo 2.

Variable dependiente: Gestión de tecnologías de información

Gestión de TI considerada una variable cualitativa de tipo ordinal. Según Ñaupas et al. (2018), las características de esta variable señalan cualidades de tipo categórico – ordinal, porque se pueden observar y medir de utilizando algún tipo de sucesión.

Definición conceptual de la variable gestión de tecnologías de información

Sánchez y Valles (2021), mencionan que el enfoque de gestión de TI en un marco de buenas prácticas de servicio, genera un valor agregado en todos los procesos y

servicios que se brindan y se ejecuten con mayor eficiencia. De este modo se establecen mediante las dimensiones de estrategia de servicio, operación de servicio y continuidad, esto con la finalidad de detectar cuellos de botella en los servicios de gestión de TI.

Definición operacional de la variable gestión de tecnologías de información

Gestión de TI se operacionaliza en tres dimensiones: Estrategia de servicio, Operación de servicio y Continuidad de servicio; asimismo, la información obtenida será analizada mediante escala Likert en 5 valores: Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5); de manera similar se aplicó mediante 3 niveles: Malo con un rango de 18 a 42, Regular con un rango de 43 a 67 y Bueno con un rango de 68 a 90, ver Anexo 2.

3.3. Población, muestra y muestreo

Población

Ñaupas et al. (2018), una población está definida como una totalidad de elementos de las cuales tienen una determinada característica para un caso de estudio. En ese contexto, en la investigación se consideró una población de 321 servidores públicos de una institución aseguradora de salud de los distritos de Lima y Callao. Los cuales se detallan en tabla siguiente:

Tabla 1

Caracterización de la población

Población	Cantidad
Gerencia Macro Regional Centro Medio	35
Sede Central – Lima	215
UDR Callao	12
UDR Lima Metropolitana Centro	9
UDR Lima Metropolitana Este	17
UDR Lima Metropolitana Norte	11
UDR Lima Metropolitana Sur	11
UDR Lima Región	11
Total	321

Muestra

Según, Hernández y Mendoza (2018), una muestra viene a ser un subgrupo o cierto porcentaje de un total de la población, en la cual se realiza para elegir los datos relevantes para un estudio en particular. Al respecto, con el aplicativo de análisis estadístico Decision Analyst STATS v.2.0, se comprobó la dimensión de la muestra registrando en el aplicativo la población de 321 servidores, con una confianza (95%) y margen (5%). Obteniéndose como resultado una muestra de 175 servidores de una institución aseguradora de salud, las cuales indicaremos:

Tabla 2

Caracterización de la muestra

Población	Cantidad
Gerencia Macro Regional Centro Medio	18
Sede Central – Lima	100
UDR Callao	12
UDR Lima Metropolitana Centro	7
UDR Lima Metropolitana Este	11
UDR Lima Metropolitana Norte	8
UDR Lima Metropolitana Sur	9
UDR Lima Región	10
Total	175

Muestreo

En la investigación se determinó realizar una muestra probabilística aleatorio simple, Hernández y Mendoza (2018), menciona que un muestreo aleatorio simple, es una técnica en la cual, todos los elementos de estudio tienen la misma probabilidad de selección en toda la muestra. En ese contexto, se considera toda población (servidores activos de la IAFAS), las cuales serán seleccionadas con igual probabilidad de manera aleatoria con la herramienta de hoja de cálculo Excel.

Unidad de Análisis

Para la investigación planteada, se tomará en cuenta a los servidores públicos de la IAFAS de las sedes a nivel de los distritos de Lima y Callao, asimismo mencionar que la unidad análisis presenta mismas características en un ámbito laboral específico. Esto según, definición de Hernández y Mendoza (2018), donde menciona que la unid. de análisis básicamente representa una fracción de la población total.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

En el proceso de recopilación de datos de información, se utilizó técnica de encuesta. En ese aspecto, Hernández y Mendoza (2018), señala una encuesta ayuda al investigador como una técnica para recopilar datos de información con mayor rapidez en un periodo corto, para realizar un análisis e interpretación del mismo.

Instrumentos de recolección de datos

En la investigación, se consideró la utilización de instrumento para la recopilación de datos un cuestionario en línea. En ese aspecto, Hernández y Mendoza (2018), menciona que un cuestionario puede utilizar para obtener información de manera sistemática a través de preguntas correlacionadas con el objeto de la investigación. Por esta razón se establece en escala de Likert la valoración de los argumentos de medición de cada variable y su respectiva dimensión. Las cuales indicaremos en la tabla 3:

Tabla 3

Ficha técnica del instrumento de recolección de datos

Nombre del Instrumento:	Cuestionario para los servidores de una IAFAS, Lima 2022.
Autor	Ampelio Juan de Mata Mallqui Mallqui
Año:	2022
Tipo de Instrumento:	Cuestionario
Objetivo:	Determinar la incidencia de la ciberseguridad en la gestión de TI en una IAFAS, Lima 2022.
Población:	321 servidores públicos de una institución aseguradora de salud a nivel de Lima y Callao
Número de Items:	36 preguntas
Aplicación:	En línea
Tiempo de administración:	10 minutos

Nombre del Instrumento:	Cuestionario para los servidores de una IAFAS, Lima 2022.
Normas de aplicación:	El servidor público encuestado deberá elegir una opción de acuerdo a la realidad institucional y que en su opinión considere correcto.
Escala:	Escala de Likert (1) Totalmente en desacuerdo (2) Desacuerdo (3) Ni en descuerdo, ni de acuerdo (4) De acuerdo (5) Totalmente de acuerdo

Niveles y rangos:

Variable: Ciberseguridad

Nivel	Valor	Rango
No optimo	1	18-42
Moderado	2	43-67
Optimo	3	68-90

Variable: Gestión de Tecnologías de Información

Nivel	Valor	Rango
Malo	1	18-42
Regular	2	43-67
Bueno	3	68-90

Validez

Se consideró la validez del instrumento a través de juicio de experto, que determinaron pertinencia, claridad y relevancia en las preguntas consideradas en el cuestionario (Ver Anexo 4). Al respecto, Hernández y Mendoza (2018), mencionan validez de un instrumento es una capacidad para recopilar datos de información con características relevantes en el ámbito de estudio. En ese sentido, se consideró a los siguientes profesionales en el campo de ingeniería.

Tabla 4

Validación del instrumento de recolección de datos

DNI	Grado Académico, Apellidos y Nombres	Institución donde labora	Calificación
09656793	Dr. Lezama Gonzales, Pedro Martin	Universidad Cesar Vallejo - UCV	Aplicable
42097456	Dr. Acuña Benites, Marlon Frank	Universidad Cesar Vallejo - UCV	Aplicable
42385497	Mgt. Quiroz Angulo, Christian Janderson	Ministerio del Ambiente - MINAM	Aplicable

Confiabilidad

Hernández y Mendoza (2018), menciona que la confiabilidad es la condición en la que el instrumento genera resultados coherentes y consistentes. En ese contexto, en la investigación se utilizó Alfa de Cronbach que se ejecutó a través del aplicativo SPSS Statistics v25; la cual ha permitido determinar que el instrumento aplicado recopilación de información en líneas es confiable.

Para el análisis de confiabilidad se desarrolló un piloto con 20 encuestados, obteniéndose 0.929 de Alfa de Cronbach y para la prueba general con 175 encuestas se obtuvo de 0.971 de Alfa de Cronbach. Al respecto, Tuapanta et al. (2017), describen la clasificación de niveles de fiabilidad de los resultados de alfa de Cronbach: Deficiente [0-0.3], Regular [0.3-0.5], Bueno [0.5-0.7], Muy Bueno [0.7-0.9], Excelente [0.9-1]. Según las premisas, se determina que el instrumento de recolección de datos, presenta un excelente nivel de confiablidad; cuyos resultados se muestran a continuación:

Tabla 5

Resultado del análisis de confiabilidad a través del Alfa de Cronbach

Tipo de Aplicación	N° de encuestas	N° de elementos	Alfa de Cronbach
Piloto	20	36	0.929
General	175	36	0.971

3.5. Procedimientos

Para el proceso de selección de datos de información, se generó un instrumento de encuesta para cada variable con sus respectivas dimensiones. Donde el instrumento ha sido validado por 03 juicios de expertos que determinaron la validez y confiabilidad del mismo; posteriormente se ejecutó un piloto con 20 encuestas obteniendo un valor de 0.929 de Alfa de Cronbach. Luego se consideró el total de la muestra establecida de 175 encuestas, obteniendo un valor de 0.971 de Alfa de Cronbach. Asimismo, se realizó la generación de la información en hoja de cálculo

Excel y finalmente con los resultados obtenidos a través del aplicativo SPSS Statistics v2, se procedió con la ejecución del análisis descriptivo e inferencial.

3.6. Método de análisis de datos

Para el análisis de información estadística, se desarrolló en el aplicativo SPSS Statistics v25, con todos los datos recolectados a través del cuestionario en línea, la cual se ha realizado encuestas a los servidores públicos de la IAFAS con una muestra especifica objetivo de la investigación.

Al respecto, para el análisis descriptivo se desarrolló con tablas cruzadas e histogramas, cuyos resultados sirvieron para interpretación de cada uno de las dimensiones e indicadores de la investigación.

Para el análisis inferencial se desarrolló con pruebas paramétrico y para análisis estadístico coeficiente de regresión ordinal, de esta manera se tiene el grado correlacional que existen entre las variables de ciberseguridad y la gestión de TI.

3.7. Aspectos éticos

La investigación se desarrolló conforme a los estándares y principios éticos de la Universidad César Vallejo establecidos con la Resolución de Consejo Universitario N°0340-2021/UCV.

Principio de propiedad intelectual: En la investigación se respeta el derecho del autor, establecido con el DL N° 822 y publicado el 24-04-1996.

Principio de autonomía: Los participantes en la investigación tiene capacidad de elección para retirarse en cualquier momento que lo requieran.

Principio de transparencia: Con la publicación de la investigación ha de ser posible su replicación de la metodología y la verificación de la validez de resultados.

IV. RESULTADOS

Análisis descriptivo

Análisis descriptivo de la variable ciberseguridad y la variable gestión de tecnologías de información

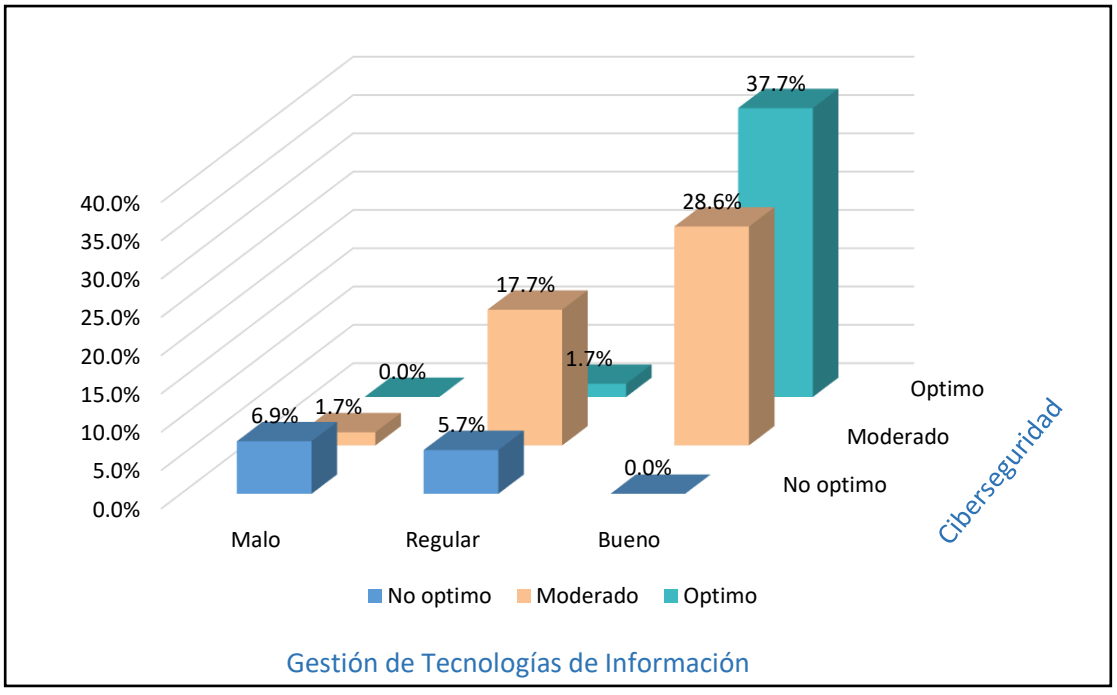
Tabla 6

*Tabla cruzada V1 – Ciberseguridad * V2 - Gestión de Tecnologías de Información*

		V2 - Gestión de Tecnologías de Información			
		Malo	Regular	Bueno	Total
V1 - Ciberseguridad	No óptimo	12 (6.9%)	10 (5.7%)	0 (0.0%)	12 (12.6%)
	Moderado	3 (1.7%)	31 (17.7%)	28 (28.6%)	84 (48.0%)
	Óptimo	0 (0.0%)	3 (1.7%)	66 (37.7%)	69 (39.4%)
	Total	15 (8.6%)	44 (25.1%)	116 (66.3%)	175 (100,0%)

Figura 1

*Histograma V1 – Ciberseguridad * V2 - Gestión de Tecnologías de Información*



En la tabla 6 y figura 1, se puede apreciar un índice de mayor aceptación en las respuestas con nivel “Óptimo” en la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 37.7% equivalente a 66 respuestas de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS. Asimismo, se tienen un índice intermedio de aceptación en las respuestas de nivel “Moderado” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 28.6% que es equivalente a 50 respuesta del total de 175 cuestionarios registrados y finalmente, con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0% es decir, con ninguna respuesta registrada en el cuestionario.

Análisis descriptivo de la dimensión estrategias de seguridad de la variable ciberseguridad y la variable gestión de tecnologías de información

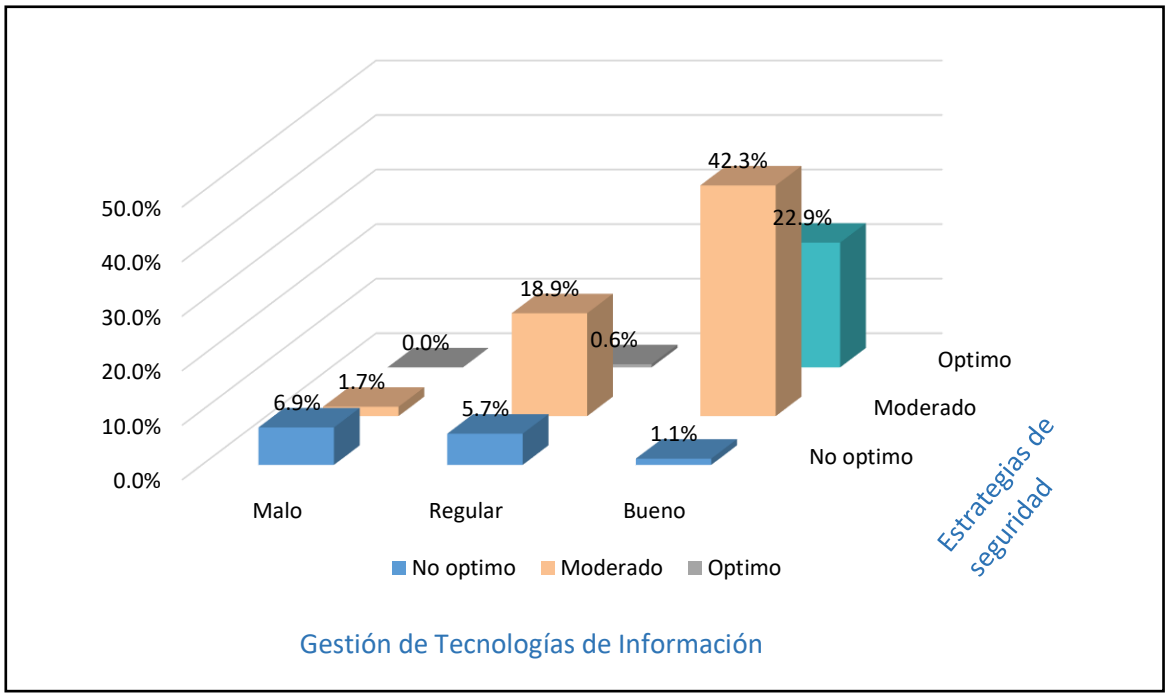
Tabla 7

*Tabla cruzada D1V1 - Estrategias de seguridad * V2 - Gestión de Tecnologías de Información*

		V2 - Gestión de Tecnologías de Información			
		Malo	Regular	Bueno	Total
D1V1 - Estrategias de seguridad	No óptimo	12 (6.9%)	10 (5.7%)	2 (1.1%)	24 (13.7%)
	Moderado	3 (1.7%)	33 (18.9%)	74 (42.3%)	110 (62.9%)
	Óptimo	0 (0.0%)	1 (0.6%)	40 (22.9%)	41 (23.4%)
	Total	15 (8.6%)	44 (25.1%)	116 (66.3%)	175 (100,0%)

Figura 2

*Histograma D1V1 - Estrategias de seguridad * V2 - Gestión de Tecnologías de Información*



En la tabla 7 y figura 2, se puede apreciar un índice de mayor aceptación en las respuestas con nivel “Moderado” en la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 42.3% equivalente a 74 respuestas de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS. Asimismo, se tienen un índice intermedio de aceptación en las respuestas de nivel “Óptimo” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 22.9% que es equivalente a 40 respuesta del total de 175 cuestionarios registrados y finalmente, con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0% es decir, con ninguna respuesta registrada en el cuestionario.

Análisis descriptivo de la dimensión protección de infraestructura crítica de la variable ciberseguridad y la variable gestión de tecnologías de información

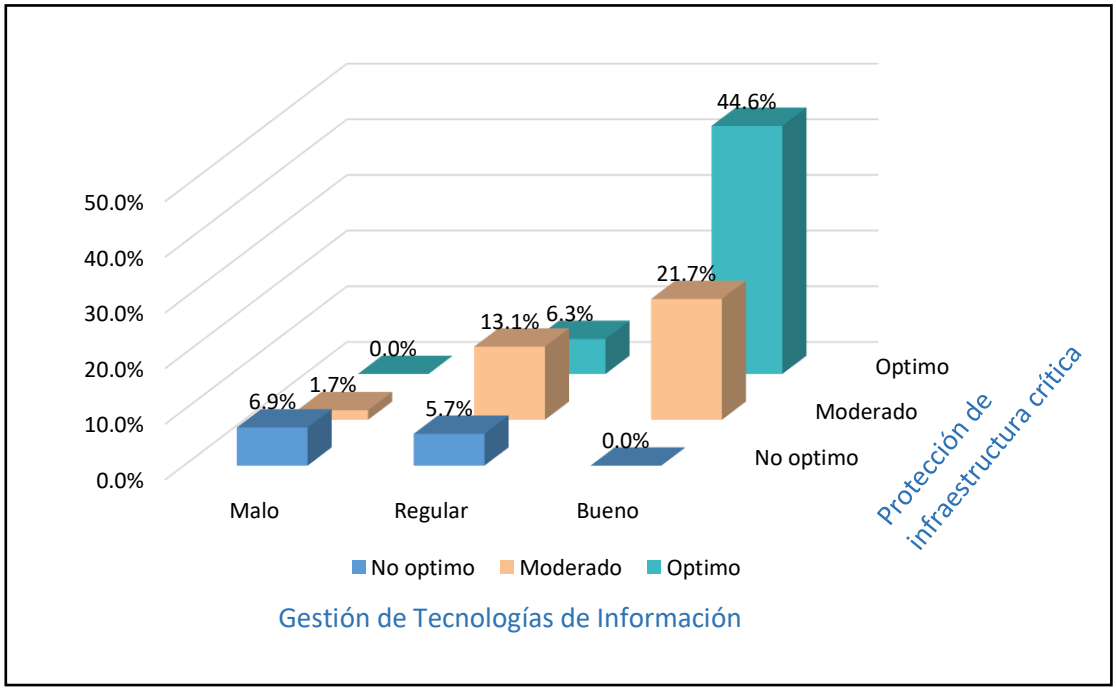
Tabla 8

*Tabla cruzada D2V1 - Protección de infraestructura crítica * V2 - Gestión de Tecnologías de Información*

		V2 - Gestión de Tecnologías de Información			
		Malo	Regular	Bueno	Total
D2V1 - Protección de infraestructura crítica	No óptimo	12 (6.9%)	10 (5.7%)	0 (0.0%)	22 (12.6%)
	Moderado	3 (1.7%)	23 (13.1%)	38 (21.7%)	64 (36.6%)
	Óptimo	0 (0.0%)	11 (6.3%)	78 (44.6%)	89 (50.9%)
	Total	15 (8.6%)	44 (25.1%)	116 (66.3%)	175 (100,0%)

Figura 3

*Histograma D2V1 - Protección de infraestructura crítica * V2 - Gestión de Tecnologías de Información*



En la tabla 8 y figura 3, se puede apreciar un índice de mayor aceptación en las respuestas con nivel “Óptimo” en la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 44.6% equivalente a 78 respuestas de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS. Asimismo, se tienen un índice intermedio de aceptación en las respuestas de nivel “Moderado” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 21.7% que es equivalente a 38 respuesta del total de 175 cuestionarios registrados y finalmente, con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0% es decir, con ninguna respuesta registrada en el cuestionario.

Análisis descriptivo de la dimensión control técnico de seguridad de la variable ciberseguridad y la variable gestión de tecnologías de información

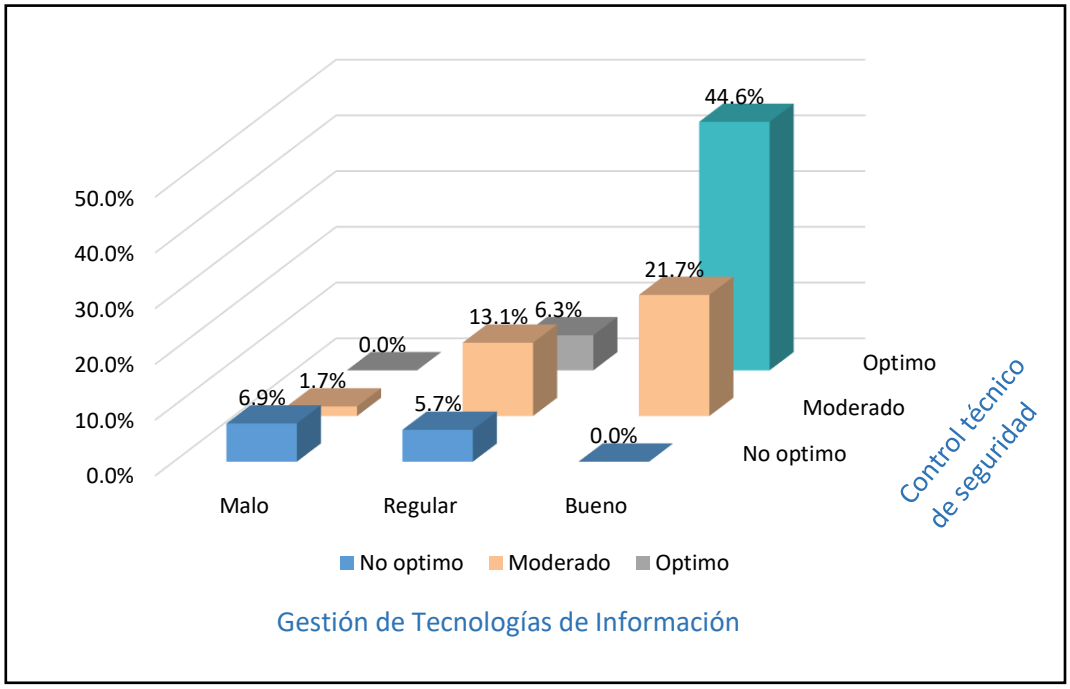
Tabla 9

*Tabla cruzada D3V1 - Control técnico de seguridad * V2 - Gestión de Tecnologías de Información*

		V2 - Gestión de Tecnologías de Información			
		Malo	Regular	Bueno	Total
D3V1 - Control técnico de seguridad	No óptimo	12 (6.9%)	10 (5.7%)	0 (0.0%)	22 (12.6%)
	Moderado	3 (1.7%)	23 (13.1%)	38 (21.7%)	64 (36.6%)
	Óptimo	0 (0.0%)	11 (6.3%)	78 (44.6%)	89 (50.9%)
	Total	15 (8.6%)	44 (25.1%)	116 (66.3%)	175 (100,0%)

Figura 4

*Histograma D3V1 - Control técnico de seguridad * V2 - Gestión de Tecnologías de Información*



En la tabla 9 y figura 4, se puede apreciar un índice de mayor aceptación en las respuestas con nivel “Óptimo” en la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 44.6% equivalente a 78 respuestas de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS. Asimismo, se tienen un índice intermedio de aceptación en las respuestas de nivel “Moderado” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 21.7% que es equivalente a 38 respuesta del total de 175 cuestionarios registrados y finalmente, con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0% es decir, con ninguna respuesta registrada en el cuestionario.

Análisis inferencial

Para el análisis inferencial de la investigación se determinó método paramétrico con análisis estadístico de regresión ordinal; que busca determinar a través de las hipótesis el grado de dependencia correlacional que existe entre las dos variables de estudio. Santabárbara (2019), menciona que, la asociación de la variable independiente y variable depende, son expresadas en forma analítica mediante cálculo estadístico denominado coeficiente de Pearson y que estas, generan una intensidad o intervalo de relación, según los valores mencionados: De 0.00 al 0.09 [No hay correlación de variables], de 0.10 al 0.25 [correlación débil], de 0.25 al 0.49 [correlación moderada], de 0.50 al 0.74 [correlación considerable], de 0.75 al 0.89 [correlación muy fuerte] y finalmente de 0.90 al 1.00 [correlación perfecta].

Prueba de Hipótesis

Prueba de Hipótesis General

Formulación de hipótesis estadística:

H_1: La ciberseguridad incide significativamente en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

H_0: La ciberseguridad no incide significativamente en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 10

Información sobre el ajuste del modelo que explica la incidencia de la variable ciberseguridad en la variable gestión de tecnologías de información.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	116.175			
Final	16.223	99.952	2	0.000

En la tabla 10 se demostró una significancia p=0.000, cuyo resultado es inferior a 0.05; la misma que determina incidencia significativa de la variable ciberseguridad en la variable gestión de TI, cuyo enfoque de análisis y aplicación es en regresión ordinal.

Tabla 11

Bondad de ajuste de la incidencia de la variable ciberseguridad en la variable gestión de tecnologías de información

	Chi-cuadrado	gl	Sig.
Pearson	1.215	2	0.545
Desviación	1.967	2	0.374

En la tabla 11 se comprobó que el Chi-cuadrado de Pearson tiene un valor de 0.545, cuyo resultado es mayor a 0.05, la cual determina como resultados que la información registrada es consistente.

Tabla 12

Pseudo R Cuadrado de la incidencia de la variable ciberseguridad en la variable gestión de tecnologías de información.

Coeficiente R^2	Valor
Cox y Snell	0.435
Nagelkerke	0.537
McFadden	0.344

En la tabla 12, en el análisis de coeficiente de R^2 de Nagelkerke se obtuvo un valor 0.537, cuyo resultado es superior a Cox y Snell y McFadden. Este resultado representa un 53.7 % de incidencia de la ciberseguridad en la gestión de TI. De tal forma, se comprobó que los valores resultantes están de 0.50 al 0.74 que indica una correlación positiva considerable. Por tanto, se considera la hipótesis alterna (H_1).

Tabla 13

Estimaciones de los parámetros de incidencia de la variable ciberseguridad en la variable gestión de tecnologías de información.

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[V2 = 1]	-6,331	0,826	58,742	1	0,000	-7,950	-4,712
	[V2 = 2]	-3,093	0,591	27,406	1	0,000	-4,251	-1,935
Ubicación	[V1=1]	-6,569	0,911	52,008	1	0,000	-8,354	-4,783
	[V1=2]	-2,723	0,631	18,634	1	0,000	-3,960	-1,487

En la tabla 13, se evidenció que existe una representación de -2.723 en la estimación de incidencia de la ciberseguridad en la gestión de TI, con significancia de p=0.000, el cual es inferior a 0.0.5 y que determina que existe incidencia significativa de las dos variables. Asimismo, el coeficiente de estimación Wald es mayor 1. Por tanto, se considera la hipótesis alterna (H_1).

Prueba de Hipótesis específica 1:

Formulación de hipótesis estadística:

H_1: Existe incidencia significativa entre la dimensión estrategias de seguridad de la variable ciberseguridad y la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

H_0: No existe incidencia significativa entre la dimensión estrategias de seguridad de la variable ciberseguridad y la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 14

Información sobre el ajuste del modelo que explica la incidencia de la dimensión estrategias de seguridad de la variable ciberseguridad en la variable la gestión de tecnologías de información.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	189.384			
Final	11.609	177.775	2	0.000

En la tabla 14 se demostró una significancia p=0.000, cuyo resultado es inferior a 0.05; la misma que determina incidencia significativa de la dimensión estrategia de seguridad de la ciberseguridad sobre la gestión de TI, cuyo enfoque de análisis aplica regresión ordinal.

Tabla 15

Bondad de ajuste de la incidencia de la dimensión estrategias de seguridad de la variable ciberseguridad en la variable gestión de tecnologías de información

	Chi-cuadrado	gl	Sig.
Pearson	0.023	2	0.989
Desviación	0.045	2	0.978

En la tabla 15 se comprobó que el Chi-cuadrado de Pearson tiene un valor de 0.989, cuyo resultado es mayor a 0.05, la cual determina como resultado que la información registrada es consistente.

Tabla 16

Pseudo R Cuadrado de la incidencia de la dimensión estrategias de seguridad de la variable ciberseguridad en la variable gestión de tecnologías de información

Coeficiente R^2	Valor
Cox y Snell	0.638
Nagelkerke	0.763
McFadden	0.562

En la tabla 16, análisis de coeficiente de R^2 de Nagelkerke se obtuvo un valor 0.763, cuyo resultado es superior a Cox y Snell y McFadden. Este resultado representa un 76.3% de incidencia de la ciberseguridad en la gestión de TI. De tal forma, se comprobó que los valores resultantes están de 0.75 al 0.89 que indica una correlación positiva muy fuerte. Por tanto, se considera la hipótesis alterna (H_1).

Tabla 17

Estimaciones de los parámetros de incidencia de la dimensión estrategias de seguridad variable ciberseguridad en la variable gestión de tecnologías de información.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[D1V1 = 1]	-8,067	1,173	47,289	1	,000	-10,366	-5,767
	[D1V1 = 2]	-,322	,244	1,745	1	,187	-,800	,156
Ubicación	[V1=1]	-11,111	1,557	50,940	1	,000	-14,162	-8,060
	[V1=2]	-4,763	1,035	21,197	1	,000	-6,791	-2,736

En la tabla 17, se evidenció que existe una representación de -4.763 en la estimación de incidencia de la ciberseguridad en la gestión de TI, con significancia de p=0.000, el cual es inferior a 0.0.5 y que determina que existe incidencia significativa de las dos variables. Asimismo, el coeficiente de estimación Wald es mayor 1. Por tanto, se considera la hipótesis alterna (H_1).

Prueba de Hipótesis específica 2:

Formulación de hipótesis estadística:

H_1: Existe incidencia significativa entre la dimensión protección de infraestructura crítica de la variable ciberseguridad y la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

H_0: No existe incidencia significativa entre la dimensión protección de infraestructura crítica de la variable ciberseguridad y la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 18

Información sobre el ajuste del modelo que explica la incidencia de la dimensión protección de infraestructura critica de la variable ciberseguridad en la variable la gestión de tecnologías de información.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	195.975			
Final	12.118	183.857	2	0.000

En la tabla 18 se demostró una significancia p=0.000, cuyo resultado es inferior a 0.05; la misma que determina incidencia significativa de la dimensión protección de infraestructura crítica de la ciberseguridad sobre la gestión de TI, cuyo enfoque de análisis aplica regresión ordinal

Tabla 19

Bondad de ajuste de la incidencia de la dimensión protección de infraestructura critica de la variable ciberseguridad en la variable gestión de tecnologías de información

	Chi-cuadrado	gl	Sig.
Pearson	0.033	2	0.984
Desviación	0.065	2	0.968

En la tabla 19 se comprobó que el Chi-cuadrado de Pearson tiene un valor de 0.984, cuyo resultado es mayor a 0.05, la cual determina como resultado que la información registrada es consistente.

Tabla 20

Pseudo R Cuadrado de la incidencia de la dimensión protección de infraestructura critica de la variable ciberseguridad en la variable gestión de tecnologías de información

Coeficiente R^2	Valor
Cox y Snell	0.650
Nagelkerke	0.759
McFadden	0.540

En la tabla 20, análisis de coeficiente de R^2 de Nagelkerke se obtuvo un valor 0.759, cuyo resultado es superior a Cox y Snell y McFadden. Este resultado representa un 75.9% de incidencia de la dimensión protección de infraestructura crítica de ciberseguridad en la gestión de TI. De tal forma, se comprobó que los valores resultantes están de 0.75 al 0.89 que indica una correlación positiva muy fuerte. Por tanto, se considera la hipótesis alterna (H_1).

Tabla 21

Estimaciones de los parámetros de incidencia de la dimensión protección de infraestructura critica de la variable ciberseguridad en la variable gestión de tecnologías de información.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[D2V1 = 1]	-7,861	1,117	49,560	1	,000	-10,049	-5,672
	[D2V1 = 2]	-2,550	,464	30,143	1	,000	-3,460	-1,640
Ubicación	[V1=1]	-10,906	1,515	51,841	1	,000	-13,874	-7,937
	[V1=2]	-3,410	,522	42,652	1	,000	-4,433	-2,386

En la tabla 21, se evidenció que existe una representación de -3.410 en la estimación de incidencia de la dimensión protección de infraestructura crítica de ciberseguridad en la gestión de TI, con significancia de p=0.000, el cual es inferior a 0.0.5 y que determina que existe incidencia significativa de las dos variables. Asimismo, el

coeficiente de estimación Wald es mayor 1. Por tanto, se considera la hipótesis alterna (H_1).

Prueba de Hipótesis específica 3:

Formulación de hipótesis estadística:

H_1: Existe incidencia significativa entre la dimensión control técnico de seguridad de la variable ciberseguridad y la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

H_0: No existe incidencia significativa entre la dimensión control técnico de seguridad de la variable ciberseguridad y la variable gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.

Contrastación de hipótesis estadística:

Tabla 22

Información sobre el ajuste del modelo que explica la incidencia de la dimensión control técnico de seguridad de la variable ciberseguridad en la variable la gestión de tecnologías de información.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	195.975			
Final	12.118	183.857	2	0.000

En la tabla 22 se demostró una significancia p=0.000, cuyo resultado es inferior a 0.05; la misma que determina incidencia significativa de la dimensión control técnico de seguridad de la ciberseguridad sobre la gestión de TI, cuyo enfoque de análisis aplica regresión ordinal

Tabla 23

Bondad de ajuste de la incidencia de la dimensión control técnico de seguridad de la variable ciberseguridad en la variable gestión de tecnologías de información

	Chi-cuadrado	gl	Sig.
Pearson	0.033	2	0.984
Desviación	0.065	2	0.968

En la tabla 23 se comprobó que el Chi-cuadrado de Pearson tiene un valor de 0.984, cuyo resultado es mayor a 0.05, la cual determina como resultado que la información registrada es consistente.

Tabla 24

Pseudo R Cuadrado de la incidencia de la dimensión control técnico de seguridad de la variable ciberseguridad en la variable gestión de tecnologías de información

Coeficiente R^2	Valor
Cox y Snell	0.650
Nagelkerke	0.759
McFadden	0.540

En la tabla 24, análisis de coeficiente de R^2 de Nagelkerke se obtuvo un valor 0.759, cuyo resultado es superior a Cox y Snell y McFadden. Este resultado representa un 75.9% de dimensión control técnico de seguridad de la ciberseguridad en la gestión de TI. De tal forma, se comprobó que los valores resultantes están de 0.75 al 0.89 que indica una correlación positiva muy fuerte. Por tanto, se considera la hipótesis alterna (H_1).

Tabla 25

Estimaciones de los parámetros de incidencia de la dimensión control técnico de seguridad de la variable ciberseguridad en la variable gestión de tecnologías de información.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[D3V1 = 1]	-7,861	1,117	49,560	1	,000	-10,049	-5,672
	[D3V1 = 2]	-2,550	,464	30,143	1	,000	-3,460	-1,640
Ubicación	[V1=1]	-10,906	1,515	51,841	1	,000	-13,874	-7,937
	[V1=2]	-3,410	,522	42,652	1	,000	-4,433	-2,386

En la tabla 25, se evidenció que existe una representación de -3.410 en la estimación de la dimensión control técnico de seguridad de la ciberseguridad en la gestión de TI, con significancia de p=0.000, el cual es inferior a 0.0.5 y que determina que existe incidencia significativa de las dos variables. Asimismo, el coeficiente de estimación Wald es mayor 1. Por tanto, se considera la hipótesis alterna (H_1).

V. DISCUSIÓN

Con los resultados obtenidos y descritos en el capítulo anterior de la investigación, se procedió a realizar las discusiones con respecto a la incidencia de la ciberseguridad en la gestión TI en una IAFAS, Lima 2022.

Respecto al objetivo general, en el análisis descriptivo, se comprobó un índice de mayor aceptación en el nivel “Óptimo” de la variable ciberseguridad y con nivel “Bueno” de la variable gestión de TI, que representa un 37.7%; con un índice intermedio de aceptación en el nivel “Moderado” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 28.6% y con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la variable gestión de TI que representa un 0%, de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS.

Asimismo, en el análisis inferencial, se consideró expresar de forma analítica el cálculo de coeficiente de correlación que existe en las dos variables de estudio, para ello se consideró la aplicación de regresión ordinal; con una significancia de 0.000 y que viene a ser un valor inferior a 0.05; de la misma forma, se obtuvo coeficiente R^2 de Nagelkerke que representa un 53.7% de incidencia de la ciberseguridad en la gestión TI; cuyos valores resultantes están de 0.50 al 0.74 que indica correspondencia positiva considerable. Por tanto, se considera la hipótesis alterna (H_1).

Los resultados obtenidos en la investigación concuerdan con Gumucio (2021), que en su investigación sostiene que, gestión de ciberseguridad alineado en un marco de buenas prácticas para la evaluación de riesgos NIST, traerá beneficio a la entidad financiera para asegurar los posibles riesgos de operación y la confidencialidad de información de los cibernautas. De manera similar Vosikas (2021), en su investigación determina la que implementación efectiva de un plan

de ciberseguridad incide notablemente en la gestión de TI y seguridad de información de los dispositivos y aplicativos interconectados en una tecnología del internet de las cosas médicas IoMT. Igualmente, Xiaoyan (2020) en su investigación demostró que una adecuada gestión seguridad de información aplicando ISO 27001 en los procesos de TI, incide en un 48% del nivel cumplimiento de los mecanismos de control de la ciberseguridad y la gestión de TI. Finalmente, Manrique (2022), demostró que la aplicación de ciberseguridad mejoró en la protección y gestión de TI, la cual optimiza los procesos a través de controles establecidos en la institución.

Lo mencionado está relacionado con la variable independiente ciberseguridad, donde Romero (2018), indica que la ciberseguridad es está compuesto por políticas y directrices como métodos de gestión de riesgos que se utilizan para proteger la información almacenada en ciberentorno, asimismo Reta et al. (2019), menciona que la ciberseguridad es un conjunto de acciones ejecutadas para mitigar los riesgos en el ciberespacio; la variable gestión de TI, según Bermeo et al. (2020), son técnicas de apoyo en el desarrollo de interacción de las TIC, cuyas herramientas permiten mejora de los procesos de informática, infraestructura tecnológica e internet. De manera similar, Villarreal at al. (2021), indica que la gestión de TI consiste en definir el proceso de transformación de los activos de información a través de la creación de servicios y políticas de TI, para lograr una vista holística de un entorno gestionado. Los mismos que se fundamenta con la teoría general de sistemas, según Maldonado (2017), indica que la TGS está conformada por metodologías y métodos para facilitar una visión general del universo, que permiten una dinámica en la generación de ideas.

Respecto al objetivo específico 1, en el análisis descriptivo, se comprobó un índice de mayor aceptación en el nivel “Moderado” de la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 42.3%; con un índice intermedio de aceptación en las respuestas de nivel “Óptimo” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el

22.9% y con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0%, de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS.

Asimismo, en el análisis inferencial, se consideró expresar de forma analítica el cálculo de coeficiente de correlación que existe en las dos variables de estudio, para ello se consideró la aplicación de regresión ordinal; con una significancia de 0.000 y que viene a ser un valor inferior a 0.05; de la misma forma, se obtuvo coeficiente R^2 de Nagelkerke que representa un 76.3% de incidencia de la ciberseguridad en la gestión TI; cuyos valores resultantes están de 0.75 al 0.89 que indica correspondencia positiva muy fuerte. Por tanto, se considera la hipótesis alterna (H_1).

Los resultados mencionados en la investigación concuerdan con Avellán y Zambrano (2019), en su investigación sostienen que la identificación de riesgos de ciberseguridad ha mejorado notablemente en la gestión de controles de TI y la seguridad de las plataformas tecnológicas de la institución educativa. De manera similar, Mendoza y Vega (2019), determinaron que la implementación del marco NIST como estrategia de seguridad, permitió mejorar la gestión y capacidad de respuesta ante eventos críticos de ciberataques. Igualmente, Cruzado y Rodríguez (2022), demostraron que la implementación del modelo de ciberseguridad denominado “HOGO”, permitió aplicar como estrategias de seguridad los controles del marco ISO 27032 que garantiza la integridad de información en las pymes, de esta forma la aplicación de la ciberseguridad mejoró en una brecha de 25% en los procesos de gestión de TI.

Lo mencionado está relacionado con la dimensión estrategias de seguridad de la variable independiente ciberseguridad, donde Aguilar (2019), define que las estrategias de seguridad permitirán consolidar una política de ciberseguridad y para prevenir posibles ciberamenazas, asimismo Díaz (2021), indica que una

estrategia de seguridad busca variables de análisis para asignar prioridades y recursos en la prevención y elaboración de un plan para la ciberseguridad, de igual forma, Aguilar (2021), menciona que los ejes de un marco legal para la ciberseguridad y el cibercrimen, debe estar establecido como estrategia de seguridad. Por otro lado, la variable gestión de tecnologías de información, según Casanova y Calderón (2019). Indica que gestión de TI es un proceso de transformación estratégica para mejorar los procesos de negocio, reducir costos de operación e innovación, garantizando el cumplimiento de objetivos como organización. Los mismos que se fundamenta con la teoría general de sistemas y la teoría de restricciones - TOC, según Sagasti y Mitroff (1973) y Kish et al. (2021), sostienen que un sistema se tiene que analizar en forma holística, donde se integre todos los componentes que conlleven a una interrelación propia del sistema y finalmente Hernández et al. (2020), menciona que TOC, está basado a un pensamiento sistemático que aborda la identificación de restricciones para aumentar la productividad y mejorar los objetivos.

Respecto al objetivo específico 2, en el análisis descriptivo, se comprobó un índice de mayor aceptación en el nivel “Óptimo” en la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 44.6%; con un índice intermedio de aceptación en las respuestas de nivel “Moderado” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 21.7% y con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0%, de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS.

Asimismo, en el análisis inferencial, se consideró expresar de forma analítica el cálculo de coeficiente de correlación que existe en las dos variables de estudio, para ello se consideró la aplicación de regresión ordinal; con una significancia de 0.000 y que viene a ser un valor inferior a 0.05; de la misma forma, se obtuvo coeficiente R^2 de Nagelkerke que representa un 75.9% de incidencia de la

ciberseguridad en la gestión TI; cuyos valores resultantes están de 0.75 al 0.89 que indica correspondencia positiva muy fuerte. Por tanto, se considera la hipótesis alterna (H_1).

Los resultados mencionados en la investigación concuerdan con Rajamäki (2021), que en su investigación sostiene, que la integración del sistema de control de seguridad gestionada de TI aplicado en los controles de operaciones de TI, mejora la gestión de riesgos en la protección de infraestructura crítica, como la protección de enpoints, redundancia y segmentación de redes como mecanismo de ciberseguridad y las habilidades de gestión TI. De manera similar Salinas (2020), en su investigación indica que adoptar un modelo de ciberseguridad, permite generar y mejorar el enfoque de transformación digital y una protección de infraestructura crítica, aplicando controles de seguridad en el marco NIST para la gestión de riesgos de los servicios de las cajas municipales y la generación de una cultura de ciberseguridad para la institución. Igualmente, Ormachea (2019), en su investigación menciona que el desarrollo de estrategias de la ciberseguridad será más eficiente y eficaz con la implantación de políticas de seguridad a nivel nacional, el cual conlleva a una identificación de las limitaciones y brechas que se tiene para el desarrollo, evaluación y actualización de estrategias de protección de infraestructura en la ciberseguridad frente a la gestión de TI.

Lo mencionado está relacionado con la dimensión protección de infraestructura crítica de la variable independiente ciberseguridad, donde Zuluaga (2020), menciona que la protección de infraestructura crítica presta un servicio esencial y fundamental en el ciberespacio, para ello se tiene que establecer un plan de protección y defensa a nivel de ciberseguridad. De la misma forma, Kulugh et al. (2022), menciona la protección de una infraestructura critica apoya a la sociedad moderna a enfrentar las amenazas inherentes a los ciberataques y permite asegurar la disponibilidad continua de los servicios tecnológicos, de igual forma López et al. (2021), donde indican que la protección de una infraestructura crítica es clave para una adecuada estrategia nacional de ciberseguridad, determinar

directrices y dicho desarrollo que involucre a la sociedad como medida de seguridad de entorno. Por otro lado, la variable gestión de tecnologías de información, Rodríguez y Espinosa (2022), menciona que gestión de TI, es el grado de sinergia que tiene la gerencia o área de TI, para desarrollar una planificación de TI alineados a las estrategias de la organización, con el propósito de optimizar los procesos de respuesta a las incidencias a nivel operativo. De manera similar, Quintero y Peña (2017), indican que la estrategia de servicio es un componente fundamental para proveer la gestión de TI, donde pueda incluir políticas y marcos de trabajo estandarizado. Los mismos que se fundamenta con la teoría general de sistemas y la teoría de restricciones, el cual según Rosen (1969), sostiene un sistema es una interdependencia e interacción con un solo propósito en común y finalmente Horna (2020) define que un TOC, es una restricción optimizada de los procesos del negocio, que permitirá determinar una mezcla optima de producción para una adecuada gestión y la toma de decisión.

Respecto al objetivo específico 3, en el análisis descriptivo, se comprobó un índice de mayor aceptación en el nivel “Óptimo” en la variable ciberseguridad y con nivel “Bueno” en la variable gestión de TI, que representa un 44.6%; con un índice intermedio de aceptación en las respuestas de nivel “Moderado” de la variable ciberseguridad con el nivel “Bueno” de la variable gestión de TI, que representa el 21.7% y con menor índice de aceptación se realizó en las respuestas del nivel “Óptimo” de la variable ciberseguridad y el nivel “Malo” de la gestión de TI que representa un 0%, de un total de 175 cuestionarios registrados por los servidores públicos de una IAFAS.

Asimismo, en el análisis inferencial, se consideró expresar de forma analítica el cálculo de coeficiente de correlación que existe en las dos variables de estudio, para ello se consideró la aplicación de regresión ordinal; con una significancia de 0.000 y que viene a ser un valor inferior a 0.05; de la misma forma, se obtuvo coeficiente R^2 de Nagelkerke que representa un 75.9% de incidencia de la ciberseguridad en la gestión TI; cuyos valores resultantes están de 0.75 al 0.89

que indica correspondencia positiva muy fuerte. Por tanto, se considera la hipótesis alterna (H_1).

Los resultados mencionados en la investigación concuerdan con Xiaoyan (2020), que en su investigación sostiene que, la implementación de políticas de seguridad en el marco ISO 27001 para la gestión de información mejoró en un 48% de cumplimiento de controles frente al ciberataque. De manera similar Cruzado y Rodríguez (2022), en su investigación demostraron que la implementación del modelo de ciberseguridad denominado “HOGO”, el cual permitió aplicar como estrategias de seguridad los controles del marco ISO 27032 que garantiza la integridad de información en las pymes, de esta forma la aplicación de la ciberseguridad mejoró en una brecha de 25% en los procesos de gestión de TI. Igualmente, Salinas (2020), en su investigación indica que adoptar un modelo de ciberseguridad, permite generar y mejorar el enfoque de transformación digital y una protección de infraestructura crítica, aplicando controles de seguridad en el marco NIST para la gestión de riesgos de los servicios de las cajas municipales y la generación de una cultura de ciberseguridad para la institución.

Lo mencionado está relacionado con la dimensión control técnico de seguridad de la variable independiente ciberseguridad, donde Sabillón y Cano (2019), definen que un control técnico de seguridad permitirá materializar un programa de ciberseguridad y desarrollar un marco de trabajo para realizar auditorías y concientizar en seguridad de la información basado a los objetivos de empresa, asimismo Gutiérrez (2020), menciona que establecer los controles seguridad permitirá a las organizaciones a centrarse y mejorar el despliegue de estándares de seguridad cibernética a fin de aminorar los ciberataques, de igual forma, Zekos (2022), mencionan que el control de seguridad es un programa de ciberseguridad para proteger la información valiosa de manera confidencial y asegurar la evaluación efectiva de ciberseguridad. Por otro se tiene la variable gestión de tecnologías de información, según Casanova y Calderón (2019). Indica que gestión de TI es un proceso de transformación estratégica para mejorar los procesos de

negocio, reducir costos de operación e innovación, garantizando el cumplimiento de objetivos como organización. De manera similar, Sánchez y Valles (2021) mencionan que el enfoque de gestión tecnologías de información es un marco de buenas prácticas de servicio de TI, que detecta cuellos de botella y genera valor agregado en los servicios de gestión de TI. Los mismos que se fundamenta con la teoría general de sistemas y la teoría de restricciones, el cual según Sagasti y Mitroff (1973) y Kish et al. (2021), sostienen que un sistema se tiene que analizar en forma holística, donde se integre todos los componentes y esta conllevara a una interrelación propia del sistema y finalmente Marín (2013) y Jiang y Wu (2013), indican que la teoría de restricciones permite administrar de manera efectiva las operaciones de producción enfocados para detectar, definir capacidad y considera la variabilidad de elementos que componente un sistema.

Respecto a la metodología de investigación, se consideró que, al ser de tipo de estudio básico, permitió una exploración de conocimientos, desde una fase inicial como la recolección de datos de información a través de un cuestionario en línea, las cuales han sido respondidos por los servidores públicos de una IAFAS. Se aplicó una investigación de diseño no experimental y para el análisis estadístico inferencial se consideró como método paramétrico, desarrollándose con el coeficiente de regresión ordinal, donde se comprobó que existe una incidencia significativa de la ciberseguridad en la gestión de TI en una institución asegurad de salud.

Por otro lado, mencionar que la encuesta realizada a los servidores públicos de una IAFAS, presenta cierto sesgo subjetivo debido a que se depende de la apreciación del encuestado. Asimismo, mencionar que los objetivos establecidos y sustentados en la investigación, ha permitido a la institución aseguradora en salud, conocer un análisis de la situación actual con respecto a la ciberseguridad y su incidencia en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud.

VII. CONCLUSIONES

Con los resultados de obtenidos y descrita en los capítulos anteriores de la investigación, se concluye lo siguiente:

Primera: Se determina que la variable ciberseguridad incide significativamente en la variable gestión de tecnologías de información, debido a que el P valor de significancia es de 0.000 y el coeficiente de R cuadrado de Nagelkerke, se obtuvo un valor representa 53.7%, el cual indica que existe una correlación positiva considerable. Por lo tanto, se cumplió con el objetivo general de la investigación, por contener datos consistentes con el modelo ajustado.

Segunda: Se determina que la dimensión estrategias de seguridad de la variable ciberseguridad incide significativamente en la variable gestión de tecnologías de información, debido a que el P valor de significancia es de 0.000 y el coeficiente de R cuadrado de Nagelkerke, se obtuvo un valor representa 76.3%, el cual indica que existe una correlación positiva muy fuerte. Por lo tanto, se cumplió con el primer objetivo específico de la investigación, por contener datos consistentes con el modelo ajustado.

Tercera: Se determina que la dimensión protección de infraestructura critica de la variable ciberseguridad incide significativamente en la variable gestión de tecnologías de información, debido a que el P valor de significancia es de 0.000 y el coeficiente de R cuadrado de Nagelkerke, se obtuvo un valor representa 75.9%, el cual indica que existe una correlación positiva muy fuerte. Por lo tanto, se cumplió con el segundo objetivo específico de la investigación, por contener datos consistentes con el modelo ajustado.

Cuarta: Se determina que la dimensión control técnico de seguridad de la variable ciberseguridad incide significativamente en la variable gestión de

tecnologías de información, debido a que el P valor de significancia es de 0.000 y el coeficiente de R cuadrado de Nagelkerke, se obtuvo un valor representa 75.9%, el cual indica que existe una correlación positiva muy fuerte. Por lo tanto, se cumplió con el tercer objetivo específico de la investigación, por contener datos consistentes con el modelo ajustado.

VIII. RECOMENDACIONES

Con los resultados de obtenidos y las conclusiones descritas en los capítulos anteriores de la investigación, se recomienda lo siguiente:

Primera: Para mejorar la incidencia de la ciberseguridad en la gestión TI de la IAFAS, se recomienda al secretario general y al director ejecutivo de la Oficina General de Tecnología de la Información (OGTI), establecer comité de ciberseguridad debido a que la institución no cuenta en la actualidad. Esto con la finalidad de implementar y optimizar los procesos en el marco ISO 27032.

Segunda: Para mantener la incidencia de la dimensión estrategias de seguridad de la ciberseguridad en la gestión de TI de la IAFAS, se recomienda al director ejecutivo de la OGTI y al oficial de seguridad, establecer mecanismos y controles de políticas de seguridad, como indicadores de gestión en la institución. Esto con la finalidad de dar cumplimiento el marco ISO 27032.

Tercera: Para mantener la incidencia de la dimensión protección de infraestructura crítica de la ciberseguridad en la gestión de tecnologías de información en la IAFAS, se recomienda al director ejecutivo de la OGTI y al jefe de la unidad de infraestructura TI, establecer controles para la gestión de riesgos y respuestas ante eventos críticos. Esto con la finalidad de dar cumplimiento el marco ISO 27032.

Cuarta: Para mantener la incidencia de la dimensión control técnico de seguridad de la ciberseguridad en la gestión de TI de la IAFAS, se recomienda al director ejecutivo de la OGTI y al oficial de seguridad, establecer auditorias de control interno. Esto con la finalidad de dar cumplimiento el marco ISO 27032.

REFERENCIAS

Aguilar, J. (2021). Latin America challenges and opportunities in cyber security in the face of the global context of cyber threats to national security and foreign policy. 169-197. Disponible en: https://scielo.conicyt.cl/pdf/rei/v53n198/0719-3769-rei-53-198-00169.pdf

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO Revista Latinoamericana de Estudios Seguridad, (25), 24-40.DOI: https://doi.org/10.17141/urvio.25.2019.4007

Andrade, M. (2021). Implementación de service desk de tecnología Punto de contacto para la mejora de la calidad de los servicios en la empresa Servicios Call Center del Perú (SCC) Lima-2021. Disponible en: http://repositorio.ulasamericas.edu.pe/handle/upa/1761

Astudillo, P. y Encalada, C. (2019). Gestión de servicios tecnológicos, para una empresa pública de la ciudad de Cuenca, basados en ITIL V.3. Revista Polo del Conocimiento.34 (6).300-325. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7164349

Avellán, N. y Zambrano, M. (2019). Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí. Ecuador. Disponible en: http://repositorio.espam.edu.ec/handle/42000/1032

Baena, G. (2017). Metodología de la investigación (3a. Ed.). Grupo Editorial Patria. Disponible en: http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Bermeo, M., Montoya, L., Valencia, A. y Mejía, M. (2020). Incursión de las TIC en la gestión de la información financiera en las empresas pyme comerciales: estudio de caso.NOVUM, 1(10), 25 – 41 Disponible en: https://revistas.unal.edu.co/index.php/ novum/article/view /84003/73642

Carrillo, J., Zambrano, N. y Bravo, M. (2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. Revista Ibérica de sistemas e tecnologías de Información, 41-50. Disponible en: https://www.proquest.com/scholarly-journals/proceso-de-ciberseguridad-guía-metodológica-para/docview/2394538125/se-2

Casanova, M. y Calderón, C. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. Tecnológicas, 23(48), 31-53. DOI: https://doi.org/10.22430/22565337.1449

Casanova, M. y Calderón, C. (2019). Sistema para ejecutar políticas sobre Infraestructuras de Tecnologías de la Información. Ingeniare: Revista Chilena de Ingeniería, 27(3), 479-494. Disponible en: https://www.proquest.com/scholarly-journals/sistema-para-ejecutar-políticas-sobre/docview/2345929530/se-2

Criollo W., López M. y Yáñez J. (2020). Guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto. Disponible en: https://www.researchgate.net/publication/354582493_Guia_de_aplicacion_para_el_monitoreo_de_ciberseguridad_con_herramientas_de_codigo_abierto

Cornejo, Y. (2019). Cyberdefense, Cybersecurity And Its Effects In The Society. 4(2). International Multilingual Journal of Science and Technology. Disponible en: http://www.imjst.org/wp-content/uploads/2019/02/IMJSTP29120135.pdf

Cruzado, C. y Rodriguez, L. (2022). Marco de referencia “HOGO” para ciberseguridad en PyMES basado en ISO 27002 y 27032. Disponible en: http://hdl.handle.net/20.500.12840/5200

Cuesta, Y. (2020). Propuesta de modelo de gestión y operación de servicios de tecnologías de información para Colombian Shared Services. Universidad Externado de Colombia. Disponible en: https://bdigital.uexternado.edu.co/handle/001/3550

Díaz P., Rodríguez, M. y Espinosa, J. (2022). Niveles de madurez de la capacidad en tecnologías de información en micro, pequeñas y medianas empresas. Innovar, 32(84), 175-191. DOI: https://doi.org/10.15446/innovar.v32n84.100595

Diaz, R. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe, Santiago, Comisión Económica para América Latina y el Caribe (CEPAL). Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/47240/S2100485_es.pdf?sequence=1&isAllowed=y

Domínguez, V., y López, M. (2019). Teoría General de Sistemas, un enfoque práctico. TECNOCIENCIA Chihuahua, 10(3), 125-132. Disponible en: https://148.229.0.27/index.php/tecnociencia/article/view/174

Galeano, R. y González, O. (2021). Auditoría informática basada en combinación de normas ITIL y COBIT aplicada al sistema de gestión del Laboratorio de Informática, FPUNE. FPUNE Scientific, (15). Disponible en: http://servicios.fpune.edu.py:83/fpunescientific/index.php/fpunescientific/article/view/207

Gómez, F. y Valencia, H. (2021). Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa. Disponible en: http://hdl.handle.net/20.500.12622/5197

Gumucio, J. (2021). Guía de implementación de un programa de gestión de riesgos de Ciberseguridad en entidades de Intermediación Financiera. Chile. Disponible en: https://repositorio.uchile.cl/handle/2250/180169

Gutiérrez J. (2020). OEA: México debe mejorar ciberseguridad. La Jornada. Disponible en: https://www.proquest.com/newspapers/oea-méxico-debe-mejorar-ciberseguridad/docview/2428999352/se-2?accountid=37408

Hernández, M. (2022). Situation of digital financial services, information security and cybersecurity in the Popular and Solidarity Financial Sector. 6(14). 18-32.

Disponible en: https://ojs.supercias.gob.ec/index.php/X-pedientes _Economicos/article/view/100/91

Hernández H, Solórzano J., y Jinete J. (2020). Teoría de restricciones para los procesos de gestión y control en las IPS del Caribe Colombiano, Investigación E Innovación En Ingenierías, 8(1), 54-68. Disponible en: https://doi.org/10.17081/invinno.8.1.3624

Hernández, R. y Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Ed. Mc Graw Hill Education. ISBN: 978-1-4562-6096-5. Disponible en: https://virtual.cuautitlan.unam.mx/ rudics/?p=2612

Horna, M. (2020). Impacto de la teoría de restricciones en la calidad del servicio de las tecnologías de la información y comunicaciones y la economía circular. Disponible en: https://hdl.handle.net/11354/3051

IT Reseller (2022). Tres de cada 10 empresas españolas han sufrido ciberataques en el último año. Revista de tecnología y consultoría. IT Digital Media Group. España. Disponible en: https://www.itreseller.es/seguridad/2022/04/tres-de-cada-10-empresas-espanolas-han-sufrido-ciberataques-en-el-ultimo-ano

Jara F. y Jorquera A. (2021). Liability of the State Administration for cybersecurity breaches. Revista chilena de derecho y tecnología, 10(1), 201-230. Disponible en: https://dx.doi.org/10.5354/0719-2584.2021.58776

Jiang, Y., Wu, H. (2013) Optimization of setup frequency for TOC supply chain replenishment system with capacity constraints. Neural Comput & Applic 23, 1831–1838. DOI: https://doi.org/10.1007/s00521-013-1376-0

Kish, K., Mallery, D., Yahya, G., Melgar, R. y Burke, M. (2021). Fostering critical pluralism with systems theory, methods, and heuristics. Ecological Economics, 189, 107171. Disponible en: https://sci-hub.se/https://doi.org/10.1016/j.ecolecon.2021.107171

Kulugh, V., Mbanso, U. y Chukwudebe, G. (2022). Cybersecurity Resilience Maturity ssessment Model for Critical National Information Infrastructure.SN Computer Science, 3 (3), art. no. 217.DOI: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85128007197&doi=10.1007%2fs42979-022-01108-x&partnerID=40&md5

Leyva, A. (2021). Proposal of cyber security strategies. Theoretical - practical approaches towards readiness in Latin American countries. Ciencias tecnicas y aplicadas. 7(1). 1186-1208. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8385888

López, F, Ruete, D. y Gatica, G. (2021). Critical Infrastructure and Cybersecurity in Chile: Guidelines for Consensus. RISTI - Revista Ibérica de sistemas y tecnologías de Informacao,41-55. Disponible en: https://www.scopus.com/record/display.uri?eid=2-s2.0-85124399710&origin=inward&txGid=e1d0281dd99c86d7267b055503eeeaa0&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1

Malatji, M., Marnewick, A. y Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information and Computer Security, 30(2), 255-279. DOI: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116864184& doi =10.1108%2fICS-06-2021-0091&partnerID=40&md5=6

Maldonado, C. (2017). Ciencia hecha realidad. Reseña de C. A. Ossa, Teoría general de sistemas. Conceptos y aplicaciones. INNOVAR. Revista de Ciencias Administrativas y Sociales, 27(64), 157-159. Disponible en: https://www.redalyc.org/articulo.oa?id=81850404014

Manrique, V. (2022). Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima - 2021. Disponible en: https://hdl.handle.net/20.500.12692/84954

Marín, W. (2013). Desarrollo e implementación de un modelo de teoría de restricciones para sincronizar las operaciones en la cadena de suministro,

volumen 10. 67-77. Disponible en: http://www.scielo.org.co/pdf/eia/n19/n19a06.pdf

Meléndez, K. y Dávila, A. (2018). Adoption's problems of information technology service management models. A systematic literature review. Dyna, 85(204), 215-222. DOI: http://dx.doi.org/10.15446/dyna.v85n204.57076

Mendoza, S. y Vega, G. (2019). Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC. Disponible en: http://hdl.handle.net/11354/2250

Mishima, M. (2021), EY Perú: Más del 60% de empresas peruanas muestra preocupación por su capacidad para enfrentar ataques de ciberseguridad. Disponible en: https://www.ey.com/es_pe/news/2021/10/empresas-peruanas-preocupacion-ataques-ciberseguridad

Moreno et al. (2020). Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. Reporte de Ciberseguridad. BID-OEA, pp. 42-45 Disponible en: http://dx.doi.org/10.18235/0002513

Moudoubah, L., Yamami, A. y Mansouri, K. (2021). From IT service management to IT service governance: An ontological approach for integrated use of ITIL and COBIT frameworks. International Journal of Electrical and Computer Engineering, 11 (6), 5292-5300. Disponible en: http://doi.org/10.11591/ijece.v11i6.pp5292-5300

Muhamet, G., Naim, P. y Peter, K. (2018). IT Infrastructure Library (ITIL) framework approach to IT Governance,Vol 51,181-185. DOI: https://doi.org/10.1016/j.ifacol.2018. 11.283

Nina, A. y Vera, M. (2021). Analyzing content of tasks in Business Process Management. Blending task execution and organization perspectives, Computers in Industry,Vol. 130.1666-3615. DOI: https://doi.org/10.1016/j.compind.2021.103463

Ñaupas, H., Mejía, E., Novoa, E. y Villagómez A. (2018). Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis. 5a. Ed. Ediciones de U. Disponible en: https://www.academia.edu/59660080/%C3%91aupas_Metodolog%C3%ADa_de_la_investigaci%C3%B3n_4ta_Edici%C3%B3n_Humberto_%C3%91aupas_Pait%C3%A1n

Ormachea, M. (2019). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Disponible en: http://renati.sunedu.gob.pe/handle/sunedu/1336266

Penagos, J., Acuña, M., y galvis L. (2012). Theory of Constraints Applied to Manufacturing and Services Company,79-68. Disponible en: https://dialnet.unirioja.es/servlet/articulo? codigo=6579705

Pérez, F., Berna J. y Fonseca, I. (2021), Strategic IT alignment Projects. Towards Good Governance, Computer Standards & Interfaces,Vol. 76.0920-5489.DOI: https://doi.org/10.1016/j.csi.2021.103514

Piñuela, J. y Quito, C. (2020). Los desafíos de la gestión por procesos en la era digital. Estudios de la Gestión: Revista Internacional de administración, (8), 127-144. DOI: https://doi.org/10.32719/25506641.2020.8.1

Quintero, L. y Peña V. (2017). Modelo basado en ITIL para la Gestión de los Servicios de TI en la Cooperativa de Caficultores de Manizales. Scientia Et Technica, 22(4), 371-380. Disponible en: https://ojs2.utp.edu.co/index.php/revistaciencia/article/view/13211

Rajamäki, A. (2021). Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center.Universidad de Ciencias aplicadas de Xamk, Finlandia. Disponible en: https://urn.fi/URN:NBN:fi:amk-2021052410764

Reta, C., Fernández, L., Uvalle, R., y Jiménez, J. (2019). Ciberseguridad en América Latina. Revista de Administración Pública INAP. Ciberseguridad Nacional.148 (1).23-46. Disponible en:

https://www.academia.edu/40689299/Ciberseguridad_estado_de_la_cuesti%C3%B3n_en_Am%C3%A9rica_Latina

Romero, J. (2018). Conceptualización De Una Estrategia De Ciberseguridad Para La Seguridad Nacional De México. 28. Disponible en: http://www.redalyc.org/articulo.oa?id=65458498003%0ACómo

Rosen, R. (1969). General System Theory. Foundations, Development, Applications. Ludwig von Bertalanffy. Braziller, New York, 1969.681–682. Disponible en: https://www.science.org/doi/10.1126/science.164.3880.681

Sabillón R. y Cano J. (2019). Audits in Cybersecurity: A model of general application for companies and nations. Revista Ibérica de sistemas y tecnologías de información, (32), 33-48. DOI: https://doi.org/10.17013/risti.32.33-48

Sagasti, F. y Mitroff, I. (1973). Operations research from the viewpoint of general systems theory. Ed. Omega. DOI: https://doi.org/10.1016/0305-0483(73)90087-X

Salinas, A. (2020). Modelo de Ciberseguridad para cajas municipales en tiempos de transformación digital – un nuevo enfoque. Disponible en: https://hdl.handle.net/11537/29733

Sánchez, A. (2020). Digitalizar la infraestructura crítica, prioridad ante ciberseguridad. Disponible en: https://www.proquest.com/wire-feeds/digitalizar-la-infraestructura-crítica-prioridad/docview/2467706119/se-2?accountid=37408

Sánchez, F. y Valles, M. (2021). Implementación de ITIL versión 3 en las organizaciones: Razones del éxito y fracaso. Revista Científica de Sistemas E Informática, 1(2), 54-66.DOI: https://doi.org/10.51252/rcsi.v1i2.191

Santabárbara, J. (2019). Cálculo del intervalo de confianza para los coeficientes de correlación mediante sintaxis en SPSS. REIRE Revista d'Innovació i Recerca en Educació, 12(2), 1–14. DOI: https://doi.org/10.1344/reire2021.14.132565

Seising, R. (2010). Cybernetics, system(s) theory, information theory and Fuzzy Sets and Systems in the 1950s and 1960s. Information Sciences, 180(23), 4459–4476. DOI: https://doi.org/10.1016/j.ins.2010.08.001

Tining, A. (2019). E-Commerce Service Design Readiness using ITIL framework with IT Balanced Scorecard Objective (Case Study: University E-Commerce), Procedia Computer Science, Vol.161.283-290. DOI: https://doi.org/10.1016/j.procs.2019.11.125

Tuapanta, J., Duque, M. y Mena, A. (2017). Alfa de Cronbach para validar un cuestionario de uso de TIC en Docentes Universitarios. Revista ESPOCH. Nº10. 37-48. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/9807

Vásquez, C., Peláez, D., y Burgos, F. (2019). Validación de un modelo de medición para la estación de la calidad del servicio en el ámbito de la auditoría de tecnologías de la información. Revista Ibérica de sistemas y tecnologías de Información. 53-66. Disponible en: https://www.proquest.com/scholarly-journals/validación-de-un-modelo-medición-para-la-gestión/docview/2348878045/se-2

Villarreal, H., Marín, W., Angeles, J. y Cano, J. (2021). Gestión de Tecnología de Información para universidades peruanas aplicando computación en la nube. Revista Venezolana de Gerencia, 26(6), 665-679.DOI: https://doi.org/10.52080/rvgluz.26.e6.40

Vosikas, L. (2021). Cybersecurity in Internet of Medical Things. Risks and Challenges. Universidad de Ciencias aplicadas de Xamk. Finlandia. Disponible en: https://urn.fi/URN:NBN:fi:amk-202102102126

Xiaoyan, M. (2020). Diseño de un sistema de gestión de la seguridad de la información en una empresa de recursos humanos. España. Disponible en: http://hdl.handle.net/10017/44660

Zekos G. (2022). Cyberspace Governance and Politics. Contributions to Political Science, pp. 337-382. Disponible en: https://www.scopus.com/inward/

record.uri?eid=2-s2.0-85127913746&doi=10.1007%2f978-3-030-94736-1_8&partnerID=40&md

Zuluaga, D. (2020). Cybersecurity for centralized and distributed power generation at ISAGEN. Ingeniería y Ciencia, 16(32), 171-194. DOI: https://doi.org/10.17230/ingciencia.16.32.8

ANEXOS

Anexo 1: Matriz de Consistencia

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

PROBLEMA	OBJETIVOS	HIPÓTESIS
Problema principal: ¿De qué manera la ciberseguridad incide en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022? **Problemas específicos:** PE1: ¿De qué manera la dimensión estrategias de seguridad de la ciberseguridad incide en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022? PE2: ¿De qué manera la dimensión protección de infraestructura critica de la ciberseguridad incide en la gestión de tecnologías de información en una Institución Administradora de	**Objetivo principal:** Determinar la incidencia de la ciberseguridad en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022 **Objetivos específicos:** OE1: Determinar la incidencia de la dimensión estrategias de seguridad de la ciberseguridad en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022 EO2: Determinar la incidencia de la dimensión protección de infraestructura de la ciberseguridad en la gestión de tecnologías de información en una Institución Administradora	**Hipótesis principal:** La ciberseguridad incide significativamente en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022 **Hipótesis específicas:** HE1: La dimensión estrategias de seguridad de la ciberseguridad incide significativamente en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022 HE2: La dimensión protección de infraestructura critica de la ciberseguridad incide significativamente en la gestión de tecnologías de información en una Institución Administradora

VARIABLES E INDICADORES

Variable Independiente: Ciberseguridad

Dimensiones	Indicadores	Ítems	Niveles
Estrategias de seguridad	Planificación	1-2	No optimo
	Prevención	3-4	
	Capacidad de repuesta	5-6	
Protección de infraestructura crítica	Detección	7-8	Moderado
	Prevención	9-10	
	Capacidad de Respuesta	11-12	Optimo
Control técnico de seguridad	Implantación	13-14	
	Revisión	15-16	
	Mejora continua	17-18	

Variable Dependiente: Gestión de tecnologías de información

Dimensiones	Indicadores	Ítems	Niveles
Estrategia de servicio	Planificación	19-20	Malo
	Revisión	21-22	
	Mejora continua	23-24	

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
Fondos de Aseguramiento en Salud, Lima 2022?	de Fondos de Aseguramiento en Salud, Lima 2022	de Fondos de Aseguramiento en Salud, Lima 2022	Operación de servicio	Diseño	25-26	
				Transición	27-28	
				Mejora continua	29-30	
PE3: ¿De qué manera la dimensión control técnico de seguridad de la ciberseguridad incide en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022?	EO3: Determinar la incidencia de la dimensión control técnico de seguridad de la ciberseguridad en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022	HE3: La dimensión control técnico de seguridad de la ciberseguridad incide significativamente en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022	Continuidad de servicio	Planificación	31-32	Regular
				Evaluación	33-34	
				Controles correctivos	35-36	Bueno

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Básica **Diseño:** No experimental	**Población:** 321 Servidores públicos de una institución aseguradora de salud **Tamaño de muestra:** 175 encuestas realizados a los servidores públicos de una institución aseguradora de salud. **Muestreo:** Tipo Probabilístico aleatorio simple	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** En el análisis descriptivo, se realizó la interpretación de los datos de información recolectada a través de histogramas y tablas de contingencia o tablas cruzadas. **Inferencial:** En el análisis inferencial, se realizó el contraste de las hipótesis de las variables, utilizando métodos paramétricos y el coeficiente de análisis de regresión ordinal, que sirvió para determinar el grado correlación existente entre las dos variables de estudio.

Anexo 2: Matriz de Operacionalización de Variables

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable Independiente: Ciberseguridad Moreno et al. (2020), define que la ciberseguridad es un conjunto de métodos que persigue la protección integral de la información que se encuentra en el ciberespacio, en la cual se determinaron las siguientes dimensiones: Estrategias de seguridad, Protección de infraestructura crítica y Control técnico de seguridad.	**Estrategias de seguridad** Leyva (2021), define que una estrategia de seguridad busca responder las nuevas necesidades de seguridad y confianza en el ciberespacio, las cuales deberán establecerse con los principios y políticas nacionales	Planificación	1	¿Cree usted, que en la institución se debería mejorar políticas de seguridad de información, para evitar la ciberdelincuencia?	(1) No optimo Rango de: 18 a 42 (2) Moderado Rango de: 43 a 67 (3) Optimo Rango de: 68 a 90
			2	¿Considera usted, que es necesario la implementación de un plan de gestión de ciberseguridad?	
		Prevención	3	¿Constantemente se socializa, los planes de mejora y/o aplicación de controles para contrarrestar la ciberdelincuencia?	
			4	¿Tiene conocimiento, si la institución cuenta con herramientas tecnológicas para evitar la ciberdelincuencia?	
		Capacidad de repuesta	5	¿La institución tiene planes y estrategias de seguridad para evitar ciberataques?	
			6	¿Considera que el personal de la Oficina General de Tecnología de Información – OGTI, está capacitado para dar respuesta ante cualquier ciberataque?	

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Protección de infraestructura crítica Kulugh et al. (2022), define que la protección de una infraestructura critica, apoya la sociedad moderna a enfrentar las amenazas inherentes a los ciberataques, que pueden tener un impacto debilitante, si no se prepara para asegurar la disponibilidad y la continua de los servicios tecnológicos	Detección	7	¿Se tiene identificado los procesos críticos a nivel de infraestructura tecnología?	
			8	¿Está de acuerdo con la implementación de tecnologías para analizar y detectar intrusos o ciberdelincuentes?	
		Prevención	9	¿La institución cuenta con políticas de seguridad de control acceso actualizado, para prevenir algún acto ilícito o robo de información?	
			10	¿Considera que los mecanismos de seguridad de control acceso a la institución con videocámaras, son efectivas?	
		Capacidad de Respuesta	11	¿Cree usted que la Oficina General de Tecnología de Información, está preparado a nivel infraestructura tecnológica para dar respuesta un ciberataque?	
			12	¿Se monitorea los mecanismos de seguridad para brindar acceso de información al personal interno y externo?	

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Control técnico de seguridad Jara y Jorquera (2021), definen que el control de seguridad es un instrumento para lograr el un adecuado funcionamiento de servicios tecnológicos en las organizaciones con la finalidad de implementar, gestionar y realizar seguimiento de políticas de privacidad y protección ante un ataque ciberdelincuente.	Implantación	13	¿Cree que se está aplicando controles de la ciberseguridad a los usuarios que acceden a los sistemas de información?	
			14	¿En los 3 últimos meses, usted tenido alguna sospecha de un ataque cibernético, con los accesos que cuenta en la institución?	
		Revisión	15	¿Considera que la Oficina de General Tecnología de Información tiene un plan de contingencia en caso de un ciberataque?	
			16	¿Son eficientes los controles de seguridad aplicados en la institución para prevenir la ciberseguridad?	
		Mejora continua	17	¿Con que frecuencia se elaboran nuevas estrategias y/o políticas de seguridad, enmarcado en la ciberseguridad?	
			18	¿Se socializa los resultados de la Oficina General de Tecnología de Información, para mejorar la ciberseguridad?	

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable Dependiente: Gestión de tecnologías de información Sánchez y Valles (2021) mencionan que el enfoque de gestión tecnologías de información es un marco de buenas prácticas de servicio de TI, que detecta cuellos de botella y genera valor agregado en los servicios de gestión de TI, de esta manera se establecen las siguientes dimensiones: Estrategia de servicio, operación de servicio y continuidad de servicio.	**Estratégica de servicio** Galeano y González (2021), definen que una estrategia de servicio de TI, está enfocado en la necesidad y demanda de los servicios de tecnología de información, de tal manera que se deben alinear en los objetivos de la organización, para asegurar la continuidad de los servicios y mitigar riesgos en el ciclo de operación	Planificación	19	¿Se comunica oportunamente los planes de acción para el mejoramiento de servicios de tecnología de información, alineadas a los objetivos de la institución?	(1) Malo Rango de: 18 a 42 (2) Regular Rango de: 43 a 67 (3) Bueno Rango de: 68 a 90
			20	¿La ejecución de los procesos Core del negocio están implementados a través de herramientas tecnológicas, para su gestión, administración y toma de decisiones?	
		Revisión	21	¿Se analizan y verifican controles de seguridad para la gestión de planes de servicios de TI?	
			22	¿Considera que es necesario el monitoreo constante de los activos de tecnología de información, a fin de optimizar los procesos con mayor eficiencia?	
		Mejora continua	23	¿Es necesario disponer con un plan de continuidad de servicio para la gestión de TI,	
			24	¿Se optimizan los procesos de gestión de TI, a través de herramientas tecnologías que ayudan al usuario final?	
	Operación de servicio	Diseño	25	¿Los niveles de escalamiento de los problemas de gestión de TI, son claros para todos los usuarios?	

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Cuesta (2020), menciona que la operación de servicio es una práctica de gestión de TI, basado en la generación de valor y control de eventos críticos en relación a los temas de prestación de servicio de tecnología la cual permitirá implementar un modelo adecuado para la gestión de servicios a nivel gerencial.		26	¿Se dispone de un catálogo de servicio entendible de todos los aspectos técnico de los servicios de TI?	
		Transición	27	¿Se dispone procedimientos para la gestión de cambios y puesta en producción alguna herramienta tecnológica en la institución?	
			28	¿Se comunica los cambios efectuados, con respecto a la gestión y operación de servicio de TI?	
		Mejora continua	29	¿En su opinión existen mejoras de servicio en los procesos de tecnología de información, que le ayuda a agilizar su actividad laboral?	
			30	¿Considera que se establecen y priorizan las mejoras a implementar en la gestión de TI?	
	Continuidad de servicio	Planificación	31	¿Se organiza de manera eficiente toda ejecución de los procesos de control en la gestión de TI?	
			32	¿Se establecen brechas y priorizan los procesos de ejecución de los servicios de TI en la institución?	

TITULO: Ciberseguridad y su incidencia en la gestión de tecnologías de información en una Institución Administradora de Fondos de Aseguramiento en Salud, Lima 2022

AUTOR: AMPELIO JUAN DE MATA MALLQUI MALLQUI

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Piñuela y Quito (2020), consideran que la continuidad de servicio es un proceso fundamental para alcanzar un alto nivel de eficiencia, mejorar la productividad en la organización para maximizar el valor para el cliente	Evaluación	33	¿Constantemente se priorizan las mejoras en la gestión de TI, las cuales son alineadas a los objetivos de la institución?	
			34	¿Todos los cambios en la gestión de TI, son parametrizados para su evaluación conjunta con el área especializado?	
		Control de correcciones	35	¿Considera que existe controles de cambios para mejorar los procesos de Gestión de TI?	
			36	¿Las políticas de contingencia son revisadas y actualizadas para mejorar los procesos de gestión de TI?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para los Servidores de la Institución Administradora de Fondos de Aseguramiento en Salud

Fecha: [/ /]

Sexo: Femenino [ ] Masculino[ ]

Cargo: Asistente [ ] Especialista [ ] Coordinador/Jefe [ ] Gerente [ ]

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo con el siguiente ejemplo: Totalmente en desacuerdo (1), En desacuerdo (2), Ni deacuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5).

N°	Pregunta	Valoración				
		1	2	3	4	5
	Ciberseguridad					
1	¿Cree usted, que en la institución se debería mejorar políticas de seguridad de información, para evitar la ciberdelincuencia?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
2	¿Considera que es necesario la implementación de un plan de gestión de ciberseguridad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
3	¿Constantemente se socializa, los planes de mejora y/o aplicación de controles para contrarrestar la ciberdelincuencia?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
4	¿Tiene conocimiento, si la institución cuenta con herramientas tecnológicas para evitar la ciberdelincuencia?	Muy poco	Poco	Regular	Bastante	Demasiado
5	¿La institución tiene planes y estrategias de seguridad para evitar ciberataques?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
6	¿Considera que el personal de la Oficina General de Tecnología de Información – OGTI, está capacitado para dar respuesta ante cualquier ciberataque?	Muy poco	Poco	Regular	Bastante	Demasiado
7	¿Se tiene identificado los procesos críticos a nivel de infraestructura tecnología?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
8	¿Está de acuerdo con la implementación de tecnologías para analizar y detectar intrusos o ciberdelincuentes?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
9	¿La institución dispone con políticas de seguridad de control acceso actualizado, para prevenir algún acto ilícito o robo de información?	Muy poco	Poco	Regular	Bastante	Demasiado
10	¿Considera que los mecanismos de seguridad de control acceso a la institución con videocámaras, son efectivas?	Nunca	Casi nunca	A veces	Siempre	Casi siempre

N°	Pregunta	Valoración				
		1	2	3	4	5
11	¿Cree usted que la Oficina General de Tecnología de Información, está preparado a nivel infraestructura tecnológica para dar respuesta un ciberataque?	Muy poco	Poco	Regular	Bastante	Demasiado
12	¿Se monitorea los mecanismos de seguridad para brindar acceso de información al personal interno y externo?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
13	¿Cree que se está aplicando controles de la ciberseguridad a los usuarios que acceden a los sistemas de información?	Muy poco	Poco	Regular	Bastante	Demasiado
14	¿En los 3 últimos meses, usted tenido alguna sospecha de un ataque cibernético, con los accesos que cuenta en la institución?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
15	¿Considera que la Oficina de General Tecnología de Información tiene planes de contingencia en caso de un ciberataque?	Muy poco	Poco	Regular	Bastante	Demasiado
16	¿Son eficientes los controles de seguridad aplicados en la institución para prevenir la ciberseguridad?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
17	¿Con que frecuencia se elaboran nuevas estrategias y/o políticas de seguridad, enmarcado en la ciberseguridad?	Muy raramente	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente
18	¿Se socializa los resultados de la Oficina General de Tecnología de Información, para mejorar la ciberseguridad?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
	Gestión de Tecnologías de Información					
19	¿Se comunica oportunamente los planes de acción para el mejoramiento de servicios de tecnología de información, alineadas a los objetivos de la institución?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
20	¿La ejecución de los procesos core del negocio están implementados a través de herramientas tecnológicas, para su gestión, administración y toma de decisiones?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
21	¿Se analizan y verifican controles de seguridad para la gestión de planes de servicios de TI?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
22	¿Considera que es necesario el monitoreo constante de los activos de tecnología de información, a fin de optimizar los procesos con mayor eficiencia?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
23	¿Es necesario disponer con un plan de continuidad de servicio para la gestión de TI,	Nunca	Casi nunca	A veces	Siempre	Casi siempre
24	¿Se optimizan los procesos de gestión de TI, a través de herramientas tecnologías que ayudan al usuario final?	Nunca	Casi nunca	A veces	Siempre	Casi siempre

N°	Pregunta	Valoración				
		1	2	3	4	5
25	¿Los niveles de escalamiento de los problemas de gestión de TI, son claros para todos los usuarios?	Muy raramente	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente
26	¿Se dispone de un catálogo de servicio entendible de todos los aspectos técnico de los servicios de TI?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
27	¿Se dispone procedimientos para la gestión de cambios y puesta en producción alguna herramienta tecnológica en la institución?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
28	¿Se comunica los cambios efectuados, con respecto a la gestión y operación de servicio de TI?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
29	¿En su opinión existen mejoras de servicio en los procesos de tecnología de información, que le ayuda a agilizar su actividad laboral?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
30	¿Considera que se establecen y priorizan las mejoras de servicio a implementar en la gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
31	¿Se organiza de manera eficiente toda ejecución de los procesos de control en la gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
32	¿Se establecen brechas y priorizan los procesos de ejecución de los servicios de TI en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
33	¿Constantemente se priorizan las mejoras en la gestión de TI, las cuales son alineadas a los objetivos de la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
34	¿Todos los cambios en la gestión de TI, son parametrizados para su evaluación conjunta con el área especializado?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
35	¿Considera que existen controles de cambios para mejorar los procesos de Gestión de TI?	Nunca	Casi nunca	A veces	Siempre	Casi siempre
36	¿Las políticas de contingencia son revisadas y actualizadas para mejorar los procesos de gestión de TI?	Muy raramente	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente

¡Gracias por su tiempo!

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

Validación del Experto N°1

Variable Independiente: Ciberseguridad

N°	DIMENSIONES / Ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Estrategias de Seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Cree usted, que en la institución se debería mejorar políticas de seguridad de información, para evitar la ciberdelincuencia?	X		X		X		
2	¿Considera que es necesario la implementación de un plan de gestión de ciberseguridad?	X		X		X		
3	¿Constantemente se socializa, los planes de mejora y/o aplicación de controles para contrarrestar la ciberdelincuencia?	X		X		X		
4	¿Tiene conocimiento, si la institución cuenta con herramientas tecnológicas para evitar la ciberdelincuencia?	X		X		X		
5	¿La institución tiene planes y estrategias de seguridad para evitar ciberataques?	X		X		X		
6	¿Considera que el personal de la Oficina General de Tecnología de Información – OGTI, está capacitado para dar respuesta ante cualquier ciberataque?	X		X		X		
	Protección de infraestructura crítica	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se tiene identificado los procesos críticos a nivel de infraestructura tecnología?	X		X		X		
8	¿Está de acuerdo con la implementación de tecnologías para analizar y detectar intrusos o ciberdelincuentes?	X		X		X		
9	¿La institución dispone con políticas de seguridad de control acceso actualizado, para prevenir algún acto ilícito o robo de información?	X		X		X		
10	¿Considera que los mecanismos de seguridad de control acceso a la institución con videocámaras, son efectivas?	X		X		X		
11	¿Cree usted que la Oficina General de Tecnología de Información, está preparado a nivel infraestructura tecnológica para dar respuesta un ciberataque?	X		X		X		
12	¿Se monitorea los mecanismos de seguridad para brindar acceso de información al personal interno y externo?	X		X		X		
	Control técnico de seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Cree que se está aplicando controles de la ciberseguridad a los usuarios que acceden a los sistemas de información?	X		X		X		
14	¿En los 3 últimos meses, usted tenido alguna sospecha de un ataque cibernético, con los accesos que cuenta en la institución?	X		X		X		
15	¿Considera que la Oficina de General Tecnología de Información tiene un plan de contingencia en caso de un ciberataque?	X		X		X		
16	¿Son eficientes los controles de seguridad aplicados en la institución para prevenir la ciberseguridad?	X		X		X		
17	¿Con que frecuencia se elaboran nuevas estrategias y/o políticas de seguridad, enmarcado en la ciberseguridad?	X		X		X		
18	¿Se socializa los resultados de la Oficina General de Tecnología de Información, para mejorar la ciberseguridad?	X		X		X		

Firmado digitalmente por:
LEZAMA GONZALES PEDRO
MARTIN FIR 09656793 hard
Motivo: Soy el autor del
documento
Fecha: 17/05/2022 16:29:51-0500

Variable dependiente: Gestión de tecnologías de información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Estratégica de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Se comunica oportunamente los planes de acción para el mejoramiento de servicios de tecnología de información, alineadas a los objetivos de la institución?	X		X		X		
20	¿La ejecución de los procesos Core del negocio están implementados a través de herramientas tecnológicas, para su gestión, administración y toma de decisiones?	X		X		X		
21	¿Se analizan y verifican controles de seguridad para la gestión de planes de servicios de TI.?	X		X		X		
22	¿Considera que es necesario el monitoreo constante de los activos de tecnología de información, a fin de optimizar los procesos con mayor eficiencia?	X		X		X		
23	¿Es necesario disponer con un plan de continuidad de servicio para la gestión de TI.	X		X		X		
24	¿Se optimizan los procesos de gestión de TI, a través de herramientas tecnologías que ayudan al usuario final?	X		X		X		
	Operación de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Los niveles de escalamiento de los problemas de gestión de TI, son claros para todos los usuarios?	X		X		X		
26	¿Se dispone de un catálogo de servicio entendible de todos los aspectos técnico de los servicios de TI?	X		X		X		
27	¿Se dispone procedimientos para la gestión de cambios y puesta en producción alguna herramienta tecnológica en la institución?	X		X		X		
28	¿Se comunica los cambios efectuados, con respecto a la gestión y operación de servicio de TI?	X		X		X		
29	¿En su opinión existen mejoras de servicio en los procesos de tecnología de información, que le ayuda a agilizar su actividad laboral?	X		X		X		
30	¿Considera que se establecen y priorizan las mejoras a implementar en la gestión de TI?	X		X		X		
	Continuidad de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Se organiza de manera eficiente toda ejecución de los procesos de control en la gestión de TI?	X		X		X		
32	¿Se establecen brechas y priorizan los procesos de ejecución de los servicios de TI en la institución?	X		X		X		
33	¿Constantemente se priorizan las mejoras en la gestión de TI, las cuales son alineadas a los objetivos de la institución?	X		X		X		
34	¿Todos los cambios en la gestión de TI, son parametrizados para su evaluación conjunta con el área especializado?	X		X		X		
35	¿Considera que existe controles de cambios para mejorar los procesos de gestión de TI?	X		X		X		
36	¿Las políticas de contingencia son revisadas y actualizadas para mejorar los procesos de gestión de TI?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombre s del juez evaluador: Pedro Martin Lezama Gonzales **DNI: 09656793**

Especialista: Metodólogo [X] **Temático [ ]**

Grado: Maestro [ ] **Doctor [X]**

Fecha: 17 de mayo del 2022

FIRMA DIGITAL

Firmado digitalmente por: LEZAMA GONZALES PEDRO MARTIN FIR 09656793 hard
Motivo: Soy el autor del documento
Fecha: 17/05/2022 16:31:08-0500

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 Independiente: Ciberseguridad

N°	DIMENSIONES / Ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Estrategias de Seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Cree usted, que en la institución se debería mejorar políticas de seguridad de información, para evitar la ciberdelincuencia?	X		X		X		
2	¿Considera que es necesario la implementación de un plan de gestión de ciberseguridad?	X		X		X		
3	¿Constantemente se socializa, los planes de mejora y/o aplicación de controles para contrarrestar la ciberdelincuencia?	X		X		X		
4	¿Tiene conocimiento, si la institución cuenta con herramientas tecnológicas para evitar la ciberdelincuencia?	X		X		X		
5	¿La institución tiene planes y estrategias de seguridad para evitar ciberataques?	X		X		X		
6	¿Considera que el personal de la Oficina General de Tecnología de Información – OGTI, está capacitado para dar respuesta ante cualquier ciberataque?	X		X		X		
	Protección de infraestructura crítica	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se tiene identificado los procesos críticos a nivel de infraestructura tecnología?	X		X		X		
8	¿Está de acuerdo con la implementación de tecnologías para analizar y detectar intrusos o ciberdelincuentes?	X		X		X		
9	¿La institución dispone con políticas de seguridad de control acceso actualizado, para prevenir algún acto ilícito o robo de información?	X		X		X		
10	¿Considera que los mecanismos de seguridad de control acceso a la institución con videocámaras, son efectivas?	X		X		X		
11	¿Cree usted que la Oficina General de Tecnología de Información, está preparado a nivel infraestructura tecnológica para dar respuesta un ciberataque?	X		X		X		
12	¿Se monitorea los mecanismos de seguridad para brindar acceso de información al personal interno y externo?	X		X		X		
	Control técnico de seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Cree que se está aplicando controles de la ciberseguridad a los usuarios que acceden a los sistemas de información?	X		X		X		
14	¿En los 3 últimos meses, usted tenido alguna sospecha de un ataque cibernético, con los accesos que cuenta en la institución?	X		X		X		
15	¿Considera que la Oficina de General Tecnología de Información tiene un plan de contingencia en caso de un ciberataque?	X		X		X		
16	¿Son eficientes los controles de seguridad aplicados en la institución para prevenir la ciberseguridad?	X		X		X		
17	¿Con que frecuencia se elaboran nuevas estrategias y/o políticas de seguridad, enmarcado en la ciberseguridad?	X		X		X		
18	¿Se socializa los resultados de la Oficina General de Tecnología de Información, para mejorar la ciberseguridad?	X		X		X		

Variable dependiente: Gestión de tecnologías de información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Estratégica de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Se comunica oportunamente los planes de acción para el mejoramiento de servicios de tecnología de información, alineadas a los objetivos de la institución?	X		X		X		
20	¿La ejecución de los procesos Core del negocio están implementados a través de herramientas tecnológicas, para su gestión, administración y toma de decisiones?	X		X		X		
21	¿Se analizan y verifican controles de seguridad para la gestión de planes de servicios de TI.?	X		X		X		
22	¿Considera que es necesario el monitoreo constante de los activos de tecnología de información, a fin de optimizar los procesos con mayor eficiencia?	X		X		X		
23	¿Es necesario disponer con un plan de continuidad de servicio para la gestión de TI,	X		X		X		
24	¿Se optimizan los procesos de gestión de TI, a través de herramientas tecnologías que ayudan al usuario final?	X		X		X		
	Operación de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Los niveles de escalamiento de los problemas de gestión de TI, son claros para todos los usuarios?	X		X		X		
26	¿Se dispone de un catálogo de servicio entendible de todos los aspectos técnico de los servicios de TI?	X		X		X		
27	¿Se dispone procedimientos para la gestión de cambios y puesta en producción alguna herramienta tecnológica en la institución?	X		X		X		
28	¿Se comunica los cambios efectuados, con respecto a la gestión y operación de servicio de TI?	X		X		X		
29	¿En su opinión existen mejoras de servicio en los procesos de tecnología de información, que le ayuda a agilizar su actividad laboral?	X		X		X		
30	¿Considera que se establecen y priorizan las mejoras a implementar en la gestión de TI?	X		X		X		
	Continuidad de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Se organiza de manera eficiente toda ejecución de los procesos de control en la gestión de TI?	X		X		X		
32	¿Se establecen brechas y priorizan los procesos de ejecución de los servicios de TI en la institución?	X		X		X		
33	¿Constantemente se priorizan las mejoras en la gestión de TI, las cuales son alineadas a los objetivos de la institución?	X		X		X		
34	¿Todos los cambios en la gestión de TI, son parametrizados para su evaluación conjunta con el área especializado?	X		X		X		
35	¿Considera que existe controles de cambios para mejorar los procesos de gestión de TI?	X		X		X		
36	¿Las políticas de contingencia son revisadas y actualizadas para mejorar los procesos de gestión de TI?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

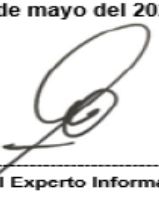
Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombre s del juez evaluador: Marlon Frank Acuña Benites **DNI: 42097456**

Especialista: Metodólogo [ ] Temático [X]

Grado: Maestro [ ] Doctor [X]

Fecha: 19 de mayo del 2022



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 Independiente: Ciberseguridad

N°	DIMENSIONES / Ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Estrategias de Seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Cree usted, que en la institución se debería mejorar políticas de seguridad de información, para evitar la ciberdelincuencia?	X		X		X		
2	¿Considera que es necesario la implementación de un plan de gestión de ciberseguridad?	X		X		X		
3	¿Constantemente se socializa, los planes de mejora y/o aplicación de controles para contrarrestar la ciberdelincuencia?	X		X		X		
4	¿Tiene conocimiento, si la institución cuenta con herramientas tecnológicas para evitar la ciberdelincuencia?	X		X		X		
5	¿La institución tiene planes y estrategias de seguridad para evitar ciberataques?	X		X		X		
6	¿Considera que el personal de la Oficina General de Tecnología de Información – OGTI, está capacitado para dar respuesta ante cualquier ciberataque?	X		X		X		
	Protección de infraestructura crítica	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se tiene identificado los procesos críticos a nivel de infraestructura tecnología?	X		X		X		
8	¿Está de acuerdo con la implementación de tecnologías para analizar y detectar intrusos o ciberdelincuentes?	X		X		X		
9	¿La institución dispone con políticas de seguridad de control acceso actualizado, para prevenir algún acto ilícito o robo de información?	X		X		X		
10	¿Considera que los mecanismos de seguridad de control acceso a la institución con videocámaras, son efectivas?	X		X		X		
11	¿Cree usted que la Oficina General de Tecnología de Información, está preparado a nivel infraestructura tecnológica para dar respuesta un ciberataque?	X		X		X		
12	¿Se monitorea los mecanismos de seguridad para brindar acceso de información al personal interno y externo?	X		X		X		
	Control técnico de seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Cree que se está aplicando controles de la ciberseguridad a los usuarios que acceden a los sistemas de información?	X		X		X		
14	¿En los 3 últimos meses, usted tenido alguna sospecha de un ataque cibernético, con los accesos que cuenta en la institución?	X		X		X		
15	¿Considera que la Oficina de General Tecnología de Información tiene un plan de contingencia en caso de un ciberataque?	X		X		X		
16	¿Son eficientes los controles de seguridad aplicados en la institución para prevenir la ciberseguridad?	X		X		X		
17	¿Con que frecuencia se elaboran nuevas estrategias y/o políticas de seguridad, enmarcado en la ciberseguridad?	X		X		X		
18	¿Se socializa los resultados de la Oficina General de Tecnología de Información, para mejorar la ciberseguridad?	X		X		X		

Firmado digitalmente por:
QUIROZ ANGULO Christian
Janderson FAU 20492066658 soft
Motivo: Soy el autor del
documento
Fecha: 17/05/2022 16:53:01-0500

Variable dependiente: Gestión de tecnologías de información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Estratégica de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Se comunica oportunamente los planes de acción para el mejoramiento de servicios de tecnología de información, alineadas a los objetivos de la institución?	X		X		X		
20	¿La ejecución de los procesos Core del negocio están implementados a través de herramientas tecnológicas, para su gestión, administración y toma de decisiones?	X		X		X		
21	¿Se analizan y verifican controles de seguridad para la gestión de planes de servicios de TI.?	X		X		X		
22	¿Considera que es necesario el monitoreo constante de los activos de tecnología de información, a fin de optimizar los procesos con mayor eficiencia?	X		X		X		
23	¿Es necesario disponer con un plan de continuidad de servicio para la gestión de TI,	X		X		X		
24	¿Se optimizan los procesos de gestión de TI, a través de herramientas tecnologías que ayudan al usuario final?	X		X		X		
	Operación de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Los niveles de escalamiento de los problemas de gestión de TI, son claros para todos los usuarios?	X		X		X		
26	¿Se dispone de un catálogo de servicio entendible de todos los aspectos técnico de los servicios de TI?	X		X		X		
27	¿Se dispone procedimientos para la gestión de cambios y puesta en producción alguna herramienta tecnológica en la institución?	X		X		X		
28	¿Se comunica los cambios efectuados, con respecto a la gestión y operación de servicio de TI?	X		X		X		
29	¿En su opinión existen mejoras de servicio en los procesos de tecnología de información, que le ayuda a agilizar su actividad laboral?	X		X		X		
30	¿Considera que se establecen y priorizan las mejoras a implementar en la gestión de TI?	X		X		X		
	Continuidad de servicio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Se organiza de manera eficiente toda ejecución de los procesos de control en la gestión de TI?	X		X		X		
32	¿Se establecen brechas y priorizan los procesos de ejecución de los servicios de TI en la institución?	X		X		X		
33	¿Constantemente se priorizan las mejoras en la gestión de TI, las cuales son alineadas a los objetivos de la institución?	X		X		X		
34	¿Todos los cambios en la gestión de TI, son parametrizados para su evaluación conjunta con el área especializado?	X		X		X		
35	¿Considera que existe controles de cambios para mejorar los procesos de gestión de TI?	X		X		X		
36	¿Las políticas de contingencia son revisadas y actualizadas para mejorar los procesos de gestión de TI?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFIENCIA

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

Fecha: 17 de mayo del 2022

Apellidos y nombre s del juez evaluador: Quiroz Angulo, Christian Janderson **DNI: 42385497**

Especialista: Metodólogo [ ] **Temático [X]**

Grado: Maestro [X] **Doctor [ ]**

[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

Firmado digitalmente por: QUIROZ ANGULO Christian Janderson FAU 20492966658 soft
Motivo: Soy el autor del documento
Fecha: 17/05/2022 16:53:01-0500

Firma del Experto Informante

Anexo 5: Base de datos

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
1	2	1	5	5	3	3	3	3	4	5	1	1	2	4	4	1	2	1	1	1	2	2	2	1	4	2	1	2	2	2	1	1	1	2	2	1	2	2
2	2	2	5	5	3	3	3	4	4	5	3	4	3	4	4	1	4	4	1	2	2	3	3	4	5	4	4	4	3	2	4	2	2	2	2	2	5	2
3	2	2	5	5	1	1	3	3	4	5	2	3	2	1	4	1	1	1	1	1	2	5	2	5	4	2	2	1	2	4	2	1	1	2	1	1	1	1
4	2	2	5	5	3	3	4	3	3	5	3	5	2	1	4	2	2	3	1	1	2	4	3	5	5	3	3	2	3	3	3	5	4	5	5	4	4	3
5	1	1	5	5	1	1	3	4	4	5	4	3	4	5	3	1	2	3	2	3	1	3	3	5	5	3	4	3	1	1	5	1	4	4	4	4	3	2
6	1	1	4	4	3	1	3	3	4	4	2	1	1	5	5	1	1	3	3	2	3	3	4	1	5	3	3	2	3	3	2	5	3	3	3	5	3	5
7	2	2	5	4	5	1	4	3	4	5	4	3	2	5	5	1	3	4	5	4	3	2	1	5	5	3	4	3	5	4	5	5	4	3	4	3	4	4
8	1	2	5	4	3	3	3	3	4	5	3	3	3	5	3	2	5	5	3	2	4	4	4	3	5	3	4	3	4	4	4	3	4	3	4	5	4	5
9	2	2	4	4	3	4	3	3	4	5	5	4	4	5	3	5	4	4	4	5	3	4	5	4	5	4	5	5	4	5	4	5	4	4	5	5	5	4
10	2	2	4	5	3	3	4	4	4	5	3	5	5	5	3	2	4	1	4	5	4	4	3	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5
11	2	2	5	4	3	4	4	3	3	5	4	4	5	5	5	5	3	2	4	3	3	3	3	3	3	4	4	2	3	4	4	4	3	4	5	5	3	5
12	2	2	5	5	1	3	4	3	4	5	3	3	3	5	5	1	3	1	3	3	4	5	5	2	5	1	4	4	4	4	5	5	4	4	1	5	5	5
13	1	2	5	5	3	4	3	4	4	5	3	5	3	5	3	5	5	4	4	3	3	4	5	5	5	4	4	5	4	5	5	4	4	4	5	5	3	5
14	2	2	4	4	5	3	4	4	4	5	4	3	5	5	5	4	3	3	4	3	3	4	3	4	2	4	3	4	5	4	5	2	4	4	5	5	5	5
15	2	2	4	5	3	1	3	3	4	5	4	3	4	3	3	1	5	5	3	4	5	5	3	5	3	4	4	4	3	4	4	5	4	4	5	5	5	5
16	2	2	5	5	3	1	3	3	4	5	4	3	3	5	5	3	3	3	3	1	4	2	5	4	5	3	5	4	4	3	4	5	4	4	2	5	5	5
17	1	2	4	4	3	1	4	3	4	5	3	3	4	5	5	5	5	5	3	4	4	3	3	3	5	4	5	5	4	5	5	4	4	4	3	5	4	5
18	1	2	5	5	3	4	4	3	3	5	3	2	3	5	5	3	2	4	4	4	3	5	1	4	5	5	5	5	4	4	4	5	5	5	5	5	4	5
19	1	1	5	4	3	1	4	3	4	5	4	4	3	5	3	2	3	5	3	2	4	5	4	5	3	5	5	1	3	3	4	3	4	4	5	2	1	5
20	1	1	4	4	1	1	4	3	3	5	3	4	3	5	5	1	3	3	3	2	3	3	4	5	1	1	5	5	4	4	3	5	4	4	2	5	5	5
21	2	1	5	5	3	3	4	3	5	5	4	5	4	5	5	2	5	4	4	5	3	5	4	5	5	5	5	5	5	5	5	3	4	5	5	5	5	5
22	1	1	4	4	3	1	3	3	3	5	3	5	3	5	5	1	3	5	4	3	4	3	5	5	5	3	5	5	5	5	5	2	4	4	3	5	5	5
23	1	1	4	4	3	3	4	3	4	5	4	4	3	5	3	4	3	2	4	3	4	5	4	5	5	3	5	5	5	4	5	5	4	5	5	5	5	5
24	2	2	4	4	3	1	3	3	3	5	4	5	4	5	5	3	4	4	4	4	4	3	4	5	5	5	5	5	5	5	4	5	3	4	5	5	3	5
25	2	1	5	5	3	4	4	3	3	5	3	4	2	5	3	2	5	4	4	4	4	5	4	5	3	5	5	5	5	5	3	5	3	4	1	5	3	5

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
26	2	1	4	4	3	1	3	3	3	5	3	4	2	5	5	2	4	5	4	3	4	5	4	5	5	5	2	5	5	5	4	5	4	4	5	5	5	5
27	2	1	4	4	3	1	3	3	3	5	3	4	2	5	4	2	4	5	4	3	4	5	4	5	5	5	2	3	5	5	4	5	4	4	5	5	5	5
28	2	1	5	4	3	3	3	3	3	5	4	4	4	5	4	3	3	5	4	3	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5
29	1	4	5	5	3	3	4	3	4	5	2	4	3	5	4	3	4	3	4	3	4	3	4	5	2	3	5	3	5	5	2	5	4	4	5	5	5	5
30	2	2	4	4	3	4	4	3	4	4	4	4	4	5	3	3	5	3	3	3	4	5	4	5	3	5	5	5	5	5	5	5	4	4	5	5	5	5
31	1	2	4	4	3	3	3	3	4	5	4	4	4	5	4	2	3	3	3	3	4	5	4	5	3	5	5	5	5	5	5	5	3	4	5	5	3	5
32	2	2	5	4	3	1	3	3	4	5	4	4	3	5	4	3	3	4	4	4	3	3	4	5	5	5	5	5	2	5	3	5	5	4	5	5	5	3
33	1	2	4	4	3	3	3	3	3	5	3	1	3	5	4	1	3	3	4	4	4	3	4	5	3	5	5	5	5	5	5	4	5	4	5	5	5	5
34	2	2	5	4	3	1	2	3	4	5	4	4	4	5	4	4	2	3	4	3	4	5	5	5	5	5	5	3	5	5	5	5	4	4	4	5	5	5
35	1	2	5	4	3	3	3	3	4	5	4	4	3	5	4	1	5	4	4	4	4	5	5	5	5	5	5	5	5	5	4	5	4	4	4	5	5	5
36	2	2	5	4	3	1	4	3	4	4	3	4	4	5	3	5	5	5	3	4	4	5	5	5	5	5	5	5	4	5	5	5	5	4	4	5	5	5
37	2	2	5	5	3	3	3	4	3	5	1	4	2	5	4	1	3	2	3	3	4	5	5	5	4	4	1	5	4	5	5	5	5	4	5	5	5	3
38	2	3	4	5	3	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	2	5	5	5	3	4	4	4	5	5	5	5	4	5	5	5	3
39	2	1	4	4	5	5	5	5	5	5	4	5	4	5	4	4	4	4	5	5	4	5	3	5	2	3	4	4	4	5	4	5	4	2	2	5	5	5
40	2	3	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	2	5	5	5	5	2	5	5	5	5	5	5	5
41	2	2	3	3	2	5	3	5	5	5	5	5	4	5	3	5	4	4	3	5	5	5	3	3	5	5	3	5	5	5	5	5	5	5	5	5	5	5
42	1	2	3	3	4	4	3	5	5	5	5	5	5	5	4	4	4	5	4	5	5	5	3	3	5	5	5	5	3	5	5	5	5	5	5	5	5	5
43	1	2	3	3	2	4	2	4	2	2	2	2	2	1	2	2	3	2	3	3	4	4	3	2	4	4	4	4	2	2	4	4	4	4	4	4	3	4
44	2	1	4	3	3	3	3	3	3	3	3	5	4	4	3	4	3	3	3	3	3	3	3	3	3	3	4	4	2	4	5	4	4	4	4	4	4	4
45	2	2	3	3	2	2	2	4	3	5	5	5	4	4	4	3	2	2	2	4	4	4	1	1	4	4	4	4	3	4	5	5	5	4	4	4	4	3
46	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
47	2	2	3	3	2	2	2	4	3	3	5	5	1	1	3	4	3	2	3	3	4	2	2	2	3	4	4	4	2	4	4	4	3	4	4	3	4	4
48	1	1	1	1	1	1	1	1	1	1	1	5	3	3	1	1	1	1	2	2	2	1	1	1	1	2	3	3	3	4	4	4	4	3	4	3	3	2
49	1	2	1	1	1	1	2	3	2	3	4	4	4	4	2	3	1	1	1	2	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
50	2	2	1	1	1	1	1	1	3	3	3	2	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4	4	4	4	4	4	2
51	2	3	4	4	2	2	3	3	2	3	3	2	3	2	3	4	2	1	2	3	3	2	2	2	4	4	4	3	3	4	4	3	5	4	5	4	4	4
52	2	3	2	3	3	5	4	5	5	5	5	5	5	5	3	4	2	2	3	5	4	4	2	3	4	4	4	4	3	4	4	4	4	4	4	4	4	4

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
53	2	2	4	4	4	4	3	4	5	5	5	5	4	4	3	4	3	1	3	4	4	4	1	3	3	3	4	4	4	4	4	4	4	4	3	4	4	4
54	2	2	4	4	4	5	4	5	4	5	5	5	4	4	5	5	4	5	4	5	5	5	3	3	5	5	5	5	4	4	5	5	5	5	5	4	4	5
55	2	1	3	3	3	3	3	3	3	3	3	3	3	3	4	4	3	3	3	3	4	4	3	3	4	3	4	4	4	4	3	4	4	4	3	4	4	4
56	2	2	5	5	4	5	4	5	4	5	4	4	5	4	5	4	4	4	5	4	4	5	5	5	5	5	5	5	4	5	5	4	5	4	5	5	4	5
57	2	2	3	5	5	4	5	4	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5	4	5	5	4	5	4	5	4	5	4	4	5	5	4	4
58	2	1	4	5	5	4	3	4	5	5	5	4	3	4	4	5	5	4	5	5	4	5	5	5	4	5	5	5	5	5	5	4	5	4	5	5	5	5
59	2	2	5	5	4	4	4	5	5	4	5	5	4	4	5	4	5	5	4	5	5	5	4	4	5	4	5	4	5	5	5	4	4	5	5	5	4	5
60	1	2	5	5	4	5	4	5	4	5	4	4	4	5	4	5	4	5	5	4	4	5	4	5	5	5	4	5	4	5	5	5	4	5	4	5	4	4
61	1	2	5	4	4	5	5	4	4	5	4	4	5	4	5	4	5	4	5	4	5	5	5	4	4	4	5	4	5	5	4	5	4	5	4	5	5	4
62	2	1	5	4	4	5	5	5	4	4	5	5	4	4	4	4	4	4	4	4	5	4	5	4	5	4	4	5	5	5	4	5	5	4	5	4	5	4
63	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	5	5	5	5	5	5	5
64	2	1	4	4	4	4	4	4	4	4	5	5	5	5	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
65	2	1	3	3	2	3	3	4	3	4	3	3	3	3	4	4	3	3	2	3	4	3	3	3	4	4	4	3	2	4	4	4	4	4	4	4	4	4
66	2	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	3	3	3	2	5	3	5	3	3	4	4	2	4	4	4	4	4	4
67	2	3	3	3	4	4	4	4	4	5	5	5	1	1	3	4	4	3	3	4	4	4	2	2	3	3	4	4	4	4	5	5	5	4	4	4	4	4
68	2	2	3	3	3	3	3	4	3	4	4	4	3	3	4	4	3	3	3	3	4	4	3	3	4	4	4	4	4	2	4	4	4	4	4	4	4	4
69	2	1	2	5	4	5	4	5	5	5	5	5	4	4	5	4	4	4	3	3	4	4	4	4	4	4	4	4	5	4	5	3	4	4	3	4	4	4
70	1	2	3	3	2	5	2	5	4	4	2	4	3	4	5	5	4	1	3	3	5	5	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5
71	1	1	3	3	3	3	2	4	4	3	3	3	3	3	4	4	3	4	3	3	4	4	2	2	4	4	4	4	4	4	4	4	4	4	3	3	3	3
72	2	1	2	2	2	5	2	5	4	5	5	5	4	5	4	4	2	2	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
73	1	1	4	4	3	4	3	3	4	5	5	5	4	4	4	4	3	2	2	2	4	5	2	2	4	4	5	4	3	4	4	3	4	4	4	2	3	3
74	2	1	2	2	2	3	3	3	3	3	3	3	3	3	4	4	3	3	3	3	3	4	4	2	4	3	4	4	4	3	4	3	3	3	3	4	4	4
75	2	1	1	1	3	3	3	3	3	3	5	5	4	5	4	4	3	3	3	5	5	5	3	3	4	4	4	4	3	4	4	4	4	4	3	4	4	4
76	1	2	4	3	5	5	4	5	5	5	5	5	5	1	5	5	3	4	4	5	4	3	3	3	5	5	4	2	3	4	5	5	5	5	5	4	4	3
77	2	2	3	3	5	5	5	5	5	5	5	5	3	3	4	5	3	4	4	4	5	3	3	3	4	4	4	4	4	4	4	5	5	5	4	3	4	4
78	1	2	3	3	4	4	4	5	4	5	5	5	4	4	4	4	4	4	4	4	5	5	3	3	5	5	5	5	5	5	5	3	5	5	5	5	5	5
79	1	2	1	1	1	1	1	1	1	1	1	1	1	1	4	4	1	1	1	1	4	4	1	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
80	1	2	5	5	3	5	5	4	4	5	1	3	5	4	5	3	4	5	5	4	5	4	3	3	5	3	5	5	3	5	3	5	5	5	3	5	5	3
81	2	3	5	5	5	5	5	5	4	4	1	4	4	4	5	5	5	4	3	5	5	4	5	3	5	3	5	5	3	5	4	4	5	5	5	5	5	5
82	2	2	5	5	5	5	5	5	5	5	3	4	5	5	5	5	5	5	3	5	5	4	3	3	5	3	5	5	3	5	5	5	5	5	5	5	5	5
83	2	1	5	5	5	3	3	4	4	4	3	4	5	4	4	3	4	5	1	5	3	4	5	5	5	3	5	5	3	4	5	5	5	5	5	5	5	5
84	1	1	4	4	5	4	4	5	5	4	4	4	5	5	5	4	4	4	3	5	5	4	4	5	5	3	5	5	3	5	4	4	5	5	5	5	4	5
85	2	1	5	5	5	5	5	4	5	5	5	3	5	5	4	5	5	4	5	5	5	4	5	5	5	3	5	5	3	5	5	5	5	5	3	5	5	5
86	2	2	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	5	3	5	5	4	4	5	5	3	5	5	3	5	4	4	5	4	5	5	4	5
87	2	2	5	5	5	5	5	5	5	4	1	4	5	5	4	5	4	5	5	5	5	4	5	5	5	3	5	3	3	5	5	5	5	4	5	5	5	5
88	2	2	5	5	3	5	5	5	5	4	5	3	4	5	4	5	5	5	5	4	5	3	4	4	5	3	5	5	5	5	4	4	5	4	3	5	5	5
89	1	2	5	5	3	3	4	4	4	4	2	3	5	5	5	3	5	5	2	4	5	3	5	4	5	3	5	5	5	5	5	5	5	4	5	5	5	5
90	1	1	4	4	5	4	4	4	5	5	4	4	5	5	5	4	4	5	5	5	5	3	4	4	5	3	5	5	5	5	5	5	5	4	5	5	5	5
91	2	1	4	4	3	4	4	5	5	4	4	3	5	5	5	4	5	5	5	3	5	3	4	4	5	3	5	5	2	5	4	4	5	4	5	5	5	5
92	2	1	5	5	3	3	3	5	5	4	2	3	5	5	5	3	5	5	2	3	5	3	4	4	5	5	5	3	2	5	5	5	5	4	5	5	5	5
93	2	1	5	5	3	3	3	4	5	5	2	3	5	5	5	3	4	5	3	3	5	3	5	5	5	5	5	5	5	5	5	3	5	4	5	5	5	5
94	2	2	4	4	3	4	4	5	5	5	4	3	5	5	5	4	4	5	3	3	5	3	5	5	5	5	5	5	5	5	4	4	5	4	5	5	5	5
95	2	1	5	4	3	3	3	3	4	5	3	4	5	5	5	4	5	5	3	3	5	3	5	5	5	5	5	5	2	5	5	3	2	4	5	5	5	5
96	2	1	4	5	3	3	2	3	4	5	4	3	4	3	5	3	4	3	3	3	4	4	5	5	5	5	5	5	5	5	5	3	5	4	5	5	5	4
97	2	2	4	5	3	4	3	3	4	5	3	2	4	5	5	3	5	3	3	2	4	3	5	5	5	5	5	3	5	5	4	5	5	5	5	2	5	4
98	2	2	5	5	3	4	3	3	4	5	1	3	4	5	5	4	3	3	2	3	4	3	5	5	5	5	5	5	4	5	4	5	5	5	5	2	3	4
99	1	2	5	5	3	4	3	3	4	5	1	3	4	5	5	4	3	3	2	3	4	3	5	5	5	5	5	5	4	5	4	5	5	5	5	2	3	4
100	2	2	5	5	3	4	3	3	4	5	3	3	5	3	4	3	5	5	2	3	4	3	5	5	5	4	5	5	4	5	4	4	2	5	5	5	3	5
101	2	2	5	4	3	3	3	3	3	5	3	5	5	3	4	4	5	5	2	2	5	3	5	5	5	4	5	5	4	5	5	5	2	5	5	5	3	5
102	1	2	5	4	3	4	4	3	3	5	3	5	5	5	5	4	5	5	2	3	5	5	5	5	5	5	4	5	4	5	5	4	5	5	5	5	5	5
103	1	1	5	5	3	3	3	3	3	5	3	5	4	3	5	3	5	3	3	3	5	5	5	5	5	4	4	5	4	5	4	5	4	5	4	5	5	2
104	2	2	4	5	3	4	3	3	4	5	3	5	4	5	4	3	5	3	3	2	5	5	5	5	5	4	4	3	5	4	4	5	2	5	4	2	3	5
105	2	2	5	4	3	1	2	3	4	5	4	4	4	5	5	3	3	5	5	3	5	4	5	5	5	4	4	3	5	4	4	4	5	5	4	5	5	5
106	1	2	4	4	3	1	3	3	3	5	3	5	5	5	4	3	5	5	5	3	5	4	5	5	5	4	4	5	5	4	4	5	3	5	4	5	3	5

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información															
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
107	2	2	4	4	3	3	4	4	5	5	4	5	4	5	4	3	4	5	5	3	5	4	5	5	5	5	5	5	5	4	4	4	5	4	5	5	3	5
108	1	3	5	5	3	1	2	3	4	5	3	4	4	5	4	3	5	2	5	1	5	5	5	4	5	4	4	4	5	4	5	1	4	1	5	2	1	5
109	1	2	4	4	3	3	2	3	4	5	4	3	4	5	3	3	3	5	3	2	5	5	5	4	5	5	5	4	5	4	4	5	3	4	5	4	3	5
110	1	2	4	5	5	4	5	5	5	5	3	5	4	3	5	5	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	5	5	4	5	5	5	5
111	2	1	5	5	3	3	3	3	4	5	4	3	5	3	3	3	2	5	3	3	4	2	4	4	5	5	5	4	5	4	5	4	3	4	5	2	3	5
112	1	1	5	4	3	3	2	3	4	5	4	5	5	5	4	3	4	5	3	2	4	5	4	4	5	5	5	5	5	4	5	5	5	4	5	4	3	5
113	1	1	4	4	3	3	3	3	4	5	4	3	2	5	4	3	5	3	3	2	4	5	4	4	4	5	5	5	5	4	5	5	3	4	5	4	5	5
114	1	2	4	5	3	3	3	3	3	5	4	5	5	3	4	3	2	5	5	3	4	4	4	4	5	5	5	5	5	4	4	4	5	4	5	4	5	5
115	1	2	5	5	3	3	3	3	3	5	3	3	2	5	4	4	5	3	3	2	4	4	4	4	5	5	5	5	5	4	5	4	5	4	5	3	5	5
116	2	2	5	5	3	3	3	3	3	5	3	5	3	5	3	4	5	5	5	3	4	5	4	4	4	5	5	5	5	4	5	4	5	4	5	5	5	5
117	1	2	5	5	3	3	3	3	4	5	4	4	3	5	4	3	2	5	3	3	4	5	4	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5
118	1	2	5	5	3	1	2	3	3	5	3	5	2	5	4	3	4	5	3	3	4	5	5	5	5	3	5	5	5	4	4	5	5	3	5	5	5	5
119	1	2	4	5	3	3	3	1	4	5	4	3	2	5	3	3	2	5	3	3	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
120	1	3	5	5	3	3	3	3	4	5	3	4	3	5	4	4	3	3	3	3	4	5	5	5	5	3	5	5	3	5	4	5	5	5	5	5	3	5
121	2	2	2	2	2	2	3	3	1	1	2	2	2	2	3	3	2	2	2	1	3	3	3	2	2	3	3	2	2	2	3	3	3	3	3	3	3	3
122	2	1	2	2	2	3	3	3	2	2	2	2	2	3	3	3	2	2	2	2	2	3	2	2	3	3	3	3	3	3	3	3	2	2	3	3	2	3
123	2	1	3	3	3	2	2	3	4	2	3	3	3	4	2	3	3	3	4	4	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4
124	1	1	1	1	1	2	1	1	2	1	1	1	1	2	2	2	2	1	2	2	3	3	2	3	2	2	2	3	2	2	2	1	2	1	2	1	1	2
125	2	2	3	4	3	3	3	4	3	2	3	3	4	3	4	4	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
126	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	2	2	2	2	2	3	2	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3
127	1	4	2	2	2	2	2	2	3	2	3	2	3	3	3	3	3	2	3	3	3	3	3	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
128	2	2	4	5	4	5	5	5	4	5	4	5	4	4	4	4	4	4	5	5	3	5	5	5	5	5	3	4	5	4	3	4	5	4	4	3	4	4
129	1	2	4	4	3	3	3	3	3	2	5	2	2	3	3	2	3	3	3	3	2	2	3	3	3	3	2	2	3	3	2	4	4	4	4	4	4	4
130	1	4	2	2	2	2	2	2	3	1	1	2	2	2	2	3	2	2	2	2	3	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3
131	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
132	2	2	3	2	1	3	2	4	2	5	5	5	2	2	2	2	2	4	2	2	4	4	1	1	5	5	2	2	2	2	5	5	5	5	5	1	5	5
133	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información															
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
134	1	2	2	3	3	3	4	3	3	4	4	5	3	4	4	4	3	2	3	3	3	3	3	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4
135	1	2	2	2	2	3	3	3	3	3	3	2	2	2	2	3	2	2	2	2	3	3	3	2	2	3	3	3	3	3	3	3	3	3	2	2	2	2
136	2	2	1	2	1	2	2	2	1	2	2	2	2	1	1	2	2	1	2	1	2	2	2	2	2	2	2	1	1	2	2	2	1	1	2	1	1	2
137	2	4	3	3	3	3	4	3	3	4	4	3	4	4	4	4	4	3	3	3	4	4	3	3	3	2	4	4	3	3	3	4	4	3	3	4	3	4
138	2	2	3	3	4	3	3	4	4	3	5	5	4	4	5	4	5	4	5	5	5	4	5	5	5	4	4	5	4	5	4	5	4	5	4	4	5	5
139	1	2	2	2	1	2	1	1	2	1	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1
140	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	2	1	1	2	1	2	1	1	1	2	1	1	2	2	2	2	2	2
141	1	1	2	2	2	2	2	2	2	2	1	2	1	1	1	1	2	1	1	1	2	1	2	1	2	2	2	1	1	2	1	2	2	2	2	1	1	1
142	1	1	4	4	3	3	3	4	4	4	4	3	3	3	4	4	3	3	4	2	3	4	3	4	3	4	3	3	3	3	3	3	3	3	3	3	2	3
143	2	2	2	2	2	2	2	1	1	1	1	2	2	2	2	2	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
144	1	2	2	2	2	2	2	2	2	2	2	1	1	1	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
145	1	1	3	3	3	4	4	4	4	3	3	2	3	4	4	3	4	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	4	4	3	4	4	4
146	1	1	2	2	2	2	2	1	1	1	1	1	1	2	2	2	2	1	2	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	1	1	1	1
147	2	1	4	4	5	4	5	4	4	5	5	5	4	5	4	5	5	5	4	5	5	4	5	5	5	5	5	5	4	4	5	4	5	5	4	5	5	4
148	1	2	1	1	2	1	2	1	2	1	1	1	2	2	2	1	1	2	2	2	1	1	1	2	2	1	2	1	1	1	1	1	2	2	1	2	2	1
149	2	2	2	2	2	2	2	2	2	2	1	2	1	2	1	1	1	2	1	2	1	1	1	1	1	2	2	1	2	1	2	1	1	1	1	1	1	1
150	2	1	1	1	1	1	1	1	2	2	2	1	2	2	2	1	1	2	2	2	1	1	2	2	2	1	1	1	1	2	1	1	1	1	1	1	1	2
151	1	1	4	3	3	3	4	3	3	3	4	3	3	3	3	3	3	3	3	3	4	4	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3
152	2	2	5	5	3	3	3	3	3	5	3	5	5	5	4	3	4	3	4	3	3	2	5	5	5	3	4	5	4	5	4	5	3	4	5	5	5	5
153	1	2	4	5	3	3	3	3	3	5	4	4	2	5	5	4	3	4	2	2	2	5	5	4	5	3	3	4	4	5	5	5	4	4	5	5	5	5
154	2	1	5	5	3	1	3	3	4	5	3	4	2	5	1	1	5	5	2	3	2	2	5	4	5	5	4	4	4	5	5	5	4	4	5	3	3	5
155	1	2	5	4	3	3	3	3	4	5	3	4	5	5	5	2	5	5	2	3	3	2	5	4	5	2	4	4	4	5	5	5	5	4	5	3	3	5
156	1	2	4	5	3	3	2	3	4	5	4	3	4	5	5	3	4	3	3	3	2	5	4	4	5	5	4	4	4	5	5	5	4	4	5	3	5	4
157	1	1	4	5	3	3	4	3	4	5	3	5	4	5	1	3	5	3	3	2	3	5	4	4	5	2	3	4	4	5	4	5	5	4	5	5	3	5
158	2	3	5	5	3	4	3	1	4	5	1	3	4	5	4	2	3	3	2	3	4	5	3	4	5	5	3	4	4	5	4	5	3	4	5	5	3	5
159	2	2	5	5	3	4	3	3	4	5	3	3	3	5	2	1	5	4	2	3	5	2	3	4	5	4	3	4	4	4	4	4	5	4	5	3	3	5
160	2	2	5	4	3	3	3	3	3	5	3	5	3	3	2	2	5	5	2	2	5	3	3	4	5	4	4	4	4	4	5	5	5	4	5	3	3	5

			Variable 1: Ciberseguridad																		Variable 2: Gestión de Tecnologías de Información																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N° Encuesta	Sexo	Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
161	1	2	5	4	3	4	5	3	3	5	3	5	5	5	5	4	5	5	2	3	5	3	3	5	5	5	4	4	4	4	5	4	3	4	5	5	5	5
162	2	1	5	5	3	3	3	3	3	5	3	5	4	3	5	1	5	3	3	3	5	3	5	4	5	3	4	4	4	4	4	5	4	4	4	5	2	5
163	1	1	5	4	3	4	5	3	3	4	4	5	4	5	4	3	5	4	4	3	5	5	5	4	5	4	2	4	4	5	4	4	5	5	5	5	5	5
164	2	2	5	5	3	4	3	3	4	5	3	3	2	3	1	1	3	3	2	1	2	5	3	4	5	3	4	4	4	4	5	5	4	5	5	5	2	5
165	1	1	5	5	3	3	3	3	3	5	3	4	2	5	4	1	2	3	2	1	3	3	3	4	3	2	4	4	4	3	1	5	1	5	2	4	1	2
166	2	2	5	5	3	3	3	3	4	5	3	4	4	5	3	2	3	5	4	3	2	2	3	2	3	2	4	4	4	4	4	5	3	5	4	2	4	5
167	1	1	5	4	3	3	2	3	4	5	4	5	2	5	2	1	3	3	3	2	5	4	3	3	5	2	2	4	4	4	3	5	5	5	2	3	4	3
168	2	3	5	5	3	3	3	3	4	5	3	4	4	5	3	2	3	3	4	3	3	3	5	4	4	3	4	4	4	4	5	5	2	2	5	2	5	3
169	2	2	5	5	3	3	3	3	4	5	4	5	3	5	4	1	5	3	2	3	5	2	1	4	4	3	2	2	4	5	5	4	3	5	5	2	2	3
170	1	1	4	5	3	5	4	5	5	5	5	5	4	5	4	4	4	5	5	3	3	3	5	3	2	2	5	4	4	5	4	5	3	5	5	2	3	3
171	1	3	5	5	5	5	4	4	5	5	1	4	5	5	5	3	5	5	5	5	5	4	5	5	3	3	3	3	3	5	3	5	5	5	5	2	2	2
172	2	1	4	4	3	4	3	3	3	5	3	4	4	3	4	4	4	3	3	3	3	3	5	3	3	3	3	3	3	5	3	5	3	5	5	3	5	5
173	1	1	4	5	4	5	5	4	5	5	4	5	5	5	5	5	5	4	4	4	5	4	5	4	5	4	4	4	4	4	5	4	5	5	5	5	5	5
174	1	2	5	5	3	4	3	3	4	5	3	3	3	5	2	1	5	4	2	3	5	2	3	4	5	4	3	4	4	4	4	4	5	4	5	3	3	5
175	2	2	5	4	3	3	3	3	3	5	3	5	3	3	2	2	5	5	2	2	5	3	3	4	5	4	4	4	4	4	5	5	5	4	5	3	3	5

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: "Ciberseguridad y su incidencia en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022", cuyo autor es MALLQUI MALLQUI AMPELIO JUAN DE MATA, constato que la investigación cumple con el índice de similitud establecido, y 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, 06 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
VISURRAGA AGUERO JOEL MARTIN **DNI:** 10192315 **ORCID** 0000-0002-0024-668X	Firmado digitalmente por: JMVISURRAGA el 09-08-2022 20:33:45

Código documento Trilce: TRI - 0395623

INVESTIGA UCV