UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Modelo de Gestión de riesgos de TI para la seguridad de la información de una institución del estado, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Pizarro Castro, Ivan Marco Antonio (ORCID: 0000-0002-2218-5099)

ASESOR:

Dr. Acuña Benites, Marlon Frank (ORCID: 0000-0001-5207-9353)

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

A Dios, mi madre y a mi padre que en paz descanse, por inspirarme a cumplir mis metas, por su apoyo incondicional, por enseñarme a no rendirme, por amarme y respetarme a pesar de mis errores; a mis hermanos: Paul y Daniel, por apoyarme y motivarme para lograr superarme cada día más.

Ivan

Agradecimiento

A la Escuela de postgrado de la UCV, a su honorable plana docencia y un especial agradecimiento al Dr. Acuña Benites Marlon Frank por su acertada asesoría en esta tesis. Así mismo, al Perú por ser fuente de inspiración de lucha por su progreso y bienestar; pese a sus problemas sociales, políticos, éticos y económicos, tengo fe que en nosotros está el darles solución, actuando correctamente desde el lugar donde nos encontremos.

Índice de Contenidos

Pg.

Índice de tablas

Índice de figuras

Resumen

El objetivo de la investigación fue determinar la incidencia del modelo de gestión de riesgos de TI en la seguridad de la información de una institución del estado, Lima, 2022. La investigación fue de tipo básica, nivel descriptivo, tuvo un enfoque cuantitativo, de diseño no experimental, transversal y de corte correlacional - causal, su población y muestra fue de 80 trabajadores de una institución del estado, se utilizó la encuesta como técnica y el cuestionario como instrumento de recopilación de información. Para obtener los datos de la encuesta se utilizó un formulario virtual de docs. Google, se realizó el procesamiento de datos, incorporando los datos a un estadístico Alfa de Cronbach que simplificó la consecución de porcentajes, además, mediante tablas graficas se hizo la clasificación de datos, se asignaron valores, escalas y se logró resultados obtenidos del análisis. En este estudio se empleó la validez del contenido, se efectuó el juicio de expertos. Se obtuvo un resultado RLO p = 0.000 y un coeficiente de 0.477 en la prueba Pseudo R cuadrado, concluyendo que el modelo de gestión de riesgos de TI tiene una incidencia del 47.70% en la seguridad de la información en una institución del estado, Lima 2022.

Palabras clave: *Gestión de riesgos, seguridad de la información, amenazas.*

Abstract

The objective of the research was to determine the incidence of the IT risk management model in the information security of a state institution, Lima, 2022. The research was of a basic type, descriptive level, had a quantitative approach, of design non-experimental, cross-sectional and correlational - causal, its population and sample was 80 workers from a state institution, the survey was used as a technique and the questionnaire as an information collection instrument. To obtain the survey data, a virtual form of docs was used. Google, the data processing was carried out, incorporating the data into a Cronbach's Alpha statistic that simplified the achievement of percentages, in addition, through graphic tables the data classification was made, values, scales were assigned and results obtained from the analysis were achieved. In this study, content validity was used, expert judgment was carried out. An RLO p = 0.000 result and a coefficient of 0.477 in the Pseudo R squared test were obtained, concluding that the IT risk management model has an incidence of 47.70% in information security in a state institution, Lima 2022.

Keywords: *Risk management, information security, threats.*

I. INTRODUCCIÓN

Las Tecnologías de la Información (TI) forman parte fundamental en el desarrollo de casi todas las actividades en las entidades públicas y privadas, de forma que se hace más fácil la ejecución de sus procesos. La gestión de riesgos es una competencia clave dentro de las organizaciones, por ello, es esencial integrarla y alinearla con sus procesos organizacionales y comerciales (Barafort, Mesquida y Mas, 2018). Analizar y gestionar los riesgos de TI, es un arduo trabajo al que las organizaciones se enfrentan actualmente (Colina y Túa, 2020)

A nivel internacional, para Nur & Riadi (2020), los problemas surgen debido a la gestión de riesgos de TI por lo cual los objetivos no se alcanzan adecuadamente, siendo importante su evaluación para mitigar el choque producido por los riesgos. Por otro lado, la seguridad de la información para las instituciones alude a resguardar *la "confidencialidad, integridad y disponibilidad"* de los datos, los sistemas que los procesan, mantienen y reportan, así como los medios de almacenamiento y comunicación (Benqdara, Elfergani y Sultan, 2020). Para Agrawal (2016), en su artículo "Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard", refiere que en las organizaciones a menudo se toman decisiones equivocadas respecto a la gestión de riesgos, esto se debe a la falta de conocimiento sobre la seguridad, activos, potenciales amenazas y las salvaguardas de la organización.

Panchabhai y Varade (2020), hoy en día muchas personas utilizan Internet para transferir sus datos digitalmente, en un entorno de red que no es seguro porque un intruso puede comprobar, alterar o acceder a sus datos confidenciales, por ello existe una necesidad imperante de proporcionar seguridad a estos datos. Se debe brindar seguridad de la información en términos de *confidencialidad, integridad y disponibilidad* de los datos. La gran variedad de aplicaciones web y de sistemas, unido al gran valor que gestionan están expuestos a ataques dentro y fuera de las empresas, lo que genera pérdidas financieras, así como pérdidas de confidencialidad y credibilidad cuando se pone en riesgo la integridad y disponibilidad de los datos de la organización (Gonzales, Montesinos y Gainza, 2021).

Según Deloitte (2019), en su investigación sobre “Tendencias en Gestión de Ciber Riesgos y Seguridad de la Información en América Latina y Caribe (AL&C)”, se ha identificado que en las instituciones la inteligencia de amenazas y monitoreo de ciberseguridad su capacidad es limitada, sólo el 31% lo realiza y comparte la información con otras organizaciones, por ello es de vital importancia manejar datos actualizados sobre amenazas, riesgos, controles y gestión de resguardo de los datos.

A nivel nacional, para Cruz (2019), sostuvo que un existe desconocimiento en cuanto a la gestión de riesgos en empresas distribuidoras de Lambayeque debería considerarse un proceso intrínseco, puesto que si la organización desconoce sobre el riesgo al que están expuestos sus activos de TI le será difícil estar alerta para evitar una posible ocurrencia. Según Salinas & Valencia (2017), el factor humano es crítico y vital para implementar y mantener niveles óptimos de la seguridad en la organización, para ello todos los actores deben ser capacitados y en base a sus nuevos conocimientos tratar de minimizar las posibles causas. Llontop (2018), logró implementar en la empresa Nephila, el método operativo de control de riesgo, optimizando de esta manera la eficiencia con la que se gestionan los riesgos.

Según Zevallos (2019), Implementar modelos de gestión de riesgos, acordes a los requerimientos singulares en una institución, repercuten en la simplificación de costos, tiempo y hacen más previsibles las acciones de una institución. Tener conocimiento de a que se enfrentan las organizaciones e identificar los riesgos ayuda a tomar mejores decisiones y resolverlos de forma más efectiva. Para Otoya (2018), una gestión de riesgos de TI adecuada, permite considerar causas y consecuencias, definir valores y dimensiones a los activos de información para tomar mejores decisiones ante un riesgo. Por otra parte, Huayllani Muñoz (2020), afirmó que “el sistema de gestión de seguridad de la información se relaciona con la gestión del riesgo del MINSA”, lo que permitirá analizar el desempeño de la implementación realizada.

Hoy en día, existen múltiples riesgos identificados sobre equipos y sistemas que no presentan salvaguardas (Pazmiño, Serrano y Gonzales, 2020). Es necesario mencionar que el Perú no es ajeno a sufrir riesgos de TI que ataquen directamente el resguardo de los datos de las entidades estatales y privadas, existen normas técnicas como la “NTP- (Barriga, 2019) ISO/IEC 27005:2018 Gestión de riesgo de la seguridad de la información” que proporciona instrucciones para identificar riesgos, evaluarlos, medirlos y establecer prioridades que permitan reducir su influencia negativa en la organización, asimismo, la “NTP-ISO/IEC 27001:2014 Sistemas de gestión de seguridad de la información” que proporciona lineamientos para implementar un SGSI con la finalidad de evaluar riesgos y minimizarlos. Aplicar metodologías de riesgos es de gran ayuda a las organizaciones, puesto que ofrecen lineamientos para el control de sus activos, su valor y las amenazas capaces de impactarlas, (Tejena, 2018).

En ese sentido, la institución en estudio con Resoluciones aprueba la “Metodología de Gestión de Riesgos de Seguridad de la Información”, la “Política de Seguridad de la Información”, el “Manual de Procedimientos del Macroproceso Gestión de Tecnologías de la Información” a cargo de la Oficina General de TI, además, aprobó el “plan de gobierno digital”, cuyas premisas son de aplicación para todos los trabajadores de sus órganos y unidades orgánicas. A pesar de ello, existe falta de concientización y/o desconocimiento de los trabajadores respecto a la gestión de los riesgos de TI y cada política establecida en materia de resguardo de datos.

Entre los años 2018 y 2019 un ciberdelincuente junto a su banda logró vulnerar uno de sus sistemas, suplantando la identidad de funcionarios para generar expedientes de obras y manipular el proceso de pago, sustrayendo cerca de dos millones de soles. Es por esta razón que se plantea el problema general: ¿De qué manera el modelo de gestión de riesgos de TI incide en la seguridad de la información de una institución del estado, Lima, 2022?, y los problemas específicos: ¿De qué manera el modelo de riesgos de TI incide en la confidencialidad de la seguridad de la información de una institución del estado?, también ¿De qué manera el modelo de riesgos de TI incide en la integridad de la seguridad de la

información de una institución del estado?, finalmente ¿De qué manera el modelo de riesgos de TI incide en la disponibilidad de la seguridad de la información de una institución del estado?

La justificación metodológica para esta investigación, con el fin de lograr los objetivos propuestos utilizando técnicas y métodos científicos para recopilar datos, analizarlos y demostrar su validez y confiabilidad a través software SPSS v25. Como justificación teórica la necesidad de aplicar un método que gestione las causas de TI basada en la norma ISO/IEC 27005:2018 todo ello para salvaguardar los datos de una entidad del Estado. Como justificación práctica la seguridad de la información es fundamental, ya que todo trabajador de una institución del estado, debe ser consciente de que identificar las vulnerabilidades, amenazas, riesgos existentes y tener en cuenta cada política establecida el resguardo de los datos ayuda a salvaguardar sus activos de información, minimizando pérdidas y asegurando la continuidad de sus actividades.

La investigación tiene como objetivo general determinar la incidencia del modelo de gestión de riesgos de TI en la seguridad de la información de una institución del estado, los objetivos específicos son: Determinar la incidencia del modelo de riesgos de TI en la confidencialidad de la seguridad de la información de una institución del estado; Determinar la incidencia del modelo de riesgos de TI en la integridad de la seguridad de la información de una institución del estado; Determinar la incidencia del modelo de gestión de riesgos de TI en la disponibilidad de la seguridad de la información de una institución del estado.

Referente a la hipótesis general: el modelo de gestión de riesgos de TI incide significativamente en la seguridad de la información de una institución del estado. Además, como hipótesis secundarias: el modelo de gestión de riesgos de TI incide significativamente en la confidencialidad de la seguridad de la información de una institución del estado, el modelo de gestión de riesgos de TI incide significativamente en la integridad de la seguridad de la información de una institución del estado, el modelo de gestión de riesgos de TI incide

significativamente en la disponibilidad de la seguridad de la información de una institución del estado.

II. MARCO TEÓRICO

Este estudio tiene sustento, de alguna forma, con investigaciones previas obtenidas de tesis de maestría, doctorales y antecedentes investigados que evidencian la gran relevancia de los problemas expuestos sobre la aplicación de un método que gestione las causas de las TI en el resguardo de los datos. Referente a estas dos variables de estudio se han realizado múltiples estudios, que poseen como antecedentes nacionales a los siguientes autores:

Salinas & Valencia (2017), *"Sistema de gestión de seguridad de información y riesgos de información en seis sedes de una entidad bancaria del Perú".* Trujillo - Perú. (Tesis de maestría). Tuvo una metodología donde pudo cuantificar los fenómenos, además de no maniobrando los mismos, utiliza la encuesta aplicándola a una muestra de 351 empleados distribuidos en las 6 sedes, se demostró el nivel de riesgo alto a un 50%, riesgo medio un 28% y riesgo bajo un 22% en usuarios como en equipos en las áreas, se identificaron los activos, las vulnerabilidades y amenazas para poder definir las causas presentes en la entidad, el uso del SGSI estableció que solo un 30% de las sedes investigadas cumple con el resguardo de los datos, por consiguiente, se eligieron salvaguardas y sus objetivos de resguardo de datos, aprobados por la Alta dirección de la organización o por terceros, por la que serán sostenidos, ejecutados y monitoreados.

Otoya (2018), *"Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017"*. Lima-Perú (Tesis de maestría). En su investigación, buscó "determinar la influencia de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural", implementó una metodología donde cuantificó los fenómenos de estudio en donde no experimentó con los mismos, además, utilizó la encuesta aplicándola a una muestra de 120 trabajadores del sector Agrario rural de Lima, 2017. En este estudio se evidenció que es posible que, el resguardo de los datos sea deficiente todo ello por gestionar inadecuadamente las causas que se puedan presentar. Y que la probabilidad de que dicho resguardo sea eficaz se debe a una buena gestión de riesgos, esto debido a si nivel de significancia igual a 0.035.

También se pudo apreciar que dicho resguardo arrojó un porcentaje de 44%, por su nivel de significancia de 0.000, además que identificar vulnerabilidades en los activos de los datos, lo cual pueden reducir o aumentar la actuación de amenazas en los mismos.

Calderón (2018), *"Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018".* Lima-Perú (Tesis de maestría). Implementó una metodología donde cuantificó los fenómenos de estudio en donde no experimentó con los mismos, de cuya población de 106 colaboradores, tomó una muestra de 83 trabajadores, obteniendo el valor 0.886 Rho Spearman y 0.05 de sigma bilateral, determinado así "una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del MINEDU", de igual forma concluye que cada dimensión "confidencialidad, integridad y disponibilidad" guardan relación directa con el segundo fenómeno indagado.

Huaura (2019), *"Gestión de riesgo de seguridad de la información para empresas del sector telecomunicaciones"*. Lima- Perú. En su estudio, pretendió: *"establecer que la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 incide en el control de los riesgos en empresas del sector Telecomunicaciones"*, de tipo no experimental y diseño descriptivo transeccional, aplicó la encuesta utilizando servicios web para recopilar datos, a una muestra de 82 individuos del sector telecomunicaciones. Hallándose que la fuga de información a través de medios extraíbles es el 51.2%, por equipos móviles el 26.8 %, uso de servicios en la nube el 13.4 %, por software de control de escritorio el 7.3 % y por otros medios el 1.2 %, concluyendo que gestionar correctamente los datos informativos facilita que los objetivos se cumplan.

Calderon (2019) *"Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE, 2019".* Lima-Perú (Tesis de maestría). Implementó una metodología donde cuantificó los fenómenos de estudio en donde, además, no experimentó con los mismos. Se tomó una muestra de 25 consultores, el valor obtenido de Rho Spearman fue 0.661 y el grado de significancia fue 0.000

($p < 0.05$), concluyendo así "una relación directa entre Gestión de riesgos y Seguridad de la información en el Programa Fortalece Perú del MTPE, 2019", de la misma manera para confidencialidad, un 44.00% la percibe en nivel bajo, 40.00% en nivel medio y 16.00% nivel alto; para la integridad, que un 44.00% la percibe en nivel bajo, 44.00% en nivel medio y 12.00% alto; y para la disponibilidad, un 60.00% la percibe en nivel bajo, 28.00% en nivel medio y 12.00% alto.

Banda (2019), *"Modelo basado en metodologías de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque"*, Lambayeque – Perú. Su estudio tuvo un enfoque cuantitativo. Se tomó como muestra a 4 compañías, se utilizó el cuestionario para la recolecta de información. Se validó el modelo y se obtuvo un nivel de confiabilidad de 0.81, su implementación tuvo como resultado la identificación de 20 escenarios de riesgos, catalogados 7 como soportables y 13 como inaceptables, ante ello se propusieron 8 planes para minimizar los riesgos existentes, además de métricas para monitorizarlos.

Ñañez (2021), *"Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza -Chachapoyas"*, (Tesis de maestría). Implementó una metodología donde cuantificó los fenómenos de estudio en donde además, los describió y no experimentó con los mismos. Cuyos resultados fueron de 69.00% para el nivel medio de la confidencialidad es deficiente, el 65.50% para el nivel medio de la integridad de datos lo que indica que no hay prevención de las adulteraciones de datos, el 58.60% para el nivel medio de la disponibilidad, lo cual indica que el acceso a los datos es inadecuado respecto a la seguridad de la información.

A nivel internacional, encontramos múltiples estudios relevantes, considerando aquellos autores que mencionamos a continuación.

Arévalo, Cedillo & Moscoso (2017), *"Metodología ágil para la gestión de riesgos informáticos",* Cuenca-Ecuador". (Artículo científico). Utilizó una población

de 350 empleados, aplicó su metodología diseñada, basada en el estándar ISO/IEC 27005 en empresas industriales, la cual indica las directrices para una adecuada gestión de riesgos, además de recomendaciones y buenas prácticas de otros modelos. Se identificaron 201 activos, un 59.20 %, calificados como valor alto; un 31.84% tienen un valor medio, un 6.47% tiene un valor muy alto y un 2.49 tienen un valor extremo, además, ningún activo tuvo un valor bajo o despreciable. Asimismo, 30 riesgos fueron identificados, concluyendo que el 36% son de nivel alto, 32% de nivel extremo y 12% nivel medio pues su probabilidad de que sucedan y sus consecuencias afectan a una o varias de las dimensiones de seguridad de la información, para minimizarlos propuso un proyecto de tratamiento de riesgos el cual se monitorea y verifica su cumplimiento.

Navarro (2019), en su tesis *"Aplicación de gestión de riesgos tecnológicos basada en la norma ISO/IEC 27005 en el área de base de datos y sistema operativo de la Dirección de Informática y Sistemas de la DGI"*. (Tesis de maestría). Indica que gestionar correctamente es esencial para un buen resguardo de los datos informativos, ya que a través del desarrollo de estrategias se logran minimizar los riesgos, además su aplicación fortalece la protección de sus activos a nivel de hardware, software y decisiones organizacionales, debido a que se centra en los procedimientos, análisis de amenazas, vulnerabilidades y riesgos, aprovechando los recursos y optimizando el tiempo de ejecución, evitando de esta manera la duplicidad de controles y el reprocesamiento de actividades, permitiendo aplicar medidas preventivas y correctivas que mitiguen los riesgos existentes.

Gómez & Valencia (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"*, Medellín – Colombia. (Tesis de maestría). Buscó crear un método que gestione las fallas cibernéticas y que conlleven a su completo resguardo y que se entrelace con una secuencia operativa, basado en estándares pueda dar una respuesta conjunta, reduciendo los riesgos. Dicho procedimiento fue validado a través de un caso de estudio llegando a la conclusión que puede ser replicado a cualquier organización puesto que se

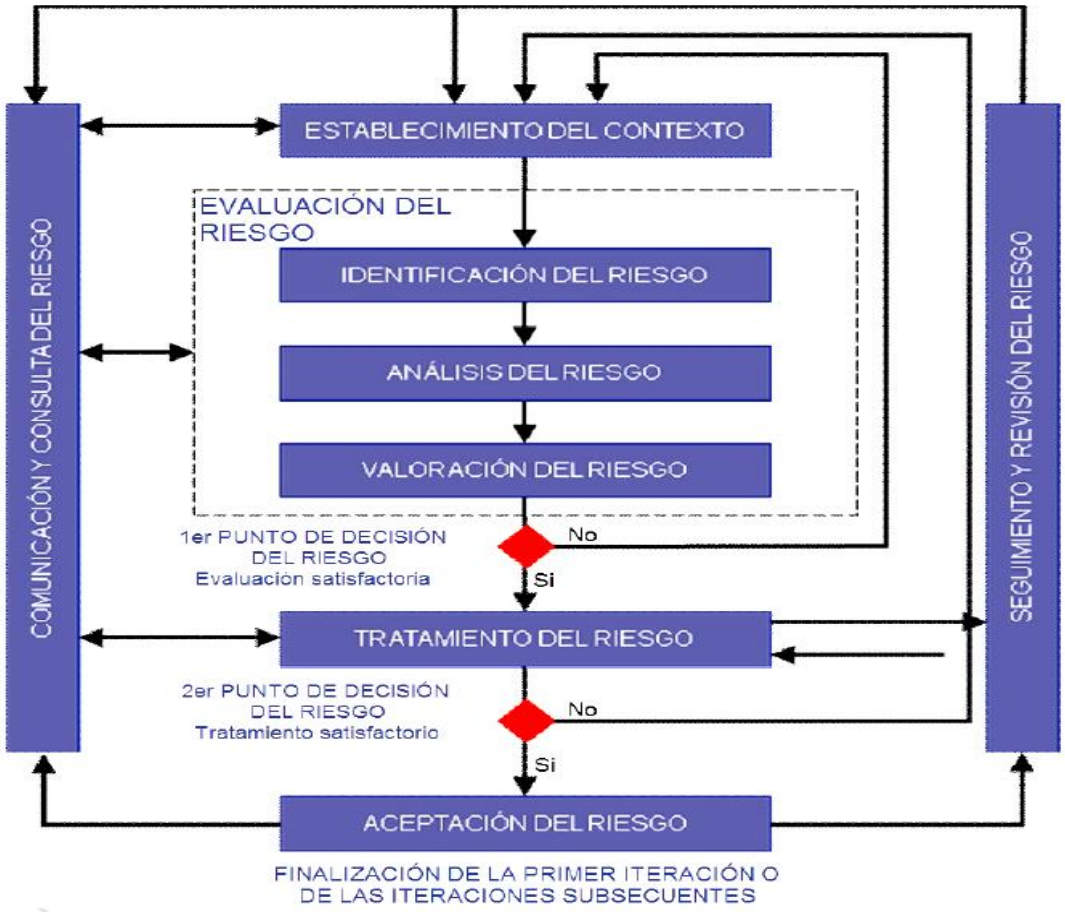
encuentra conformado por el PHVA que hace gestionar más eficaz ante los riesgos asegurando una respuesta que los minimice y que los servicios continúen. Por otro lado, los participantes de acuerdo a su rol, manifestaron que el nuevo procedimiento usa un enfoque reactivo ante eventos, incidentes y crisis aplicando una gestión integral desde el antes, el durante y el después, ello disminuye la ocurrencia y presenta una respuesta más eficaz en caso de que se materialice.

Las teorías referentes al tema de la **gestión de riesgos de TI** son expuestas por los siguientes autores:

Según la NTP-ISO/IEC 27005 (2018), las define como un conjunto de lineamientos que analizan qué puede suceder y cuáles podrían ser las consecuencias, previo a tomar una decisión de lo que se debe hacer y en qué momento, para minimizar las causas a un grado soportable. No obstante, puede ser aplicada a una parte de la organización, a un sistema específico o en fase de desarrollo o toda la organización.

Figura 1

Gestión de riesgos ISO 27005:2018 (V1)



Adaptado de "Norma Técnica Peruana NTP-ISO/IEC 27005:2018" (p.7)

Zevallos (2019), afirma que son las "actividades coordinadas para dirigir y controlar la organización con relación al riesgo". Cuyo fin es "gestionar el riesgo" estableciendo una serie de controles e indicadores que ayudan a garantizar aspectos que favorezcan a salvaguardar la información.

Corda et al., (2017), quienes afirman que la gestión de riesgos de TI, intenta minimizar las pérdidas de datos, ocasionadas por posibles fallas de los sistemas que afectan los proyectos en las compañías, fallas que pueden darse de forma natural, accidental o intencionalmente, asimismo, pueden verse involucrados riesgos legales y el comportamiento ante esas amenazas.

Masso et al., (2020), La gestión de riesgos se entiende como un cumulo de acciones coordinadas que permiten a la organización ser dirigida y controlada en lo que respecta al riesgo. (p.10)

Öbrand, Holmström & Newman (2018), definen en esencia el riesgo como una cuestión de “efecto de la incertidumbre sobre los objetivos” (ISO 31000, 2018). Así en gran medida el riesgo es una cuestión de perspectiva, donde puede tener un resultado negativo para unos y positivo para otros.

Najar y Suarez (2016), indica que no es más que la explotación de inseguridades de los activos de datos por apercibimientos potenciales, que causan daños a la organización.

Son consideradas como dimensiones de la gestión de riesgos de TI las siguientes: amenazas, impacto potencial, salvaguardas.

Según la NTP ISO/IEC 27005 (2018), una amenaza puede dañar uno o más activos de las organizaciones, se dan de forma accidental o adrede, siendo su origen humano o natural y surge desde dentro o fuera de la organización. (p.19)

De la misma forma, MARGERIT v.3 (2014), refiere que las amenazas como cosas que ocurren y, de todo ello, interesa los efectos sobre los activos de la organización y los daños que puedan causar. Sobre el impacto potencial indica que es el efecto del daño sobre los activos al materializarse una amenaza. Se define a los controles o salvaguardas como aquellas actividades o procedimientos que mitigan el riesgo.

Según la NTP ISO/IEC 27005 (2018), el impacto potencial se mide en relación al nivel de daño o pérdidas para la institución como consecuencia de un incidente, teniendo en cuenta el grado de un activo, las brechas de seguridad, las operaciones estropeadas, pérdidas financieras, variación de planes y daños a la reputación.

Según la NTP ISO/IEC 27005 (2018), los controles o también llamadas salvaguardas dan cierta protección como: “corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y concientización”. (p.35)

Así mismo la ISO 27005 (2018), menciona que los controles modifican el riesgo incluyendo para ello, prácticas, dispositivos, procesos, políticas, entre otras actividades. No siempre los controles ejercen el resultado esperado de modificación. “Los términos salvaguardas o contramedida son utilizados frecuentemente como sinónimos de control”.

Las **teorías** referentes al tema de la **seguridad de la información** son expuestas por los siguientes autores:

Según ISO 27001 (2013), define como “la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización”. (p.1)

Figura 2

Dimensiones de la seguridad de la información (V2)

Adaptado de “Instituto Nacional de Ciberseguridad” (p.6)

Zevallos (2019), lo conceptualiza refiriéndose a los activos de información a todo recurso, funcionalidad, componente físico o lógico que crea valor en la organización, a través de los cuales se pueden almacenar múltiple información correspondiente a los procesos de la organización y sumen al alcance de sus objetivos, los mismos que están expuestos a distintos riesgos de seguridad.

Rao. et. al (2021), lo define como un proceso complicado que involucra muchos factores, como la educación, factores humanos y tecnología, la cual es necesario gestionar bajo un modelo de seguridad, añade que una gestión positiva conduce a buena cultura de seguridad en las organizaciones.

Según ISOTools Excellece (2017), indica que la seguridad informática es la doctrina encargada de accionar soluciones técnicas para proteger la información. “Es así que protege un sistema informático, garantizando la confidencialidad e integridad de la información que comprende. Por lo cual, se puede decir que se trata de trazar técnicas que preserven la infraestructura y las comunicaciones que soportan el funcionamiento de una empresa”.

Barzaga. et. al (2019), menciona que es como una agrupación de métodos que ayudan a las acciones encaminadas a que la información interna, externa o contenida en cualquier medio, sea generada, almacenada, conservada y recuperada.

Orehek & Petric (2021), afirma que las organizaciones deben desarrollar un cierto nivel de cultura de medidas preventivas de tecnologías, que posibilite reducir los riesgos de seguridad, índica que muchos aspectos del factor humano son relevantes dentro del contexto de seguridad organizacional.

Valencia-Duque & Orozco-Alzate (2017), afirma que se asocia principalmente a la gestión de las TIC, cuya finalidad se basa en que los riesgos de la información institucional y de los instrumentos tecnológicos a través de los cuales se recolecta, procesa, se accede, se almacena, transforma y presenta se mantengan en niveles aceptables.

Para Avenía (2017), define un "*Sistema de Gestión de Seguridad de la Información*" (SGSI), facilita lineamientos a tomar como referencia para dar soporte, monitorear, resguardo de los bienes y servicios funcionales y cumplir con los objetivos organizacionales.

Son consideradas como cada dimensión de dicha variable las siguientes: confidencialidad, integridad, disponibilidad.

INCIBE (2019), menciona que la confidencialidad significa que el personal autorizado es el único que debe tener acceso a la información, por ello solo debe ponerse en conocimiento de los individuos, organizaciones o sistemas autorizados para acceder a ella.

Cantalejo (2019), afirma que la confidencialidad indica que es la propiedad que exige que la información solo tiene que ser accesible o divulgada a aquellos que están autorizados.

Herath, Khanna & Ahmed (2022), afirman que debe los trabajadores deberían recibir capacitación para mejorar su conocimiento sobre el uso de la confidencialidad de la información ya que el acceso ilegal, así como el uso de la información confidencial que sin querer divulgan por medio de las redes sociales, puede generar numerosos riesgos, por ejemplo, robo de identidad, fraude, acecho y pérdida de empleo.

INCIBE (2019), indica que la integridad significa que la información no debe ser adulterada, debe permanecer correcta y sin errores, ya que podría darse el caso intencionalmente de ser alterada o incorrecta y las decisiones tomarlas en base a ella.

Cantalejo (2019), define la integridad como la propiedad que garantiza que la información debe permanecer correcta, sin manipulaciones de terceros.

INCIBE (2019), afirma que la disponibilidad es la información accesible cuando se necesite.

Cantalejo (2019), sostuvo que la disponibilidad se refiere a la particularidad que garantiza que la información solo sea asequible al personal autorizado.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

Acorde con el objetivo del estudio es de tipo básico. Para Hernández (2018) este tipo de estudio busca crear nuevos conocimientos respecto a determinadas teorías. La investigación básica sirve de cimiento para los conocimientos científicos, es fuente de nuevas ideas que forman la base del desarrollo en distintas materias.

Asimismo, la investigación tuvo un enfoque cuantitativo, ya que se obtuvieron datos de los trabajadores de una institución del estado por medio de preguntas en encuestas a ambas variables, para analizarlos, sistematizarlos y luego explicarlos, al respecto Sánchez et. al (2018), indican que, “al evaluar datos numerales esencialmente mediante el rubo estadístico, estos generan la oportunidad de tener medición y cuantificación”.

Diseño de investigación

Dicho estudio utilizó el descriptivo, además de no experimental y correlativo. Para Hernández et al, (2018), menciona que la no experimental es cuando las variables de estudio no son manipuladas intencionalmente; es transversal pues recolecta la data en un momento y espacio único. La finalidad es comentar las variables presentes y determinar su responsabilidad o influencia en un momento determinado.

3.2. Variables y operacionalización

Variable: Modelo de gestión de riesgos de TI

Definición Conceptual

Según la NTP-ISO/IEC 27005 (2018), la define como un conjunto de lineamientos que analizan podría ocurrir y cuáles ser las posibles consecuencias, previo a tomar una decisión de lo que se debe hacer y en qué momento, para

minimizar el riesgo. Además, puede ser aplicada a una parte de la organización, a un sistema específico o en fase de desarrollo o toda la organización.

Definición Operacional

La gestión de riesgos de TI está definida por la puntuación obtenida a través del cuestionario, el que faculta medir su influencia en la segunda variable objeto de estudio, utilizando 19 ítems cuyas respuestas son de tipo Likert y rangos bajo, medio y alto, se precisa el empleo del cuestionario, y los resultados serán aplicados en el SPSS. v 25.

Variable: Seguridad de la información

Definición Conceptual

Según ISO 27001 (2013), define como la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Definición Operacional

La seguridad de la información, con la finalidad de lograr los objetivos del estudio se medirá en función a los 24 ítems con respuestas tipo Likert y rangos bajo, medio y alto, determinándose cómo está siendo incidida por la gestión de riesgos de TI, basándose en el cumplimiento de sus dimensiones expuestas en el marco teórico, se hace uso del cuestionario, y los resultados serán aplicados en el SPSS. v 25.

Los siguientes son tomados como indicadores de la segunda variable: cantidad de políticas de seguridad, cantidad de personal especializado, cantidad de pruebas en tráfico de red, cantidad de incidentes en manipulación de datos, frecuencia de actualización de antivirus, frecuencia de soporte a hardware y software, tiempo de respuesta de la información requerida, nivel de complejidad de

contraseñas, cantidad de copias de respaldo de información. Estos indicadores permitirán que la incidencia de ambas variables sea cuantificada.

Escala de medición

De tipo categórica se desarrolló en base a una serie de números asignados que definiera cada categoría o escala de nivel ordinal (mutuamente excluyente), la cual permite medir y evaluar los datos, sin definir la variación entre los mismos (Hernández et al., 2018). El método denominado “Escala de Likert” se utilizó, este método se distingue por utilizar un rango de puntuación para advertir el nivel de conformidad de los participantes sobre un enunciado en particular, planteando distintos niveles (entre cinco y siete).

3.3. Población, muestra, muestreo, unidad de análisis

Población:

Se conforma por 80 trabajadores de una institución del Estado.

Hernández y Mendoza (2018), definieron a una población como la agrupación del total de sucesos que encajan con una serie de descripciones, en la cual se asocia el total de la unidad de análisis.

Muestra:

Referente a la muestra, específicamente, equivale a un pequeño grupo de la totalidad poblacional. Esto quiere decir, que es un subgrupo de componentes del conjunto establecido en sus características al cual llamamos población, el determinar los elementos a analizar, precisa limitar la población para definir parámetros y generalizar resultados (Hernández, Fernández & Baptista, 2018). En la investigación el tipo de muestra es CENSAL, mismo que equivale a tomar toda la población. Hay que mencionar, además que el método al inicio todos tienen las mismas probabilidades de ser seleccionados por ello es aleatorio simple.

Sin embargo, puesto que la población tiene una cantidad limitada de integrantes y es accesible, la totalidad poblacional fue tomada de muestra, en otras palabras, a los 80 empleados de una institución del Estado.

Muestreo:

Otzen y Manterola (2017), afirman que, el muestreo tiene por objetivo estudiar las relaciones existentes entre la distribución de una variable en la población y en la muestra a estudio.

Unidad de análisis:

Trabajadores de una institución del estado.

Tabla 1

Personal que labora en una institución del estado

Cargo	Nº de trabajador
Director	01
Asesor	01
Experto	01
Coordinador	01
Especialista	18
Analista	54
Abogado	02
Apoyo administrativo	02
TOTAL	80

Fuente: Institución del estado

Criterios de selección.

Se toman a los trabajadores de la institución del Estado; se excluyen individuos que no laboran en la institución del estado.

3.4. Técnicas e instrumentos de recolección de datos

Hernandez y Duana (2020) ha señalado que las técnicas son una serie de procedimientos y acciones que permiten obtener información necesaria para responder las consultas materia de investigación, éstas pueden ser entrevistas, cuestionarios, fichas, etc.

Por lo tanto, los instrumentos para obtener datos, son recursos que utiliza un investigador para registrar la data concerniente a los fenómenos indagados Hernández & Mendoza (2018).

En tal sentido, se utilizó el cuestionario. Todos los instrumentos deben ser confiables, objetivos y tener validez que avalen los resultados obtenidos en la investigación.

Validez

Hernández & Mendoza (2018), afirman que un instrumento es válido si mide lo que pretende medir". Dicho proyecto empleó la validez del contenido, teniendo en cuenta: la pertinencia, la claridad y la relevancia, que son elementos fundamentales de cada ítem de los instrumentos (ver Anexo). Asimismo, se realizó la validación por medio de un grupo de profesionales expertos.

Tabla 2

Validación del Instrumento por Especialistas

Experto(a)	Observaciones	Puntaje
Dr. Marlon Frank Acuña Benites	Si hay suficiencia, es aplicable	Muy alto
Dr. Josue Joel Ríos Herrera	Si hay suficiencia, es aplicable	Muy alto
Mgtr. Eduardo Humberto Poletti Gaitan	Si hay suficiencia, es aplicable	Muy alto

Fuente: Certificado de validez (2022)

Confiabilidad

Hernández & Mendoza (2018), aseguran que es la consistencia de los resultados obtenidos por las mismas personas en ocasiones diferentes. Asimismo, por medio de la aplicación del coeficiente Alfa de Cronbach se logró determinar la confiabilidad de este trabajo, ya que es conveniente para escalas politómicas, por ello la Escala de Likert es la indicada.

El Alfa de Cronbach es un coeficiente que toma valores en una escala de entre 0 y 1, cuanto más cerca esté a 1, existe mayor fiabilidad, por otra parte, cuanto más se acerca a cero, no es fiable.

Alfa de Cronbach
Muy satisfactoria de 0.90 a 1.00.
Adecuada de 0.80 a 0.89.
Moderada de 0.70 a 0.79
Baja de 0.60 a 0.69.
El instrumento no pasa la prueba de fiabilidad, no se acepta si su valor es < 0.50.

Tabla 3

Estadística de fiabilidad, Variable1: "Modelo de gestión de riesgos de TI"

Alfa de Cronbach	Nº de elementos
,908	19

Fuente: El Investigador

Consta de 19 preguntas, alcanzó un coeficiente de 0.908, dicho valor es considerado como muy satisfactorio, por consiguiente, se acepta.

Tabla 4

Estadística de fiabilidad, Variable2: "Seguridad de la información"

Alfa de Cronbach	Nº de elementos
,900	24

Fuente: El Investigador

Consta de 24 preguntas, alcanzó un coeficiente de 0.900, dicho valor es considerado como muy satisfactorio, por consiguiente, se acepta.

3.5. Procedimientos

Previo a la recopilación de datos, se solicitó una carta de presentación a la universidad y se envió a una institución del Estado, cuya finalidad fue pedir autorización para desarrollar una investigación referente al tema investigativo.

Para obtener los datos de la encuesta se utilizó un formulario virtual de docs. Google, luego se exportan al programa Excel versión 2019, dichos datos son importados por software SPSS V25. Se utilizaron a los trabajadores de una institución del estado como fuente principal de recolección de información, quienes suministraron data verídica al contestar las preguntas de los cuestionarios, que

contaron con, variable 1: Modelo de gestión de riesgos de TI, 19 preguntas y variable 2: seguridad de la información, 24 preguntas, aplicadas con la escala de Likert.

3.6. Método de análisis de datos

Método descriptivo

Se aplica el software SPSS v.25, determinándose la confiabilidad por el Alfa de Cronbach, asimismo, mediante tablas graficas se hizo la clasificación de datos, se asignaron valores, escalas y se logró resultados obtenidos del análisis.

Método inferencial

Aplica métodos inferenciales para contrastar la hipótesis, dando resultados a los que se elaboran interpretaciones y se llega a obtener una conclusión.

3.7. Aspectos éticos

Desde el punto de vista de Salazar, Icaza y Alejo (2018), define a los códigos éticos, como criterios reflexivos sobre las responsabilidades conjuntas dentro de las instituciones, y menciona que no es posible su existencia sin tener una justificación que aclare las pautas para el ejercer la investigación.

En la presente investigación, se consideraron aspectos éticos como: la autorización para realizarlo, que se evidenció con la entrega de una carta de presentación a una institución del estado. El instrumento se aplicó con respeto hacia el anonimato y el compromiso confidencialidad asumido sobre información sensible de los participantes.

Además, con la premisa de no cometer plagio, todas las referencias empleadas se han citado mencionando a los autores, anotándoles minuciosamente en las fuentes bibliográficas, respetando su propiedad intelectual. Por consiguiente, es preciso informar que el presente estudio fue analizado a través de un sistema

que sirve para cuantificar el porcentaje de similitud con diversos proyectos de investigación, esto gracias al uso del software turnitin, estableciéndose que la tesis está dentro de los límites aceptables para su publicación.

También, se han respetado las directrices exigidas por la Universidad César Vallejo mencionados en la “Resolución de Vicerrectorado de Investigación N° 110-2022-VI-UCV”.

IV. RESULTADOS

Los resultados producto de la estadística se ejecutaron con 80 participantes encuestados. Los resultados originados referentes a cada variable y/o dimensión fue el que se muestra:

Tabla 5

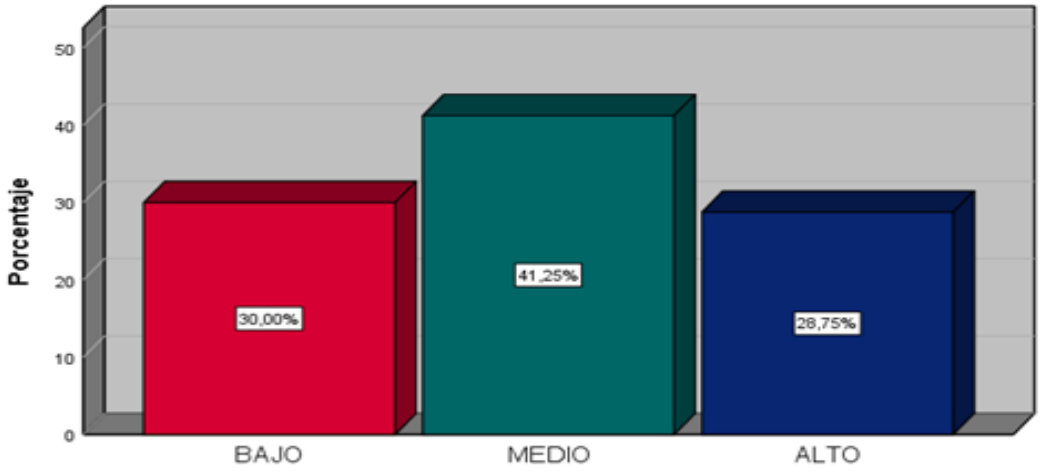
Distribución frecuencia de V1: Modelo de gestión de riesgos de TI

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Bajo	24	30,0	30,0	30,0
Medio	33	41,3	41,3	71,3
Alto	23	28,7	28,7	100,0
Total	80	100,0	100,0	

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 3

Gráfico de barras de V1: Modelo de gestión de riesgos de TI



Interpretación: Analizando la tabla 5 y figura 3, se puede verificar la distribución de la variable 1, para esta frecuencia se observa que 33 individuos (41.25%) del total de participantes, afirma que se ubica en el medio, mientras que el 30.00% (24 encuestados), indica que el Modelo (*V1*) posee un nivel bajo en cuanto a la identificación de amenazas y vulnerabilidades; y para 23 participantes que equivalen al 28,70% del total de encuestados, indican alto.

Tabla 6

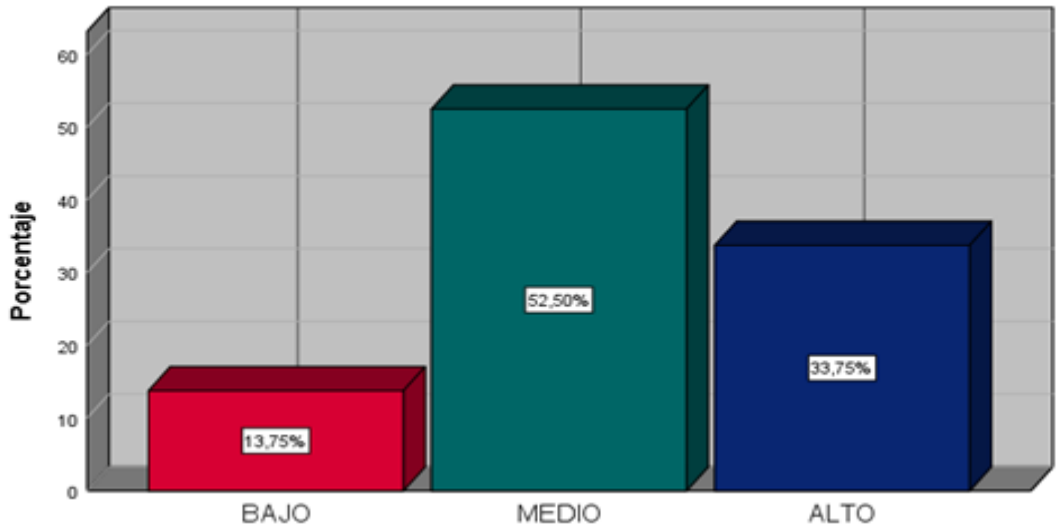
Distribución de frecuencia de V2: Seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	11	13,8	13,8	13,8
	Medio	42	52,5	52,5	66,3
	Alto	27	33,8	33,8	100,0
	Total	80	100,0	100,0	

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 4

Gráfico de barras de V2: Seguridad de la información



Interpretación: Del análisis se observan los porcentajes de 52.50% que la ubican en el medio (42 encuestados), el 33.75% en el alto (27 encuestados), quienes aseguran que coadyuva a mantener la confidencialidad, integridad y disponibilidad de la información; y el 13.75% que equivale a 11 participantes, perciben que hay un nivel bajo.

Tabla 7

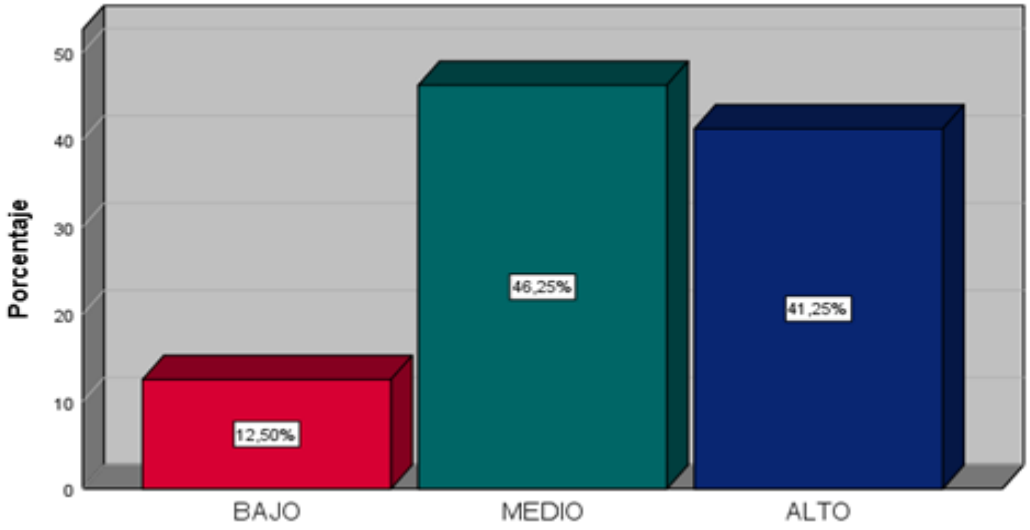
Distribución de frecuencia de la D4: Confidencialidad

		Frecuencia	*Porcentaje*	*Porcentaje válido*	Porcentaje acumulado
Válido	Bajo	10	12,5	12,5	12,5
	Medio	37	46,3	46,3	58,8
	Alto	33	41,3	41,3	100,0
	Total	80	100,0	100,0	

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 5

D4 Confidencialidad



Interpretación: Analizando dichos hallazgos se puede afirmar que del total de participantes de la encuesta, el 12.50% (10 encuestados) perciben que en la confidencialidad de la información de la institución hay un nivel bajo, mientras que el 46.25% (37 encuestados), considera que la confidencialidad se ubica en un nivel medio puesto que al realizar las pruebas de tráfico de red existen limitaciones; y el 41.25% (33 encuestados), señalan que en la políticas de seguridad de la información, se demuestra como alto.

Tabla 8

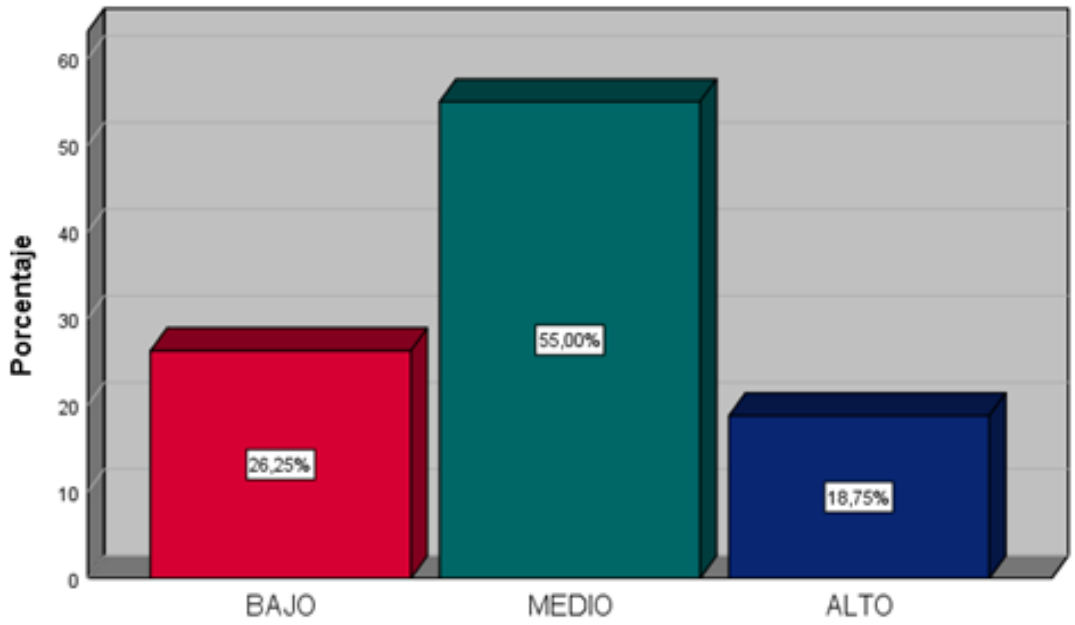
Distribución de frecuencia de D5: Integridad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Bajo	21	26,3	26,3	26,3
Medio	44	55,0	55,0	81,3
Alto	15	18,8	18,8	100,0
Total	80	100,0	100,0	

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 6

D5 Integridad



Interpretación: Analizando los hallazgos se aprecia que un 26.25% (21 participantes) consideran que la integridad de la información tiene un nivel bajo en cuanto a la manipulación de información por parte de los trabajadores, mientras que el 55.00% (44 participantes), percibe que la integridad de la información se ubica en el nivel medio en cuanto al mantenimiento de hardware y software; y solo el 18.75% (15 participantes) del total de encuestados, aseguran que en la actualización de antivirus, se demuestra como alto.

Tabla 9

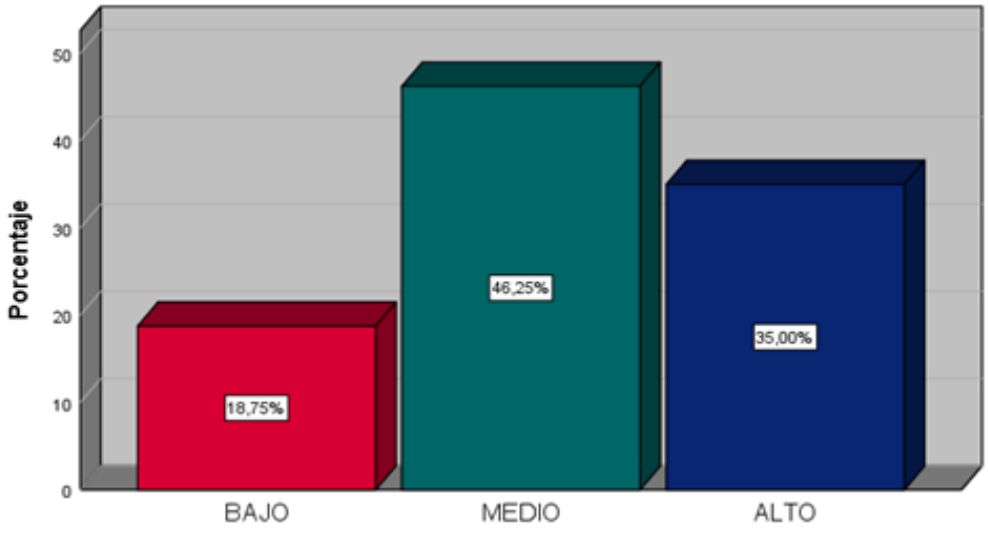
Distribución de frecuencia D6: Disponibilidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Bajo	15	18,8	18,8	18,8
Medio	37	46,3	46,3	65,0
Alto	28	35,0	35,0	100,0
Total	80	100,0	100,0	

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 7

D6: Disponibilidad



Interpretación: Analizando los hallazgos se verifica la distribución de la Disponibilidad, el 18.75% (15 participantes) afirman que hay un bajo tiempo de respuesta de la información requerida, mientras que el 46.25% (37 participantes), perciben que la cantidad de copias de respaldo de información tiene un nivel medio en cuanto a su disponibilidad; y el 35.00% (28 participantes) del total de encuestados, señalan que el nivel de complejidad de contraseñas, se evidencia como alto.

TABLAS CRUZADAS

Tabla 10

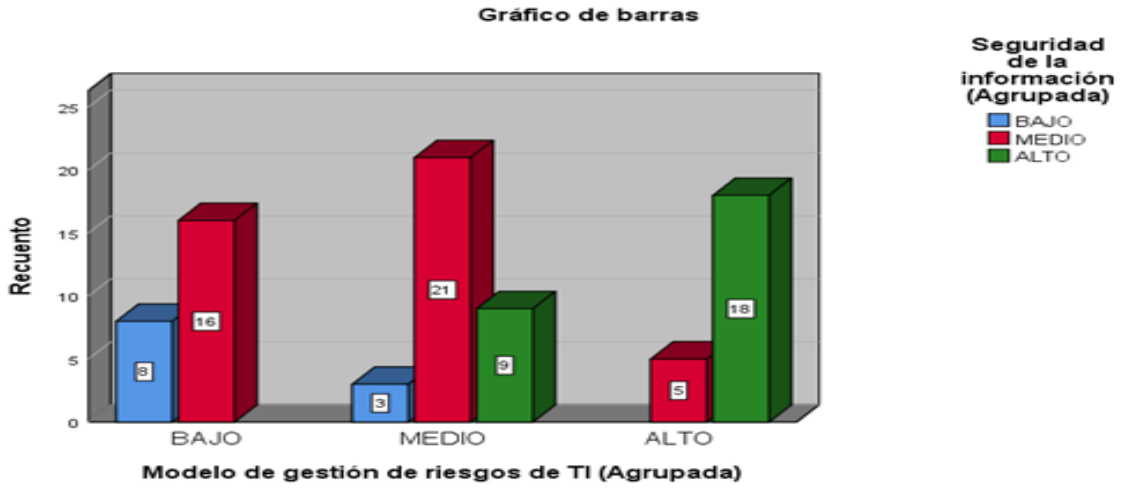
Comparación entre variables Modelo de gestión de riesgos de TI y Seguridad de la información

			Confidencialidad			
			Bajo	Medio	Alto	Total
Modelo de gestión de riesgos de TI (Agrupada)	BAJO	Recuento	8	16	0	24
		% del total	10,0%	20,0%	0,0%	30,0%
	MEDIO	Recuento	3	21	9	33
		% del total	3,8%	26,3%	11,3%	41,3%
	ALTO	Recuento	0	5	18	23
		% del total	0,0%	6,3%	22,5%	28,7%
Total		Recuento	11	42	27	80
		% del total	13,8%	52,5%	33,8%	100,0%

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 8

Comparación entre variables Modelo de gestión de riesgos de TI y Seguridad de la información.



Interpretación: Se visualizan los hallazgos referentes a las variables de estudio. Respecto al 30.00% que afirma que está en un nivel bajo, el 10.00% (8 participantes) percibe que la seguridad de la información es baja. De igual forma del 41.30% que afirma que está en un nivel medio, un 26.30% (21 participantes) perciben un nivel medio. En relación al alto, del total de 28.70% que afirma que está en un nivel alto, un 22.50% (18 participantes) afirman que es alta.

Tabla 11

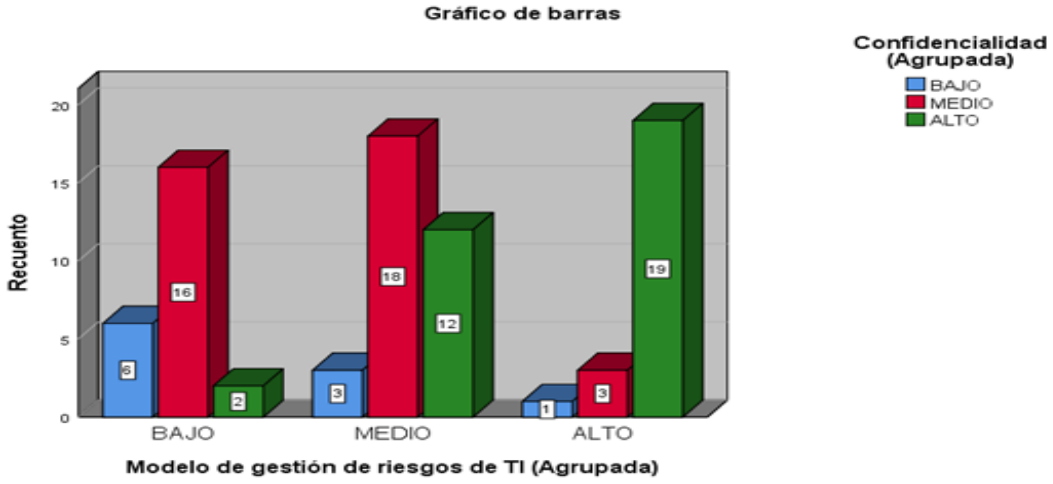
Comparación V1: Modelo de gestión de riesgos de TI y D4: Confidencialidad

			Confidencialidad			
			Bajo	Medio	Alto	Total
Modelo de gestión de riesgos de TI (Agrupada)	BAJO	Recuento	6	16	2	24
		% del total	7,5%	20,0%	2,5%	30,0%
	MEDIO	Recuento	3	18	12	33
		% del total	3,8%	22,5%	15,0%	41,3%
	ALTO	Recuento	1	3	19	23
		% del total	1,3%	3,8%	23,8%	28,7%
Total		Recuento	10	37	33	80
		% del total	12,5%	46,3%	41,3%	100,0%

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 9

Comparación entre la variable Modelo de gestión de riesgos de TI y la confidencialidad.



Interpretación: Analizando los hallazgos se demuestra que, respecto al 30.00% afirma que está en un nivel bajo, el 7.50% (6 participantes) percibe que la confidencialidad es baja. De igual forma del 41.30% que afirma que está en un nivel medio, un 22.50% (18 participantes) perciben un nivel medio de la confidencialidad. En relación al nivel alto, del total de 28.70% que afirma que está en un nivel alto, un 23.80% (19 participantes) afirman que la confidencialidad es alta.

Tabla 12

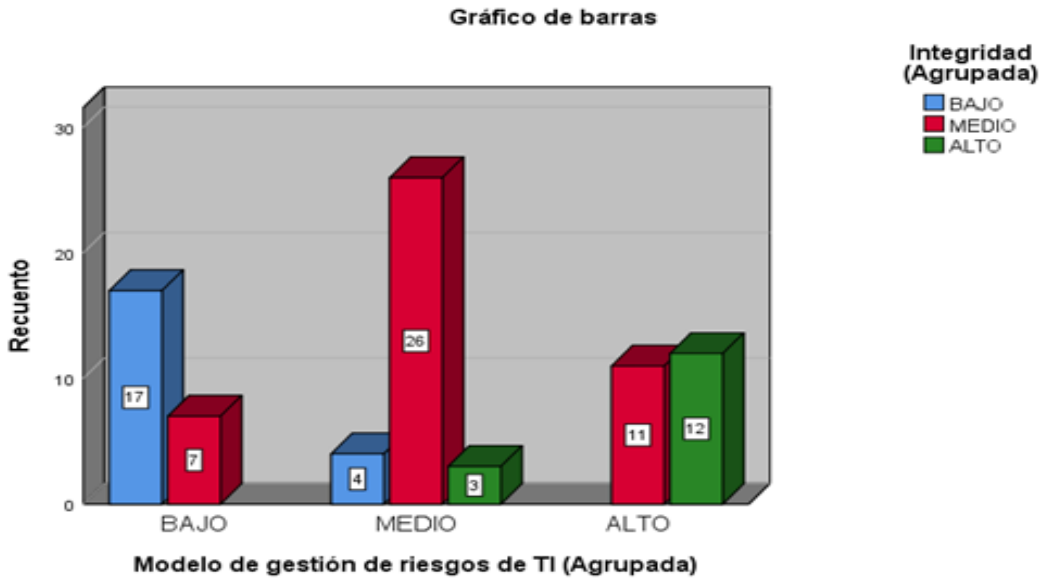
Comparación V1: Modelo de gestión de riesgos de TI y D5: Integridad

			Integridad			
			Bajo	Medio	Alto	Total
Modelo de gestión de riesgos de TI (Agrupada)	BAJO	Recuento	17	7	0	24
		% del total	21,3%	8,8%	0,0%	30,0%
	MEDIO	Recuento	4	26	3	33
		% del total	5,0%	32,5%	3,8%	41,3%
	ALTO	Recuento	0	11	12	23
		% del total	0,0%	13,8%	15,0%	28,7%
Total		Recuento	21	44	15	80
		% del total	26,3%	55,0%	18,8%	100,0%

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 10

Comparación entre la variable Modelo de gestión de riesgos de TI y la integridad.



Interpretación: De la tabla 12 y figura 10, visualizamos los resultados, respecto al 30.00% que afirma que está en un nivel bajo, el 21.30% (17 participantes) percibe que la integridad es baja. De igual forma del 41.30% que afirma que está en un nivel medio, un 32.50% (26 participantes) perciben un nivel medio de la integridad. En relación al nivel alto, del total de 28.70% que afirma que está en un nivel alto, un 15.00% (12 participantes) afirman que la integridad es alta.

Tabla 13

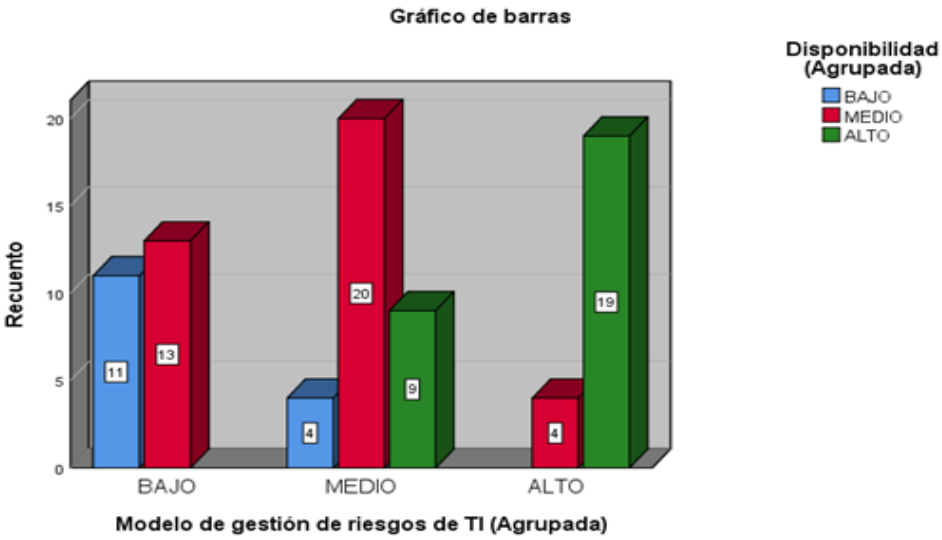
Tabla de comparación V1: Modelo de gestión de riesgos de TI y Disponibilidad

			Disponibilidad			
			Bajo	Medio	Alto	Total
Modelo de gestión de riesgos de TI (Agrupada)	BAJO	Recuento	11	13	0	24
		% del total	13,8%	16,3%	0,0%	30,0%
	MEDIO	Recuento	4	20	9	33
		% del total	5,0%	25,0%	11,3%	41,3%
	ALTO	Recuento	0	4	19	23
		% del total	0,0%	5,0%	23,8%	28,7%
Total		Recuento	15	37	28	80
		% del total	18,8%	46,3%	35,0%	100,0%

Fuente: SPSS Statistics versión 25.0 en base a las encuestas

Figura 11

Comparación entre la variable Modelo de gestión de riesgos de TI y la dimensión disponibilidad.



Interpretación: De la tabla 13 y figura 11, visualizamos los resultados, respecto al 30.00% que afirma que está en un nivel bajo, el 13.80% (11 participantes) percibe que la disponibilidad es baja. De igual forma del 41.30% que afirma que está en un nivel medio, un 25.00% (20 participantes) perciben un nivel medio de la disponibilidad. En relación al nivel alto, del total de 28.70% que afirma que está en un nivel alto, un 23.80% (19 participantes) afirman que la disponibilidad es alta.

Análisis Inferencial

Contrastación de Hipótesis General

Se detalla de la siguiente manera: p = Sig

H_o. El modelo de gestión de riesgos de TI no incide significativamente en la seguridad de la información de una institución del estado.

H_a: El modelo de gestión de riesgos de TI incide significativamente en la seguridad de la información de una institución del estado.

Decisión: p < 0.05: se rechaza H_o

p > 0.05: se acepta H_o

Tabla 14

Información de ajuste de modelo para la hipótesis general

Modelo	-2 log de la verosimilitud	Chi-cuadrado	gl	Sig.
Sólo intersección	58,406			
Final	16,254	42,151	2	,000

Fuente: base de datos contenida en SPSS v. 25

En cuanto al valor de Sig. para las variables, es menor a 0.05 (0.000 < 0.05), dicho resultado se ajusta al (RLO), el cual indica que la variable 1 incide en la variable 2.

Tabla 15

Prueba Pseudo R cuadrado de la V1 en la V2

Pesudo R cuadrado	
Cox y Snell	,410
Nagelkerke	,477
McFadden	,269

Fuente: base de datos contenida en SPSS v. 25

Interpretación: Del análisis de la Tabla 15, se puede evidenciar a través del coeficiente de Nagelkerke que el fenómeno de estudio 1 incide en un 47.70% en la variable 2.

Tabla 16

Estimaciones de los parámetros de la incidencia de la V1 en la V2

		Estimación	Error típ.	Wald	gl	Sig.	Intervalo de confianza 95%	
							Límite inferior	Límite superior
Umbral	[V.2 = 1]	-5,132	,796	41,527	1	,000	-6,693	-3,571
	[V.2 = 2]	-1,288	,506	6,478	1	,011	-2,281	-,296
Ubicación	[V.1=1]	-4,548	,858	28,068	1	,000	-6,230	-2,865
	[V.1=2]	-2,394	,639	14,026	1	,000	-3,647	-1,141
	[V.1=3]	0[a]	.	.	0	.	.	.

Fuente: base de datos contenida en SPSS v. 25

Interpretación: Conforme a lo observado de la Tabla 16, se verifica que el valor de p es menor a 0.000 (0.000 y 0.011) y los coeficientes de Wald son mayores a 4 de ello queda demostrada la incidencia del fenómeno de estudio 1 en el 2; por consiguiente, es negada y se afirma la alternativa.

Contrastación de Hipótesis Especifica 1

H_0: El modelo de gestión de riesgos de TI no incide significativamente en la confidencialidad de la seguridad de la información de una institución del estado.

H_a: El modelo de gestión de riesgos de TI incide significativamente en la confidencialidad de la seguridad de la información de una institución del estado.

Decisión:

Si valor $p < 0.05$, se rechaza H_o

$p > 0.05$, se acepta H_o

Tabla 17

Información de ajuste de modelo para la hipótesis específica 1

Modelo	-2 log de la verosimilitud	Chi-cuadrado	gl	Sig.
Sólo intersección	48,704			
Final	19,367	29,337	2	,000

Fuente: base de datos contenida en SPSS v. 25

En cuanto al valor de Sig. para las variables, es menor a 0.05 (0.000 < 0.05), dicho resultado se ajusta al (RLO), el cual indica que el fenómeno de estudio 1 incide en la confidencialidad.

Tabla 18

Prueba Pseudo R cuadrado de la V1 en la confidencialidad

Pesudo R cuadrado	
Cox y Snell	,307
Nagelkerke	,357
McFadden	,187

Fuente: base de datos contenida en SPSS v. 25

Interpretación: De los resultados de la Tabla 18, se puede evidenciar a través del coeficiente de Nagelkerke que el cual indica que el fenómeno de estudio 1 incide en un 35.70% en la confidencialidad.

Tabla 19

Estimaciones de los parámetros de la V1en la D4: confidencialidad

		Estimación	Error típ.	Wald	gl	Sig.	Intervalo de confianza 95%	
							Límite inferior	Límite superior
Umbral	[D.4 = 1]	-4,472	,706	40,154	1	,000	-5,856	-3,089
	[D.4 = 2]	-1,518	,542	7,831	1	,005	-2,581	-,455
Ubicación	[V.1=1]	-3,523	,747	22,228	1	,000	-4,987	-2,058
	[V.1=2]	-2,096	,646	10,528	1	,001	-3,361	-,830
	[V.1=3]	0[a]	.	.	0	.	.	.

Fuente: base de datos contenida en SPSS v. 25

Interpretación: Conforme a lo observado de la Tabla 19, se verifica que el valor de p es menor a 0.000 (0.000 y 0.005) y los coeficientes de Wald son mayores a 4 de ello queda demostrada la incidencia del fenómeno de estudio 1 en la confidencialidad; por consiguiente, es negada y se afirma la alternativa.

Contrastación de Hipótesis Especifica 2

H_0: El modelo de gestión de riesgos de TI no incide significativamente en la integridad de la seguridad de la información de una institución del estado.

H_a: El modelo de gestión de riesgos de TI incide significativamente en la integridad de la seguridad de la información de una institución del estado.

Decisión:

Si valor $p < 0.05$, se rechaza H_o

$p > 0.05$, se acepta H_o

Tabla 20

Información de ajuste de modelo para la hipótesis específica 2

Modelo	-2 log de la verosimilitud	Chi-cuadrado	gl	Sig.
Sólo intersección	67,615			
Final	13,858	53,757	2	,000

Fuente: base de datos contenida en SPSS v. 25

En cuanto al valor de Sig. para las variables, es menor a 0.05 (0.000 < 0.05), dicho resultado se ajusta al (RLO), el cual indica que el fenómeno de estudio 1 incide en la integridad.

Tabla 21

Prueba Pseudo R cuadrado de la V1 en la integridad

Pesudo R cuadrado	
Cox y Snell	,489
Nagelkerke	,567
McFadden	,338

Fuente: base de datos contenida en SPSS v. 25

Interpretación: De los resultados de la Tabla 21, se puede evidenciar a través del coeficiente de Nagelkerke que el cual indica que el fenómeno de estudio 1 incide en un 56.70% en la integridad.

Tabla 22

Estimaciones de los parámetros de la V1en la D5: integridad

		Estimación	Error típ.	Wald	gl	Sig.	Intervalo de confianza 95%	
							Límite inferior	Límite superior
Umbral	[D.5 = 1]	-4,600	,823	31,248	1	,000	-6,212	-2,987
	[D.5 = 2]	-,106	,416	,065	1	,799	-,921	,709
Ubicación	[V.1=1]	-5,493	,934	34,592	1	,000	-7,324	-3,663
	[V.1=2]	-2,529	,728	12,085	1	,001	-3,955	-1,103
	[V.1=3]	0[a]	.	.	0	.	.	.

Fuente: base de datos contenida en SPSS v. 25

Interpretación: Conforme a lo observado de la Tabla 22, se verifica que, en el nivel bajo de la integridad, el valor de p es menor a 0.000 (0.000) y el coeficiente de Wald es mayor a 4 de ello queda demostrada la incidencia del fenómeno de estudio 1 en la integridad de la seguridad de la información de una entidad del estado, Lima 2022; cabe recalcar que se observa una incidencia significativa en el nivel bajo y medio de la variable independiente en la variable dependiente siendo p menor a 0.000 (0.000 y 0.001) y el coeficiente de Wald es mayor a 4, por consiguiente, es negada y se afirma la alternativa.

Contrastación de Hipótesis Especifica 3

H_0: El modelo de gestión de riesgos de TI no incide significativamente en la disponibilidad de la seguridad de la información de una institución del estado.

H_a: El modelo de gestión de riesgos de TI incide significativamente en la disponibilidad de la seguridad de la información de una institución del estado.

Decisión:

Si valor $p < 0.05$, se rechaza H_o

$p > 0.05$, se acepta H_o

Tabla 23

Información de ajuste de modelo para la hipótesis específica 3

Modelo	-2 log de la verosimilitud	Chi-cuadrado	gl	Sig.
Sólo intersección	64,955			
Final	16,228	48,727	2	,000

Fuente: base de datos contenida en SPSS v. 25

En cuanto al valor de Sig. para las variables, es menor a 0.05 (0.000 < 0.05), dicho resultado se ajusta al modelo de regresión logística ordinal (RLO), el cual indica que el fenómeno de estudio 1 incide en la disponibilidad.

Tabla 24

Prueba Pseudo R cuadrado de la V1en la disponibilidad

Pesudo R cuadrado	
Cox y Snell	,456
Nagelkerke	,522
McFadden	,293

Fuente: base de datos contenida en SPSS v. 25

Interpretación: Del análisis de la Tabla 24, se puede evidenciar a través del coeficiente de Nagelkerke que el cual indica que el fenómeno de estudio 1 incide en un 52.20% en la disponibilidad.

Tabla 25

Estimaciones de los parámetros de la V1en la D6: disponibilidad

		Estimación	Error típ.	Wald	gl	Sig.	Intervalo de confianza 95%	
							Límite inferior	Límite superior
Umbral	[D.6 = 1]	-4,956	,776	40,740	1	,000	-6,478	-3,434
	[D.6 = 2]	-1,567	,551	8,076	1	,004	-2,647	-,486
Ubicación	[V.1=1]	-4,866	,851	32,722	1	,000	-6,534	-3,199
	[V.1=2]	-2,671	,675	15,680	1	,000	-3,993	-1,349
	[V.1=3]	0[a]	.	.	0	.	.	.

Fuente: base de datos contenida en SPSS v. 25

Interpretación: Conforme a lo observado de la Tabla 25, se verifica que el valor de p es menor a 0.000 (0.000 y 0.004) y los coeficientes de Wald son mayores a 4 de ello queda demostrada la incidencia del fenómeno de estudio 1 en la disponibilidad de la seguridad de la información de una entidad del estado, Lima 2022; por consiguiente, es negada y se afirma la alternativa.

V. DISCUSIÓN

En cuanto a la discusión, como objetivo general del estudio realizado se tuvo el determinar la incidencia del modelo de gestión de riesgos de TI en la seguridad de la información de una institución del estado; como objetivos específicos; determinar la incidencia del modelo de gestión de riesgos de TI en la confidencialidad, en la integridad y en la disponibilidad de la seguridad de la información de una institución del estado; asimismo, los resultados al aplicar el cuestionario le dan validez y confiabilidad.

En cuanto a la hipótesis general, se concluye que el modelo de gestión de riesgos de TI tiene una incidencia de 47.70% en la seguridad de la información en una institución del estado, Lima 2022; debido a que estas variables presentan un nivel de significancia de p= 0.000 (p < 0.050); en donde es rechazada la hipótesis nula y es aceptada la hipótesis alterna, se afirma que el modelo de gestión de riesgo de TI incide significativamente en la seguridad de la información. Así mismo la investigación denota la confidencialidad, integridad, disponibilidad.

Hay que mencionar que, concuerda con los resultados conseguidos en el estudio presentado por Otoya (2018) en su tesis titulada “Gestión de riesgos de TI en la seguridad de la información del programa de desarrollo productivo agrario rural”, donde se buscó “determinar la influencia de la gestión de riesgos de TI en la seguridad de la información”, donde p_valor es igual a 0.035 frente al nivel de significancia α igual a 0.05 (p < α), por lo cual se rechazó la hipótesis nula, la data obtenida de las variables son dependientes, ello indica que la seguridad de la información depende de la gestión de riesgos de TI. Además, el modelo presentado que estaría explicando la dependencia de la seguridad de la información en 44.00% de la gestión de riesgos de TI, llegó a la conclusión de que los profesionales admiten no conocer a fondo los procedimientos que aumentan la seguridad de la información, por lo cual no lo ponen en práctica en sus proyectos y a su vez les preocupa la sensación con que perciben la seguridad sus clientes; es por esta razón que la Secretaria de Gobierno Digital, dispuso, de forma obligatoria el uso de la “Norma Técnica Peruana: NTP – ISO 17999:2014 EDI para la Gestión de la Seguridad de la Información”.

También es similar los resultados propuestos, en la investigación de Calderón (2018) en su tesis titulada “Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación”, sostuvo que desde la forma como es percibido por los participantes, se obtuvieron los resultados: para el nivel bueno un 40.96%, un 48.19% para el nivel regular y sólo un 3.61% la ubica en un nivel malo en la seguridad de la información y la gestión de riesgos. Se concluyó que entre de la seguridad de la información y la gestión de riesgos se da la existencia de una relación altamente significativa, con los valores obtenidos en las pruebas efectuadas, para $p = 0.000$ ($p < 0.05$) con un Rho de Spearman de 0.886, por consiguiente, se aceptó la hipótesis alterna y la hipótesis nula se rechazó. Es decir, hubo factores similares como la confidencialidad, integridad y disponibilidad de la información.

En lo referente a la primera hipótesis específica: El modelo de gestión de riesgos de TI incide significativamente en la confidencialidad de la seguridad de la información de una institución del estado. Para corroborar la hipótesis, luego de aplicar la estadística correspondiente, se halló que el valor de p es 0.000 ($p<0.05$), resultado en la tabla 17; por lo cual Ho es rechazada y Ha es aceptada, el Modelo de gestión de riesgos de TI incide significativamente en la confidencialidad de la información en una institución del estado, Lima 2022, con un resultado estadístico de 35.70%, dicho valor se representa el porcentaje de incidencia directa. Al aplicar el programa estadístico, lo que se puede visualizar en la tabla 7 y figura 5, se puede afirmar que del total de participantes de la encuesta, el 12.50% (10 encuestados) perciben que en la confidencialidad de la información de la institución hay un nivel bajo, mientras que el 46.25% (37 encuestados), considera que la confidencialidad se ubica en un nivel medio puesto que al realizar las pruebas de tráfico de red existen limitaciones; y el 41.25% (33 encuestados), señalan que en la políticas de seguridad de la información, hay un nivel alto.

Dichos resultados, son comparables con la investigación de Arévalo, Cedillo & Moscoso (2017), donde concluyeron que la mayor parte de los riesgos, un 56.00% se ubican en el nivel alto luego de ser analizados y valorados, pues éstos fueron provocados deliberadamente o por error, el 32% de riesgos, se catalogaron como un nivel extremo, el 12% fueron catalogados de nivel medio y como nivel bajo

ninguno, puesto que cada uno de ellos pueden ocurrir y sus consecuencias afectarían a una o más dimensiones de seguridad de la información (confidencialidad, integridad o disponibilidad).

Similares a los resultados de la investigación propuesta por Calderón (2019), quien obtuvo para la confidencialidad de la seguridad de la información, que un 44.00% la percibe en nivel bajo, 40.00% en nivel medio y 16.00% nivel alto; para la integridad, que un 44.00% la percibe en nivel bajo, 44.00% en nivel medio y 12.00% alto; y para la disponibilidad, un 60.00% la percibe en nivel bajo, 28.00% en nivel medio y 12.00% alto, su grado de significancia fue 0.000 ($p < 0.05$), concluyendo así "una relación directa entre Gestión de riesgos y Seguridad de la información en el Programa Fortalece Perú del MTPE, 2019"

La segunda hipótesis específica: El modelo de gestión de riesgos de TI incide significativamente en la integridad de la seguridad de la información de una institución del estado. A través de lo mostrado en la tabla 12 y figura 10, se corroboró y podemos visualizar los resultados. Respecto al 30.00% que afirma que el Modelo de gestión de riesgos de TI está en un nivel bajo, el 21.30% (17 participantes) percibe que la integridad es baja. De igual forma del 41.30% que afirma que dicho Modelo está en un nivel medio, un 32.50% (26 participantes) perciben un nivel medio de la integridad. En relación al nivel alto, del total de 28.70% que afirma que el dicho Modelo está en un nivel alto, un 15.00% (12 participantes) afirman que la integridad es alta. Del análisis de la Tabla 20, se obtiene el valor de p es 0.000 ($p < 0.05$); por consiguiente, Ho se rechaza y se acepta la Ha, con un resultado estadístico de 56.70%, dicho valor quiere decir que el modelo de gestión de riesgos de TI tiene una incidencia positiva muy fuerte en la integridad de la seguridad de la información de una institución del estado, Lima 2022.

Esto resulta divergente a lo ocurrido en el estudio realizado por Arévalo, Cedillo & Moscoso (2017), donde se identificaron un total de 201 activos, un 59.20 %, calificados con valor alto en relación a las dimensiones de seguridad; un 31.84% con valor medio, y ninguno tuvo valor bajo, puesto la mayor parte de ellos, como son información física, electrónica, software, hardware, telecomunicaciones, etc, poseen un nivel crítico en relación a la integridad de la seguridad de la información

que se gestiona en el área sobre procesos y normas, órdenes de producción, recursos de procedimientos de elaboración, base de datos, etc, se formuló un proyecto de tratamiento de riesgos el cual se monitorea y verifica su cumplimiento.

A su vez, Calderón (2018), en su investigación, quien obtuvo como resultado de los participantes, en relación a la dimensión integridad, ubican en el nivel bueno al 53.01%, en el regular al 43.37% y en al malo al 3.61%, además, se obtuvo un grado de significancia de 0.000 ($p < 0.05$), un $rs = 0.886$, por lo tanto, se aceptó la hipótesis alterna y la hipótesis nula se rechazó, de esta manera se aprecia entre la seguridad de la información y la gestión de riesgos, una relación significativa fuerte. Acorde a lo hallado, los encargados de la oficina de TI, deberán establecer planes claros, que incluyan políticas de seguridad, constantes capacitaciones, adquisición de software y hardware para preservar la confidencialidad, integridad y disponibilidad de la información, asimismo, reducir los riesgos y asegurar la continuidad del negocio de la institución investigada.

Finalmente, La tercera hipótesis específica: El modelo de gestión de riesgos de TI incide significativamente en la disponibilidad de la seguridad de la información de una institución del estado, al respecto, en la tabla 9 y figura 7, se verifica la distribución de la Disponibilidad, el 18.75% (15 participantes) afirman que hay un bajo tiempo de respuesta de la información requerida, mientras que el 46.25% (37 participantes), perciben que la cantidad de copias de respaldo de información tiene un nivel medio en cuanto a su disponibilidad; y el 35.00% (28 participantes) del total de encuestados, señalan que el nivel de complejidad de contraseñas, se ubica en un nivel alto. Asimismo, se comprobó en la tabla 13 y figura 11 respecto al modelo de gestión de riesgos de TI con la disponibilidad, del 30.00% que afirma que el Modelo de gestión de riesgos de TI está en un nivel bajo, el 13.80% (11 participantes) percibe que la disponibilidad es baja. De igual forma del 41.30% que afirma que dicho Modelo está en un nivel medio, un 25.00% (20 participantes) perciben un nivel medio de la disponibilidad. Finalmente, respecto al nivel alto, del total de 28.70% que afirma que dicho Modelo está en un nivel alto, un 23.80% (19 participantes) afirman que la disponibilidad es alta. Conforme a la tabla 23 se obtiene el valor de p es 0.000 ($p<0.05$); por lo que la H0 es rechazada y la Ha se acepta; con un resultado estadístico de 52.20%, lo que demuestra que el modelo

de gestión de riesgos de TI incide significativamente en la disponibilidad de la información de una institución del estado, Lima 2022.

Una investigación importante a nuestro modo de ver es la de Calderón (2019), quien obtuvo para la disponibilidad de la información, un 60.00% la percibe en nivel bajo, 28.00% en nivel medio y 12.00% alto, del mismo modo para las otras dimensiones de la seguridad de la información como son la confidencialidad e integridad, se apreció para la confidencialidad de la seguridad de la información, que un 44.00% la percibe en nivel bajo, 40.00% en nivel medio y 16.00% nivel alto; para la integridad, que un 44.00% la percibe en nivel bajo, 44.00% en nivel medio y 12.00% alto, sumado a sus hallazgos, su grado de significancia fue 0.000 ($p < 0.05$), concluyendo así “una relación directa entre Gestión de riesgos y Seguridad de la información en el Programa Fortalece Perú del MTPE, 2019”.

Por otro lado, es comparable con los resultados hallados en la investigación de Ñañez (2021), por consiguiente, cuyos resultados fueron de 69.00% para el nivel medio de la confidencialidad es deficiente, el 65.50% para el nivel medio de la integridad de datos lo que indica que no hay prevención de las adulteraciones de datos, el 58.60% para el nivel medio de la disponibilidad, lo cual indica que el acceso a los datos es inadecuado respecto a la seguridad de la información, además insta a poner en práctica los lineamientos del modelo para crear un cultura de gestión de riesgos de TI adecuada que fortalezca la seguridad de la información.

Estos resultados son comparables con los hallazgos en la investigación de Huaura (2019), quien obtuvo un valor rs de 0.592, dicho valor significa la existencia de una correlación positiva media entre la gestión de riesgos y la seguridad de la información. Por consiguiente, “una gestión de riesgos de seguridad de la información basada en un estándar internacional NTP ISO/IEC 31000 en las Empresas del sector Telecomunicaciones” influye en el control de los riesgos de seguridad de la información, se afirma que la hipótesis pasa la prueba. El no tener controles al gestionar los accesos y la utilización de la tecnología, podría aumentar los riesgos relacionado a la seguridad de la información.

Dicho esto, no queda duda de la importancia de seguir los lineamientos del modelo de gestión de riesgos de TI, a través de la secuencia de pasos establecidas,

se podrán tener mapeado los elementos relevantes en la institución e identificar los riesgos a los que están expuestos, y que medidas o acciones tomar que refuercen la seguridad de la información y eviten pérdidas a gran escala.

V. CONCLUSIONES

Conforme a los resultados encontrados, se manifiestan las conclusiones siguientes:

Primera:

Se ha determinado que el fenómeno indagado 1 incide en la seguridad de la información en una institución del estado, Lima 2022. Cuyo resultado estadístico de 47.70% y positiva (p = .000 menor que p = .050).

Segunda:

Se ha determinado que el fenómeno indagado 1 incide significativamente en la confidencialidad de la información en una institución del estado, Lima 2022. Cuyo resultado de 35.70%, por tanto, posee una relación positiva significativa, se encontró que, del total de la encuesta, el 12.50% consideran que hay un nivel bajo en la confidencialidad de la información de la institución, mientras que el 46.25% (37 encuestados), considera que la confidencialidad se ubica en un nivel medio puesto que al realizar las pruebas de tráfico de red existen limitaciones; y el 41.25% señalan que, en las políticas de seguridad de la información, hay un nivel alto.

Tercera:

Se ha identificado una incidencia significativa del fenómeno indagado 1 sobre la integridad de la información en una institución del estado, Lima 2022, con un resultado de 56.70%. Respecto al 30.00% que afirma que el fenómeno indagado 1 está en un nivel bajo, el 21.30% (17 participantes) percibe que la integridad es baja. De igual forma del 41.30% que afirma que fenómeno indagado 1 está en un nivel medio, un 32.50% (26 participantes) perciben un nivel medio de la integridad. En relación al nivel alto, del total de 28.70% que afirma que fenómeno indagado 1 está en un nivel alto, un 15.00% (12 participantes) afirman que la integridad es alta, dichos resultados corroboran la incidencia del fenómeno indagado 1 y el 2.

Cuarta:

Se ha determinado el fenómeno indagado 1 incide significativamente en la disponibilidad de la información en una institución del estado, Lima 2022, cuyo

resultado fue 52.20%. Se comprobó que el fenómeno indagado 1 con la disponibilidad de un total del 30.00% que afirma que el fenómeno indagado 1 está en un nivel bajo, el 13.80% (11 participantes) percibe que la disponibilidad es baja. De igual forma del 41.30% que afirma que fenómeno indagado 1 está en un nivel medio, un 25.00% (20 participantes) perciben un nivel medio de la disponibilidad. En relación al nivel alto, del total de 28.70% que afirma que fenómeno indagado 1 está en un nivel alto, un 23.80% (19 participantes) afirman que la disponibilidad es alta.

VI. RECOMENDACIONES

Primera:

Se aconseja al Director de la oficina de la institución del estado, mantener una comunicación constante y abierta donde pueda difundir el modelo de gestión de riesgos de TI, basado en la ISO 27005:2018, ya que permite minimizar los riesgos y mantener la seguridad de la información, identificando las amenazas, midiendo el impacto y aplicando las salvaguardas del modelo, así como también concientizar a los trabajadores sobre mantener la confidencialidad, la integridad y la disponibilidad de la información.

Segunda:

Para lograr la confidencialidad de la seguridad de la información, se recomienda al director de la oficina de la institución del estado, cumplir con las políticas de seguridad dispuestas, aplicar las pruebas de tráfico de red, tener un personal especializado que comprometa a los trabajadores con la confidencialidad de la información siguiendo los lineamientos del modelo.

Tercera:

La integridad de datos tiene una incidencia positiva muy fuerte con la seguridad de la información, lo que compromete a que el director de la oficina de la institución del estado inste a los encargados de la oficina de TI, deberán establecer planes claros, que incluyan políticas de seguridad, constantes capacitaciones, adquisición de software y hardware para preservar la confidencialidad, integridad y disponibilidad de la información, asimismo, reducir los riesgos y asegurar la continuidad del negocio de la institución investigada.

Cuarta:

La disponibilidad tiene una incidencia significativamente con el sistema de información, motivo por el cual, a través del director de la oficina de la institución del estado, el área de Tecnologías de la Información deberá contar con un plan que incluya controles frente a posibles riesgos que pongan en peligro la continuidad de los servicios.

REFERENCIAS

Agrawal, V. (2016). Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard. *ISBN: 978-1-84102-413-4*, 101-111. Retrieved from https://www.cscan.org/?page=openaccess&eid=17&id=304

Arévalo Moscoso, F. M., Cedillo Orellana, I. P., & Moscoso Bernal, S. A. (2017). Metodología ágil para la gestión de riesgos informáticos. *Revista Killkana Técnica vol.1 núm.2*, 31-42. Retrieved from https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/81

Avenía Delgado, C. A. (2017). Fundamentos de seguridad informática. *Fondo editorial Areandino*, 8-61. Retrieved from https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%C3%A1tica.pdf?sequence=1&isAllowed=y

Baena Paz, G. (2017). *Metodología de la Investigación.* México: 3a edición - Grupo Editorial Patria. All rights reserved. Retrieved from http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Banda Santisteban, J. C. (2019). *Modelo basado en metodologías de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque.* Lambayeque-Perú: Maestría en Ingeniería de Sistemas: Dirección Estratégica de Tecnologías de Información. Retrieved from https://tesis.usat.edu.pe/handle/20.500.12423/2159

Barafort, B., Mesquida Lluís, A., & Mas, A. (2018). Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces-volume 60*, 57-66. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0920548918300497?via%3Dihub

Barriga, G. (2019). Gestión integral de riesgos y antisoborno: un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001. *Revista Universidad y Empresa*. Retrieved from https://revistas.urosario.edu.co/index.php/empresa/article/view/6089

Barzaga Sablón, O. S., Vélez Pincay, H., Nevárez Barberán, J., & Arroyo Cobeña, M. V. (2019). Gestión de la información y toma de decisiones en organizaciones educativas. *Revista de Ciencias Sociales (Ve), vol. XXV, núm. 2*, 4-11. Retrieved from https://www.redalyc.org/articulo.oa?id=28059953010

Benqdara, S., Elfergani, A., & Sultan, A. (2020). Assessment of Security Issues in Banking Sector of Libya. *International Journal of Computer Applications*,

176. Retrieved from https://www.ijcaonline.org/archives/volume176/number13/benqdara-2020-ijca-920011.pdf

Brunner, M. (2020). Risk management practices in information security: Exploring the status quo in the DACH region, Computers & Security. *Volume 92, 2020, 101776, ISSN 0167-4048*. Retrieved from https://doi.org/10.1016/j.cose.2020.101776.

Calderón Sánchez, J. A. (2019). *Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018.* Lima: Repositorio de la Universidad César Vallejo. Retrieved from https://repositorio.ucv.edu.pe/handle/20.500.12692/30014

Calderon Taboada, L. (2019). *Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE, 2019.* Lima: Universidad Cesar Vallejo. Retrieved from https://hdl.handle.net/20.500.12692/46705

Cantalejo García, B. (2019). *Elaboración de un plan director de seguridad para la empresa TrendTip.* Catalunya: Universitat Oberta de Catalunya. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/96986/9/bcantalejogTFM0619memoria.pdf

Colina Vargas, A. M., & Túa Ollarves, J. J. (2020). Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI. 3. Retrieved from https://revistas.uide.edu.ec/index.php/innova/article/view/1608

Corda, M. C., Viñas, M., & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Brapci*. Retrieved from https://brapci.inf.br/index.php/res/v/66060

Cruz Cabrera , W. E. (2019). *Modelo de gestión de riesgos de TI enfocado en estándares adaptados para contribuir en la protección del activo de TI en el sector de distribuidoras de la región Lambayeque.* Chiclayo-Perú: Universidad Católica Santo Toribio de Mogrovejo. Retrieved from http://hdl.handle.net/20.500.12423/2777

Deloitte, T. (2019). Tendencias en Gestión de Ciber Riesgos y Seguridad de la Información en América Latina y Caribe (AL&C). *Tendencias 2019*, 1-5. Retrieved from https://www2.deloitte.com/pe/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

Didraga, O., Brandas, C., Batagan, L., & Alecu, F. (2019). Characteristic of effective It project risk management romanian it companies. *Economic Computation and Economic Cybernetics Studies and Research, Issue 4/2019; Vol. 53*. Retrieved from http://ecocyb.ase.ro/nr2019_4/11.%20DIDRAGA%20Otniel,%20Lorena%20Batagan.pdf

Edirisinghe , V. N., & Pinsker, R. (2019). IT risk management: interrelationships based on strategy implementation. *International Journal of Accounting & Information Management, Vol. 28 No. 3*, 553-575. Retrieved from https://doi.org/10.1108/IJAIM-08-2019-0093

Gómez Orjuela, F. H., & Valencia 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.* Medellín-Colombia: Repositorio Institucional ITM. Retrieved from http://hdl.handle.net/20.500.12622/5197

González Brito, H. R., Montesino Perurena, R., & Gainza Reyes, D. (2021). Riesgos de Seguridad en Pruebas de Penetración Web. 3. Retrieved from https://www.redalyc.org/articulo.oa?id=378370462014

Herath Thilini, B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media Users: A systematic literature review. *Academic Editor: Xavier Bellekens*, 1-18. Retrieved from https://www.mdpi.com/2624-800X/2/1/1

Hernandez Mendoza, S., & Duana Avila, D. (n.d.). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA,* *9*(17), 51-53. doi:https://doi.org/10.29057/icea.v9i17

Hernández Sampieri, R., & Mendoza, C. (2018). La investigación. Las rutas cuantitativa, cualitativa y mixta. *Revista Universitaria Digital de Ciencias Sociales*. Retrieved from https://virtual.cuautitlan.unam.mx/rudics/?p=2612

Huaura Mere, M. H. (2019). *Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones.* Lima-Perú: Universidad del Perú. Decana de América. Retrieved from https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/11225/Huaura_mm.pdf?sequence=1&isAllowed=y

Huayllani Muñoz, O. Y. (2020). *Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019.* Lima-Perú. Retrieved from https://repositorio.ucv.edu.pe/handle/20.500.12692/42775

INCIBE. (2019). Protección de la información. *Colección-Protege tu empresa*, 6. Retrieved from https://www.incibe.es/

ISO 31000. (2018). *ISO 31000:2018 Risk management — Guidelines.* ISO.ORG. Retrieved from https://www.iso.org/obp/ui/es/#iso:std:iso:31000:ed-2:v1:en

ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems- Requirements. *International*

Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. Retrieved from https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC 27005:2018. (2018). Information technology - Security techniques-Information security risk management. *ISO/IEC — All rights reserved*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

ISOtools Excellence. (2017). ISO 27001: Gestión de seguridad de la información mediante el modelo de pirámide. *Sistema de Gestión de Seguridad de la Información*, 1. Retrieved from https://www.isotools.org/2015/01/28/iso-27001-gestion-seguridad-informacion-mediante-modelo-piramide/

Llontop Díaz, G. C. (2018). Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks. Retrieved from https://repositorio.ucv.edu.pe/handle/20.500.12692/17596

MAGERIT. (2014). Metodología de análisis y gestión de riesgos de los sistemas de información. *Ministerio de Hacienda y Administraciones Públicas*, 1-47. Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YpWv4qjMJPY

Masso Daza, J. E. (2020). Risk management in the software life cycle: A systematic literature review. *Computer Standards & Interfaces*, 10. Retrieved from https://www.researchgate.net/publication/339747572_Risk_management_in_the_software_life_cycle_A_systematic_literature_review

Mozsar Kovacsne , A., & Michelberger, P. (2018). It risk management and application portfolio management. *Polish journal of management studies*, 112-122. Retrieved from https://doi.org/10.17512/pjms.2018.17.2.10

Najar Pacheco, J. C., & Suárez Suárez, N. E. (2016). La seguridad de la información: un activo valioso de la organización. *Revista Vínculos*, 89-97. Retrieved from https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10518/11480

Navarro Ordeñana, J. (2019). *Aplicación de gestión de riesgos tecnológicos basada en la norma ISO/IEC 27005 en el área de base de datos y sistema operativo de la Dirección de Informática y Sistemas de la DGI.* Nicaragua: Integrando la producci{on científica y técnica de la región. Retrieved from https://repositoriosiidca.csuca.org/Record/RepoUNI2860

NTP-ISO-LEC 27005. (2018). 28431_NTP-ISO-IEC 27005. *SCRIBD*. Retrieved from https://es.scribd.com/document/433791085/28431-NTP-ISO-IEC-27005

Nur Fuad , M., & Riadi, I. (2020). Riadi. Risk Management Assessment on Human Resource Information Technology Services using COBIT 5. *International Journal of Computer Applications*, 12-19. Retrieved from https://www.ijcaonline.org/archives/volume175/number23/31590-2020920756

Ñañez Campos, O. (2021). *Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas.* Tesis, Universidad Cesar Vallejo, Chiclayo. Retrieved from https://hdl.handle.net/20.500.12692/67841

Obrand, L., Holmstrom, J., & Newman, M. (2017). Navigating Rumsfeld's quadrants: A performative perspective on IT risk management. *Technology in Society*, 1-8. Retrieved from https://www.sciencedirect.com/science/article/pii/S0160791X15300634

Öbrand, L., Holmströma, J., & Newmanb, M. (2018). Navigating Rumsfeld's quadrants: A performative perspective on IT risk management. *Technology in Society-Volume 53*, 1-8. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0160791X15300634?via%3Dihub

Orehek, Š., & Petrič, G. (2021). A systematic review of scales for measuring information security culture. *Emerald insight - ISSN: 2056-4961*. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2019-0140/full/html

Ortiz Restrepo, L., & Valencia Duque, F. J. (2017). Gestión de riesgos en el sector de telecomunicaciones y su relación con los marcos internacionales de riesgos corporativos. *Revista Logos Ciencias & Tecnología- Vol. 9 Núm. 1*, 3. Retrieved from https://revistalogos.policia.edu.co:8443/index.php/rlct/issue/view/Vol.%209%2C%20N%C3%BAm.%201%20%282017%29%3A%20Preliminar%20Julio-Diciembre%29

Otoya Verástegui, M. R. (2018). *Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.* Lima: Repositorio de la Universidad César Vallejo. Retrieved from https://repositorio.ucv.edu.pe/handle/20.500.12692/16120

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology, 35*, 227-232. doi:https://dx.doi.org/10.4067/S0717-95022017000100037

Panchbhai, V. V., & Varade, S. W. (2020). A Review on Visual Secret Sharing Schemes for Binary, Gray & Color Image. *Biosc.Biotech.Res.Comm. Special Issue Vol 13*, 268-272. Retrieved from https://bbrc.in/wp-content/uploads/2021/01/13_14-SPL-Galley-proof-063.pdf

Pazmiño Zabala, C. A., Serrano Castro, A. K., & González Rivera, M. M. (2020). Las Tics como herramienta para la gestión de riesgos. *RECIMUNDO*, 173-181. Retrieved from http://recimundo.com/index.php/es/article/view/793

Rao , F. A., Dominic P. , D. D., Azhar Ali , S. E., Rehman , M., & Sohail , A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic literature review for identifying the transformation process from noncompliance to compliance. *Advanced Technologies in Data and Information Security*, 8-11. Retrieved from https://www.mdpi.com/2076-3417/11/8/3383

Salazar Raymond, M. B., Icaza Guevara, M. d., & Alejo Machado, O. J. (2018). La importancia de la ética en la investigación. *Universidad y Sociedad*, 305-311. Retrieved from http://scielo.sld.cu/pdf/rus/v10n1/2218-3620-rus-10-01-305.pdf

Salinas, M. S., & Valencia , J. A. (2017). *Sistema de gestión de seguridad de la información y riesgos de información en seis sedes de una entidad bancaria del Perú.* Perú: Repositorio Institucional UPN. Retrieved from https://repositorio.upn.edu.pe/handle/11537/11865

Sánchez Carlessi, H., Reyes Romero, C., & Mejía Sáenz, K. (2018). *Manual de términos en investigación.* Lima. Retrieved from https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion.pdf

Tejena Macía, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del Coonocimiento*. Retrieved from https://polodelconocimiento.com/ojs/index.php/es/article/view/809

Trzeciak, M. (2021). Sustainable Risk Management in IT Enterprises. *Risks, 9(7), 135.* Retrieved from https://doi.org/10.3390/risks9070135

Zevallos Morales, M. N. (2020). *Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte.* Perú: Revista Peruana de computación y sistemas. Retrieved from https://doi.org/10.15381/rpcs.v2i2.17103

ANEXO

Anexo N°01: Matriz de Operacionalización

VARIABLES DE ESTUDIO	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Variable X	**Dimensión conceptual X**	**Definición operacional X**	**Dimensión X**	**Indicadores X**	**Ordinal**
Modelo de gestión de riesgos de TI	Se define como un "conjunto de lineamientos que analizan qué puede suceder y cuáles podrían ser las posibles consecuencias, previo a tomar una decisión de lo que se debe hacer y en qué momento, para minimizar el riesgo a un nivel aceptable. La gestión de riesgos de seguridad de la información puede ser aplicada a una parte de la organización, a un sistema específico o en fase de desarrollo o toda la organización". Según la NTP-ISO/IEC 27005 (2018), (p.4)	El modelo de gestión de riesgos de TI está definido por la puntuación obtenida a través del cuestionario, el que faculta medir su incidencia en la seguridad de información de una institución del estado, en función a los ¿? ítems con respuesta tipo Likert y rangos bajo, moderado y alto, se requiere el uso de la encuesta, cuestionario, y los resultados se aplicarán al SPSS. v 25.	Amenazas	Identificación de amenazas	
				Identificación de vulneravilidades	
				Evaluación del riesgo	
			Impacto potencial	Impacto acumulado	
				Impacto repercutorio	
			Salvaguardas	Selección salvaguardas	
				Efectos de las salvaguardas	
Variable Y	**Dimensión conceptual Y**	**Definición operacional Y**	**Dimensión Y**	**Indicadores Y**	Bajo
Seguridad de la información	Se define como la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Según ISO 27001 (2013), (p.1)	La definición operacional de la variable seguridad de la información se ha realizado en base al cumplimiento de las dimensiones presentadas en el marco teórico y para el lograr los objetivos del estudio se medirá en función a los ¿? ítems con respuesta tipo Likert y rangos bajo, moderado y alto determinándose cómo está siendo incidida por la gestión de riesgos de TI, se requiere el uso de la encuesta, cuestionario, y los resultados se aplicarán al SPSS. v 25.	Confidencialidad	Políticas de seguridad	Medio
				Personal especializado	Alto
				Pruebas en trafico de red	
			Integridad	Incidentes en manipulación de datos	
				Actualización de antivirus	
				Mantenimiento de hardware y software	
			Disponibilidad	Tiempo de respuesta de la información requerida	
				Nivel de complejidad de contraseñas	
				Cantidad de copias de respaldo de información	

Anexo N°02: Instrumento de recolección de datos:

Encuesta 01:
Variable 1: Modelo de gestión de riesgo de TI

adaptado de Calderón, 2019, p.64

Instrucciones:

Gracias por su colaboración. Marque con una "X" su nivel de acuerdo o desacuerdo respecto a los enunciados que se plantean en la siguiente encuesta. La encuesta es anónima.

Niveles de la escala:

1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

N°	Ítems	1	2	3	4	5
	Amenazas					
1	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)					
2	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)					
3	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones					
4	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental					
5	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada					
6	Se ha calculado el riesgo acumulado por cada activo de información					
7	Se ha calculado el riesgo repercutido por cada activo de información					
	Impacto potencial					
8	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.					
9	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende.					
	Salvaguardas					
10	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo					
11	Existe una salvaguarda de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)					
12	Existe una salvaguarda de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)					
13	Existe una salvaguarda de tipo correctiva (gestión de incidentes)					
14	Existe una salvaguarda de tipo recuperación (copias de seguridad backup)					
15	Existe una salvaguarda de tipo monitorización (registros de descargas de la web)					
16	Existe una salvaguarda de tipo detección (antivirus, detectores de incendios, etc.)					
17	Existe una salvaguarda de tipo concientización (cursos de concientización, cursos de formación, etc.)					
18	Existe una salvaguarda de tipo administración (inventario de activos, plan de continuidad)					
19	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales					

Encuesta 02:
Variable 2: Seguridad de la información

adaptado de Calderón, 2019, p.76

Instrucciones:

Gracias por su colaboración. Marque con una "X" su nivel de acuerdo o desacuerdo respecto a los enunciados que se plantean en la siguiente encuesta. La encuesta es anónima.

Niveles de la escala:

1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

N°	Ítems	1	2	3	4	5
	Confidencialidad					
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información					
2	Se cuenta con un adecuado inventario de los accesos a los sistemas					
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)					
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios					
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información					
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos					
7	Cuentan con políticas de intercambio de información ya sea física o electrónica					
8	Intrusos en la red					
9	Realizan controles en la red					
	Integridad					
10	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución					
11	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales					
12	Existe un plan de contingencia contra desastres que pongan en riesgo la información					
13	El equipamiento informático depende del software, hardware, comunicaciones, soporte de información identificados en el inventario de activos de información de TI					
14	Cuentan con políticas de restauración segura de backups de información					
15	Hardware con recursos limitados					
	Disponibilidad					
16	Se cuenta con Directivas o procedimientos para acceder a la información					
17	Existen restricciones para disponer de la información					
18	Existe un inventario de información de la información esencial que maneja					
19	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución					
20	Se utilizan contraseñas para que los usuarios ingresen a los sistemas					
21	Existen normas para la utilización de contraseñas, pero no se implementa					
22	Existen normas para la utilización de contraseñas y es aplicada					
23	Generan copias de seguridad en la nube de la información propia de la empresa					
24	Ausencia de equipos de reemplazo temporal					

Anexo N°03: Certificados de validez de instrumento

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MODELO DE GESTIÓN DE RIESGO DE TI

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Amenazas	Si	No	Si	No	Si	No	
1	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)	X		X		X		
2	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)	X		X		X		
3	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones	X		X		X		
4	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental	X		X		X		
5	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada	X		X		X		
6	Se ha calculado el riesgo acumulado por cada activo de información	X		X		X		
7	Se ha calculado el riesgo repercutido por cada activo de información	X		X		X		
	DIMENSIÓN 2: Impacto potencial	Si	No	Si	No	Si	No	
8	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.	X		X		X		
9	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende.	X		X		X		
	DIMENSIÓN 3: Salvaguardas	Si	No	Si	No	Si	No	
10	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo	X		X		X		
11	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)	X		X		X		
12	Existe una salvaguarda de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)	X		X		X		
13	Existe una salvaguarda de tipo correctiva (gestión de incidentes)	X		X		X		
14	Existe una salvaguarda de tipo recuperación (copias de seguridad backup)	X		X		X		
15	Existe una salvaguarda de tipo monitorización (registros de descargas de la web)	X		X		X		
16	Existe una salvaguarda de tipo detección (antivirus, detectores de incendios, etc.)	X		X		X		
17	Existe una salvaguarda de tipo concientización (cursos de concientización, cursos de formación, etc.)	X		X		X		
18	Existe una salvaguarda de tipo administración (inventario de activos, plan de continuidad)	X		X		X		
19	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales	X		X		X		

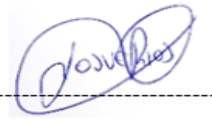
Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombres del juez validador. Dr/ Mg: **Dr. JOSUÉ JOÉL RIOS HERRERA** **DNI: 41997989**

Especialidad del validador: Ingeniero de Sistemas

15 de junio del 2022



Firma del Experto Informante.

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

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

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SEGURIDAD DE LA INFORMACIÓN

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información	X		X		X		
2	Se cuenta con un adecuado inventario de los accesos a los sistemas	X		X		X		
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)	X		X		X		
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios	X		X		X		
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información	X		X		X		
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos	X		X		X		
7	Cuentan con políticas de intercambio de información ya sea física o electrónica	X		X		X		
8	Intrusos en la red	X		X		X		
9	Realizan controles en la red	X		X		X		
	DIMENSIÓN 2: Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución	X		X		X		
11	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales	X		X		X		
12	Existe un plan de contingencia contra desastres que pongan en riesgo la información	X		X		X		
13	El equipamiento informático depende del software, hardware, comunicaciones, soporte de información identificados en el inventario de activos de información de TI	X		X		X		
14	Cuentan con políticas de restauración segura de backups de información	X		X		X		
15	Hardware con recursos limitados	X		X		X		
	DIMENSIÓN 3: Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Se cuenta con Directivas o procedimientos para acceder a la información	X		X		X		
17	Existen restricciones para disponer de la información	X		X		X		
18	Existe un inventario de información de la información esencial que maneja	X		X		X		
19	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución	X		X		X		
20	Se utilizan contraseñas para que los usuarios ingresen a los sistemas	X		X		X		
21	Existen normas para la utilización de contraseñas, pero no se implementa	X		X		X		
22	Existen normas para la utilización de contraseñas y es aplicada	X		X		X		
23	Generan copias de seguridad en la nube de la información propia de la empresa	X		X		X		
24	Ausencia de equipos de reemplazo temporal	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

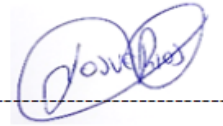
Apellidos y nombres del juez validador. Dr/ Mg: **Dr. JOSUÉ JOÉL RIOS HERRERA** **DNI: 41997989**

Especialidad del validador: Ingeniero de Sistemas

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

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

15 de junio del 2022



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MODELO DE GESTIÓN DE RIESGO DE TI

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Amenazas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)	Si		Si		Si		
2	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)	Si		Si		Si		
3	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones	Si		Si		Si		
4	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental	Si		Si		Si		
5	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada	Si		Si		Si		
6	Se ha calculado el riesgo acumulado por cada activo de información	Si		Si		Si		
7	Se ha calculado el riesgo repercutido por cada activo de información	Si		Si		Si		
	DIMENSIÓN 2: Impacto potencial	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.	Si		Si		Si		
9	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende.	Si		Si		Si		
	DIMENSIÓN 3: Salvaguardas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo	Si		Si		Si		
11	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)	Si		Si		Si		
12	Existe una salvaguarda de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)	Si		Si		Si		
13	Existe una salvaguarda de tipo correctiva (gestión de incidentes)	Si		Si		Si		
14	Existe una salvaguarda de tipo recuperación (copias de seguridad backup)	Si		Si		Si		
15	Existe una salvaguarda de tipo monitorización (registros de descargas de la web)	Si		Si		Si		
16	Existe una salvaguarda de tipo detección (antivirus, detectores de incendios, etc.)	Si		Si		Si		
17	Existe una salvaguarda de tipo concientización (cursos de concientización, cursos de formación, etc.)	Si		Si		Si		
18	Existe una salvaguarda de tipo administración (inventario de activos, plan de continuidad)	Si		Si		Si		
19	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales	Si		Si		Si		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombres del juez validador. POLETTI GAITAN, EDUARDO HUMBERTO **DNI:** 18073124

Especialidad del validador: METODÓLOGO

16 de junio del 2022

Firma del Experto Informante.

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

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

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SEGURIDAD DE LA INFORMACIÓN

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información	Si		Si		Si		
2	Se cuenta con un adecuado inventario de los accesos a los sistemas	Si		Si		Si		
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)	Si		Si		Si		
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios	Si		Si		Si		
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información	Si		Si		Si		
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos	Si		Si		Si		
7	Cuentan con políticas de intercambio de información ya sea física o electrónica	Si		Si		Si		
8	Intrusos en la red	Si		Si		Si		
9	Realizan controles en la red	Si		Si		Si		
	DIMENSIÓN 2: Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución	Si		Si		Si		
11	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales	Si		Si		Si		
12	Existe un plan de contingencia contra desastres que pongan en riesgo la información	Si		Si		Si		
13	El equipamiento informático depende del software, hardware, comunicaciones, soporte de información identificados en el inventario de activos de información de TI	Si		Si		Si		
14	Cuentan con políticas de restauración segura de backups de información	Si		Si		Si		
15	Hardware con recursos limitados	Si		Si		Si		
	DIMENSIÓN 3: Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Se cuenta con Directivas o procedimientos para acceder a la información	Si		Si		Si		
17	Existen restricciones para disponer de la información	Si		Si		Si		
18	Existe un inventario de información de la información esencial que maneja	Si		Si		Si		
19	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución	Si		Si		Si		
20	Se utilizan contraseñas para que los usuarios ingresen a los sistemas	Si		Si		Si		
21	Existen normas para la utilización de contraseñas, pero no se implementa	Si		Si		Si		
22	Existen normas para la utilización de contraseñas y es aplicada	Si		Si		Si		
23	Generan copias de seguridad en la nube de la información propia de la empresa	Si		Si		Si		
24	Ausencia de equipos de reemplazo temporal	Si		Si		Si		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

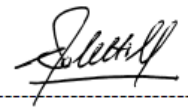
Apellidos y nombres del juez validador. POLETTI GAITAN, EDUARDO HUMBERTO **DNI:** 18073124

Especialidad del validador: METODÓLOGO

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

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

16 de junio del 2022



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MODELO DE GESTIÓN DE RIESGO DE TI

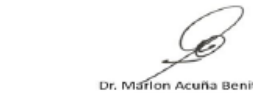
N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Amenazas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)	Si		Si		Si		
2	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)	Si		Si		Si		
3	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones	Si		Si		Si		
4	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental	Si		Si		Si		
5	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada	Si		Si		Si		
6	Se ha calculado el riesgo acumulado por cada activo de información	Si		Si		Si		
7	Se ha calculado el riesgo repercutido por cada activo de información	Si		Si		Si		
	DIMENSIÓN 2: Impacto potencial	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.	Si		Si		Si		
9	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende.	Si		Si		Si		
	DIMENSIÓN 3: Salvaguardas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo	Si		Si		Si		
11	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)	Si		Si		Si		
12	Existe una salvaguarda de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)	Si		Si		Si		
13	Existe una salvaguarda de tipo correctiva (gestión de incidentes)	Si		Si		Si		
14	Existe una salvaguarda de tipo recuperación (copias de seguridad backup)	Si		Si		Si		
15	Existe una salvaguarda de tipo monitorización (registros de descargas de la web)	Si		Si		Si		
16	Existe una salvaguarda de tipo detección (antivirus, detectores de incendios, etc.)	Si		Si		Si		
17	Existe una salvaguarda de tipo concientización (cursos de concientización, cursos de formación, etc.)	Si		Si		Si		
18	Existe una salvaguarda de tipo administración (inventario de activos, plan de continuidad)	Si		Si		Si		
19	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales	Si		Si		Si		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombres del juez validador. Acuña Benites, Marlon Frank DNI: 42097456
Especialidad del validador: Temático

17 de junio del 2022



Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto Informante.

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

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

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SEGURIDAD DE LA INFORMACIÓN

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información	Si		Si		Si		
2	Se cuenta con un adecuado inventario de los accesos a los sistemas	Si		Si		Si		
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)	Si		Si		Si		
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios	Si		Si		Si		
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información	Si		Si		Si		
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos	Si		Si		Si		
7	Cuentan con políticas de intercambio de información ya sea física o electrónica	Si		Si		Si		
8	Intrusos en la red	Si		Si		Si		
9	Realizan controles en la red	Si		Si		Si		
	DIMENSIÓN 2: Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución	Si		Si		Si		
11	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales	Si		Si		Si		
12	Existe un plan de contingencia contra desastres que pongan en riesgo la información	Si		Si		Si		
13	El equipamiento informático depende del software, hardware, comunicaciones, soporte de información identificados en el inventario de activos de información de TI	Si		Si		Si		
14	Cuentan con políticas de restauración segura de backups de información	Si		Si		Si		
15	Hardware con recursos limitados	Si		Si		Si		
	DIMENSIÓN 3: Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Se cuenta con Directivas o procedimientos para acceder a la información	Si		Si		Si		
17	Existen restricciones para disponer de la información	Si		Si		Si		
18	Existe un inventario de información de la información esencial que maneja	Si		Si		Si		
19	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución	Si		Si		Si		
20	Se utilizan contraseñas para que los usuarios ingresen a los sistemas	Si		Si		Si		
21	Existen normas para la utilización de contraseñas, pero no se implementa	Si		Si		Si		
22	Existen normas para la utilización de contraseñas y es aplicada	Si		Si		Si		
23	Generan copias de seguridad en la nube de la información propia de la empresa	Si		Si		Si		
24	Ausencia de equipos de reemplazo temporal	Si		Si		Si		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombres del juez validador. Acuña Benites, Marlon Frank **DNI:** 42097456

Especialidad del validador: Temático

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

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

17 de junio del 2022

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto Informante.

Anexo N°04: Carta de Presentación

UNIVERSIDAD CÉSAR VALLEJO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

Lima, 17 de junio de 2022
Carta P. 0377-2022-UCV-VA-EPG-F01/J

Lic.
Leslie Gisell Mendoza Cabrera
Especialista
DGPA-MEF

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a PIZARRO CASTRO, IVAN MARCO ANTONIO; identificado con DNI N° 44340300 y con código de matrícula N° 7002438030; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Modelo de Gestión de riesgos de TI para la seguridad de la información de una institución del estado, Lima 2022

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador PIZARRO CASTRO, IVAN MARCO ANTONIO asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dra. Estrella A. Esquiagola Aranda
Jefa
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

Yo, Leslie Gisell Mendoza Cabrera, Especialista de la DGPA del MEF, visto la solicitud para realizar su trabajo de investigación titulado "Modelo de Gestión de riesgos de TI para la seguridad de la información de una institución del Estado, Lima 2022" en nuestra institución, se autoriza recolectar la información necesaria para la investigación científica a través de la encuesta.

Lima, 18 de junio de 2022

Leslie Gisell Mendoza Cabrera

Anexo 5: Base de datos

Variable 1: Modelo de gestión de riesgo de TI

Variable	Modelo de gestión de riesgos de TI																		
ITEM	D1: Amenazas							D2: Impacto Potencial		D3: Salvaguardas									
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19
1	4	5	5	5	5	4	4	5	4	4	5	5	4	5	5	5	3	5	3
2	5	4	5	5	4	5	4	5	3	5	4	5	4	5	4	5	3	5	4
3	4	5	3	4	4	3	3	3	2	1	1	3	3	3	1	4	1	4	4
4	4	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	1	3	3
5	5	5	4	5	5	5	1	4	4	5	5	4	1	4	5	5	3	4	4
6	3	5	5	4	5	3	4	5	3	3	5	5	4	5	5	4	3	3	4
7	3	2	3	3	5	4	2	3	3	1	1	3	1	3	1	3	3	1	1
8	2	3	2	2	3	2	3	2	3	2	3	2	3	2	3	2	4	2	2
9	2	4	3	3	4	2	4	3	2	2	4	3	4	3	4	3	3	2	2
10	2	5	3	3	5	2	5	3	2	2	5	3	5	3	5	3	4	2	2
11	5	4	4	4	4	5	4	4	5	5	4	4	4	4	4	4	4	5	3
12	2	4	3	3	4	2	4	3	2	2	4	3	4	3	4	3	4	2	2
13	2	5	2	2	5	2	5	2	2	2	5	2	5	2	5	2	3	2	2
14	5	4	4	4	4	5	4	4	5	5	4	4	4	4	4	4	4	5	3
15	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	2
16	3	4	5	5	4	3	4	5	3	3	4	5	4	5	4	5	4	3	3
17	3	3	2	2	3	3	3	2	3	3	3	2	3	2	3	2	4	3	3
18	2	5	1	1	5	2	5	1	2	2	5	1	5	1	5	1	3	2	2
19	5	5	3	3	5	5	5	3	5	5	5	3	5	3	5	3	3	5	3
20	2	5	1	1	5	2	5	3	2	2	5	1	5	1	5	1	4	2	2
21	4	5	3	3	5	4	5	3	4	4	5	3	5	3	5	3	3	4	4
22	2	5	3	3	5	2	5	3	2	2	5	3	5	3	5	3	3	2	2
23	2	4	1	1	4	2	4	1	2	2	4	1	4	1	4	1	4	2	2
24	3	5	3	3	5	3	5	3	3	3	5	3	5	3	5	3	4	3	3
25	2	5	1	1	5	2	5	1	2	2	5	1	5	1	5	1	4	2	2
26	3	4	4	4	4	3	4	4	3	3	4	4	4	4	4	4	4	3	3
27	2	5	3	3	5	2	5	3	2	2	5	3	5	3	5	3	3	2	2
28	1	5	1	1	5	1	5	1	2	1	5	1	5	1	5	1	3	1	1
29	4	4	2	2	4	4	4	2	4	4	4	2	4	2	4	2	3	4	4
30	3	4	2	2	4	3	4	2	3	3	4	2	4	2	4	2	4	3	3
31	1	3	1	1	3	1	3	2	1	1	3	1	3	1	3	1	3	1	1
32	2	5	1	1	5	2	5	1	2	2	5	1	5	1	5	1	3	2	2
33	5	4	1	1	4	5	4	1	5	5	4	1	4	1	4	1	4	5	3
34	3	4	3	3	4	3	4	3	3	3	4	3	4	3	4	3	3	3	3
35	1	5	1	1	5	1	5	3	1	1	5	1	5	1	5	1	3	1	1
36	2	5	2	2	5	2	5	2	2	2	5	2	5	2	5	2	3	2	2
37	2	5	3	3	5	2	5	3	2	2	5	3	5	3	5	3	4	2	2
38	4	5	5	5	5	4	5	5	4	4	5	5	5	5	5	5	3	4	2
39	1	5	2	2	5	1	5	2	1	1	5	2	5	2	5	2	4	1	1
40	1	4	3	3	4	1	4	3	1	1	4	3	4	3	4	3	3	1	1
41	3	5	2	2	5	3	5	2	3	3	5	2	5	2	5	2	3	3	3
42	4	3	4	4	3	4	3	4	4	4	3	4	3	4	3	4	3	4	3
43	2	3	2	2	3	2	3	2	2	2	3	2	3	2	3	2	3	2	2
44	4	1	2	2	1	4	1	2	4	4	1	2	1	2	1	2	3	4	3
45	3	4	3	3	4	3	4	3	3	3	4	3	4	3	4	3	4	3	3
46	3	4	3	3	4	3	4	3	3	3	4	3	4	3	4	3	3	3	3
47	1	3	2	2	3	1	3	2	1	1	3	2	3	2	3	2	4	1	1
48	2	2	1	1	2	2	2	1	2	2	2	1	2	1	2	1	4	2	2
49	1	3	5	5	3	1	3	5	1	1	3	5	3	5	3	5	3	1	1
50	2	4	3	3	4	2	4	3	2	2	4	3	4	3	4	3	4	2	2
51	4	5	5	3	5	4	4	5	4	4	5	5	4	5	5	5	4	5	5
52	4	3	3	1	3	4	4	3	1	4	4	5	4	5	4	5	4	3	3
53	5	5	5	1	5	5	3	5	2	5	1	3	3	3	1	5	5	5	5
54	2	1	2	2	1	2	4	2	4	2	4	4	4	4	4	5	2	1	2
55	3	5	5	3	5	3	1	5	2	3	5	4	1	4	5	5	3	5	5
56	5	5	5	3	5	5	4	5	5	5	5	5	4	5	5	5	5	5	5
57	1	2	3	1	2	1	1	3	4	1	1	3	1	3	1	5	1	2	3
58	3	3	2	2	3	3	3	2	5	3	3	2	3	2	3	5	3	3	2
59	4	3	3	2	3	4	4	3	5	4	4	3	4	3	4	5	4	3	3
60	5	4	3	2	4	5	5	3	4	5	5	3	5	3	5	5	5	4	3
61	4	5	5	5	5	4	4	5	4	4	5	5	4	5	5	5	3	5	3
62	5	4	5	5	4	5	4	5	3	5	4	5	4	5	4	5	3	5	4
63	1	1	3	4	1	1	3	3	1	1	1	3	3	3	1	4	1	4	4
64	4	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	1	3	3
65	5	5	4	5	5	5	1	4	4	5	5	4	1	4	5	5	3	4	4
66	3	5	5	4	5	3	4	5	3	3	5	5	4	5	5	4	3	3	4
67	1	1	3	3	1	1	1	3	1	1	1	3	1	3	1	3	3	1	1
68	2	3	2	2	3	2	3	2	2	2	3	2	3	2	3	2	4	2	2
69	2	4	3	3	4	2	4	3	2	2	4	3	4	3	4	3	3	2	2
70	2	5	3	3	5	2	5	3	2	2	5	3	5	3	5	3	4	2	2
71	5	4	4	4	4	5	4	4	5	5	4	4	4	4	4	4	4	5	3
72	2	4	3	3	4	2	4	3	2	2	4	3	4	3	4	3	4	2	2
73	2	5	2	2	5	2	5	2	2	2	5	2	5	2	5	2	3	2	2
74	5	4	4	4	4	5	4	4	5	5	4	4	4	4	4	4	4	5	3
75	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	2
76	3	4	5	5	4	3	4	5	3	3	4	5	4	5	4	5	4	3	3
77	3	3	2	2	3	3	3	2	3	3	3	2	3	2	3	2	4	3	3
78	2	5	1	1	5	2	5	1	2	2	5	1	5	1	5	1	3	2	2
79	5	5	3	3	5	5	5	3	5	5	5	3	5	3	5	3	3	5	3
80	2	5	1	1	5	2	5	1	2	2	5	1	5	1	5	1	4	2	2

Variable 2: Seguridad de la información

Variable	Seguridad de la información																							
ITEM	D4: Confidencialidad									D5: Integridad						D6: Disponibilidad								
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24
1	3	5	4	4	3	5	4	4	4	3	5	4	5	4	5	5	3	5	4	4	5	5	4	5
2	3	5	4	5	3	5	4	4	4	3	5	4	4	3	5	4	3	5	4	4	5	5	4	5
3	1	3	3	1	1	3	3	3	3	1	3	3	1	1	3	1	1	3	3	3	3	3	3	3
4	1	4	4	4	1	4	4	4	4	1	4	4	4	3	4	4	1	4	4	4	4	4	4	4
5	3	4	1	5	3	4	1	1	1	3	4	1	5	4	4	5	3	4	1	1	4	4	1	4
6	3	5	4	3	3	5	4	4	4	3	5	4	5	3	5	5	3	5	4	4	5	5	4	5
7	3	3	1	1	3	3	1	1	1	3	3	1	1	1	3	1	3	3	1	1	3	3	1	3
8	4	2	3	2	4	2	3	3	3	4	2	3	3	2	2	3	4	2	3	3	2	2	3	2
9	3	3	4	2	3	3	4	4	4	3	3	4	4	2	3	4	3	3	4	4	3	3	4	3
10	4	3	5	2	4	3	5	5	5	4	3	5	5	2	3	5	4	3	5	5	3	3	5	3
11	4	4	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4
12	4	3	4	2	4	3	4	4	4	4	3	4	4	2	3	4	4	3	4	4	3	3	4	3
13	3	2	5	2	3	2	5	5	5	3	2	5	5	2	2	5	3	2	5	5	2	2	5	2
14	4	4	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4
15	3	4	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4
16	4	5	4	3	4	5	4	4	4	4	5	4	4	3	5	4	4	5	4	4	5	5	4	5
17	4	2	3	3	4	2	3	3	3	4	2	3	3	3	2	3	4	2	3	3	2	2	3	2
18	3	1	5	2	3	1	5	5	5	3	1	5	5	2	1	5	3	1	5	5	1	1	5	1
19	3	3	5	5	3	3	5	5	5	3	3	5	5	5	3	5	3	3	5	5	3	3	5	3
20	4	1	5	2	4	1	5	5	5	4	1	5	5	2	1	5	4	1	5	5	1	1	5	1
21	3	3	5	4	3	3	5	5	5	3	3	5	5	4	3	5	3	3	5	5	3	3	5	3
22	3	3	5	2	3	3	5	5	5	3	3	5	5	2	3	5	3	3	5	5	3	3	5	3
23	4	1	4	2	4	1	4	4	4	4	1	4	4	2	1	4	4	1	4	4	1	1	4	1
24	4	3	5	3	4	3	5	5	5	4	3	5	5	3	3	5	4	3	5	5	3	3	5	3
25	4	1	5	2	4	1	5	5	5	4	1	5	5	2	1	5	4	1	5	5	1	1	5	1
26	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4
27	3	3	5	2	3	3	5	5	5	3	3	5	5	2	3	5	3	3	5	5	3	3	5	3
28	3	1	5	1	3	1	5	5	5	3	1	5	5	1	1	5	3	1	5	5	1	1	5	1
29	3	2	4	4	3	2	4	4	4	3	2	4	4	4	2	4	3	2	4	4	2	2	4	2
30	4	2	4	3	4	2	4	4	4	4	2	4	4	3	2	4	4	2	4	4	2	2	4	2
31	3	1	3	1	3	1	3	3	3	3	1	3	3	1	1	3	3	1	3	3	1	1	3	1
32	3	1	5	2	3	1	5	5	5	3	1	5	5	2	1	5	3	1	5	5	1	1	5	1
33	4	1	4	5	4	1	4	4	4	4	1	4	4	5	1	4	4	1	4	4	1	1	4	1
34	3	3	4	3	3	3	4	4	4	3	3	4	4	3	3	4	3	3	4	4	3	3	4	3
35	3	1	5	1	3	1	5	5	5	3	1	5	5	1	1	5	3	1	5	5	1	1	5	1
36	3	2	5	2	3	2	5	5	5	3	2	5	5	2	2	5	3	2	5	5	2	2	5	2
37	4	3	5	2	4	3	5	5	5	4	3	5	5	2	3	5	4	3	5	5	3	3	5	3
38	3	5	5	4	3	5	5	5	5	3	5	5	5	4	5	5	3	5	5	5	5	5	5	5
39	4	2	5	1	4	2	5	5	5	4	2	5	5	1	2	5	4	2	5	5	2	2	5	2
40	3	3	4	1	3	3	4	4	4	3	3	4	4	1	3	4	3	3	4	4	3	3	4	3
41	3	2	5	3	3	2	5	5	5	3	2	5	5	3	2	5	3	2	5	5	2	2	5	2
42	3	4	3	4	3	4	3	3	3	3	4	3	3	4	4	3	3	4	3	3	4	4	3	4
43	3	2	3	2	3	2	3	3	3	3	2	3	3	2	2	3	3	2	3	3	2	2	3	2
44	3	2	1	4	3	2	1	1	1	3	2	1	1	4	2	1	3	2	1	1	2	2	1	2
45	4	3	4	3	4	3	4	4	4	4	3	4	4	3	3	4	4	3	4	4	3	3	4	3
46	3	3	4	3	3	3	4	4	4	3	3	4	4	3	3	4	3	3	4	4	3	3	4	3
47	4	2	3	1	4	2	3	3	3	4	2	3	3	1	2	3	4	2	3	3	2	2	3	2
48	4	1	2	2	4	1	2	2	2	4	1	2	2	2	1	2	4	1	2	2	1	1	2	1
49	3	5	3	1	3	5	3	3	3	3	5	3	3	1	5	3	3	5	3	3	5	5	3	5
50	4	3	4	2	4	3	4	4	4	4	3	4	4	2	3	4	4	3	4	4	3	3	4	3
51	3	5	4	4	3	5	4	4	4	3	5	4	5	4	5	5	3	5	4	4	5	5	4	5
52	3	5	4	5	3	5	4	4	4	3	5	4	4	3	5	4	3	5	4	4	5	5	4	5
53	1	3	3	1	1	3	3	3	3	1	3	3	1	1	3	1	1	3	3	3	3	3	3	3
54	1	4	4	4	1	4	4	4	4	1	4	4	4	3	4	4	1	4	4	4	4	4	4	4
55	3	4	1	5	3	4	1	1	1	3	4	1	5	4	4	5	3	4	1	1	4	4	1	4
56	3	5	4	3	3	5	4	4	4	3	5	4	5	3	5	5	3	5	4	4	5	5	4	5
57	3	3	1	1	3	3	1	1	1	3	3	1	1	1	3	1	3	3	1	1	3	3	1	3
58	4	2	3	2	4	2	3	3	3	4	2	3	3	2	2	3	4	2	3	3	2	2	3	2
59	3	3	4	2	3	3	4	4	4	3	3	4	4	2	3	4	3	3	4	4	3	3	4	3
60	4	3	5	2	4	3	5	5	5	4	3	5	5	2	3	5	4	3	5	5	3	3	5	3
61	4	4	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	5
62	4	3	4	2	4	3	4	4	4	4	3	4	4	2	3	4	4	3	4	4	3	5	4	5
63	3	2	5	2	3	2	5	5	5	3	2	5	5	2	2	5	3	2	5	5	2	3	3	3
64	4	4	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4
65	3	4	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	4	4	4	4	4	1	4
66	4	5	4	3	4	5	4	4	4	4	5	4	4	3	5	4	4	5	4	4	5	5	4	5
67	4	2	3	3	4	2	3	3	3	4	2	3	3	3	2	3	4	2	3	3	2	3	1	3
68	3	1	5	2	3	1	5	5	5	3	1	5	5	2	1	5	3	1	5	5	1	2	3	2
69	3	3	5	5	3	3	5	5	5	3	3	5	5	5	3	5	3	3	5	5	3	3	4	3
70	4	1	5	2	4	1	5	5	5	4	1	5	5	2	1	5	4	1	5	5	1	3	5	3
71	3	3	5	4	3	3	5	5	5	3	3	5	5	4	3	5	3	3	5	5	3	4	4	4
72	3	3	5	2	3	3	5	5	5	3	3	5	5	2	3	5	3	3	5	5	3	3	4	3
73	4	1	4	2	4	1	4	4	4	4	1	4	4	2	1	4	4	1	4	4	1	2	5	2
74	4	3	5	3	4	3	5	5	5	4	3	5	5	3	3	5	4	3	5	5	3	4	4	4
75	4	1	5	2	4	1	5	5	5	4	1	5	5	2	1	5	4	1	5	5	1	4	4	4
76	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	5	4	5
77	3	3	5	2	3	3	5	5	5	3	3	5	5	2	3	5	3	3	5	5	3	2	3	2
78	3	1	5	1	3	1	5	5	5	3	1	5	5	1	1	5	3	1	5	5	1	1	5	1
79	3	2	4	4	3	2	4	4	4	3	2	4	4	4	2	4	3	2	4	4	2	3	5	3
80	4	2	4	3	4	2	4	4	4	4	2	4	4	3	2	4	4	2	4	4	2	1	5	1

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, 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: "Modelo de Gestión de riesgos de TI para la seguridad de la información de una institución del estado, Lima 2022", cuyo autor es PIZARRO CASTRO IVAN MARCO ANTONIO, 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, 08 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID** 0001-5207-9353	Firmado digitalmente por: MACUNABE el 08-08-2022 10:53:03

Código documento Trilce: TRI - 0402335

INVESTIGA UCV