UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE DOCTORADO EN GESTIÓN PÚBLICA Y GOBERNABILIDAD

Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Doctor en Gestión Pública y Gobernabilidad

AUTOR :

Ñañez Campos, Oscar (ORCID: 0000-0002-7840-3999)

ASESOR :

Dr. Montenegro Camacho, Luis Arturo (ORCID: 000-0002-5224-4854)

LÍNEA DE INVESTIGACIÓN:

Reforma y modernización del estado

CHICLAYO - PERÚ

2021

Dedicatoria

La presente investigación está dedicada en primer lugar a Dios, por darme la oportunidad de vivir, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante el periodo de estudios.

A mi madre Margarita Campos Morales y a mi padre Manuel Exaltación Ñañez Chancafe, que desde el cielo donde él se encuentra, me ha iluminado para poder culminar satisfactoriamente este trabajo de investigación.

Agradecimiento

A Dios por bendecirme para llegar hasta donde he llegado, por hacer realidad una de mis metas anheladas.

Mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización de la presente tesis, en especial al Dr. Luis Arturo Montenegro Camacho, y al Mg. Fredy George Olivos Romeros por su permanente colaboración y apoyo incondicional en el desarrollo y culminación de mi Proyecto e informe de tesis.

En general a la dirección de Tecnologías de Información y Comunicaciones de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas por facilitarme el acceso a la información requerida para alcanzar los objetivos trazados en la presente tesis.

Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibido de mi familia y amigos

A todos ellos muchas gracias.

Índice de contenidos

Índices de tablas

Índices de gráficos y figuras

Índice de Abreviaturas:

UNTRM	:	Universidad Nacional Toribio Rodríguez de Mendoza
DGCA	:	Dirección de Gestión de la Calidad Académica
MGRSI	:	Modelo de Gestión de Riesgos de Sistema de información
SGSI	:	Sistema de Gestión de Seguridad de la Información
SGRSI	:	Sistema de Gestión de Riesgos de Seguridad de la información
PRSI	:	Plan de Riesgos de seguridad de la Información

Resumen

En la gestión de riesgos de seguridad de la información, los activos a proteger son la información digital y física (papel). En ese contexto el objetivo fue proponer un modelo de gestión de riesgos para la seguridad de la información en la UNTRM, cuya problemática se centró en la escasa cultura de Risk manasgement y el desconocimiento de los derechos y responsabilidades con el mal uso de tecnologías, esto contribuyen a la generación de vulnerabilidades que podrían ser explotadas y esto impactaría significativamente la continuidad del negocio. La metodología que se estableció fue el enfoque cuantitativo de tipo básico y diseño universal; la muestra no probabilística estuvo representada por 40 trabajadores docentes y administrativos, se utilizó la técnica de la encuesta validada por expertos. Entre las conclusiones se confirmó que la seguridad de la información en base a la percepción de los sujetos de estudio se encuentra un nivel regular 69%, 65.5% y 58.6%, valoraciones que expresaron la necesidad de potenciar los procesos de confidencialidad, integridad y disponibilidad. Frente a esta realidad se diseñó un modelo de gestión de riesgos que ayude a DTIC a gestionar adecuadamente la seguridad de la información en los procesos críticos de la UNTRM.

Palabras claves: Gestión de Riesgos, seguridad de la información, universidad, docentes, administrativos.

Abstract

In information security risk management, the assets to be protected are digital and physical (paper) information. In this context, the objective was to propose a risk management model for information security in the UNTRM, whose problems focused on the scarce culture of Risk management and the ignorance of the rights and responsibilities with the misuse of technologies, this They contribute to the generation of vulnerabilities that could be exploited and this would significantly impact business continuity. The methodology that was established was the quantitative approach of a basic type and universal design; the non-probabilistic sample was represented by 40 teaching and administrative workers, the survey technique validated by experts was used. Among the conclusions, it was confirmed that the information security based on the perception of the study subjects is a regular level 69%, 65.5% and 58.6%, evaluations that expressed the need to enhance the processes of confidentiality, integrity and availability. Faced with this reality, a risk management model was designed to help DTIC to adequately manage information security in the critical processes of the UNTRM.

Keywords: Risk Management, information security, university, teachers, administrative.

I. INTRODUCCIÓN

Referente a la realidad problemática podemos manifestar que mundialmente la seguridad de la información en las organizaciones, en especial la protección de la información es prioritaria, y se elaboran diferentes normas internacionales que permitan controlar y mitigar los riesgos referidos a la seguridad de la información de manera integrada. Con respecto a la problemática internacional, según Solano Cárdenas et al., (2016), mencionan que el estándar ISO 27000 es un estándar de seguridad de la información y debe ser utilizado por la empresa cuando necesite mejorar su imagen y promover sus capacidades de Certificación ISO. 27000 y NIST SP 800-53 requeridos por agencias federales en los Estados Unidos; los estándares anteriores respaldan el papel del profesional de seguridad en la organización y gestión de un programa de seguridad de la información. Asimismo, Anchundia-Betancourt, C.E. (2017) menciona que la internacionalización y el avance tecnológico traen ventajas a diferentes tipos de organizaciones y empresas, pero que estas generan grandes problemas de seguridad, protección, problemas de datos y privacidad que enfrentarán las empresas. La ciberseguridad es un fenómeno generalizado a cualquier tipo de negocio; las amenazas pueden trasladarse al contexto universitario, siendo la universidad la protagonista en la promoción de una cultura de ciberseguridad; Las instituciones académicas deben promover un ciberespacio académico seguro y liderar una cultura de ciberseguridad basada en una cultura de seguridad y defensa dentro de la universidad. Del mismo modo Tellez Carvajal, E (2018) afirma que los individuos estamos expuestos a ataques digitales, en ocasiones somos nosotros quienes ponemos en riesgo los sistemas informáticos por desconocimiento o falta de conocimientos, por lo que es importante difundir y ser conscientes de las responsabilidades y derechos que tenemos cuando usamos tecnología, las tecnologías conllevan riesgos; conocer los riesgos que implican el uso de las tecnologías es una herramienta que empodera a las personas, a ser más conscientes de los riesgos a los que nos enfrentamos con el uso de las nuevas tecnologías y poder anticiparnos a las amenazas y riesgos que tenemos hoy.

Y, por último, Altamirano Yupanqui & Bayona Oré (2017), en su artículo Políticas de Seguridad de la información afirma:

Los expertos de seguridad TI deben pensar que la seguridad de la información no solo está garantizada por el uso de sofisticados perímetros de seguridad, sino que también deben enfocarse y tomar en cuenta el factor humano en sus estrategias de protección, pues los comportamientos indeseables que presenta provocarán la cancelación de la seguridad, perímetros en su lugar, generando importantes brechas de seguridad y pérdidas económicas

Por otro lado, el problema nacional específicamente en el Perú, al igual que muchos otros países ha desarrollado una ley para la protección de la información "Ley N ° 29733 de protección de datos personales", buenas prácticas de seguridad de la información y gestión de riesgos de seguridad de la información, como NTP ISO / IEC 27001: 2014 Tecnologías de la información. Técnicas de seguridad, sistemas de gestión de seguridad de la información, que cuenta con resolución para su implementación en instituciones públicas como las que se indican a continuación: RM 042-2008 / INDECOPI Norma técnica peruana ISO / IEC 27001 fue aprobada: 2008, RM 129-2012-PCM pasa a ser obligatoria y la Resolución 029-2009 la NTP ISO / IEC 27005: 2009 “Tecnología de la Información. Técnicas de seguridad. Gestión de Riesgos de Seguridad de la Información, que se encarga de gestionar los propios riesgos de seguridad de la información, Decreto supremo N° 050-2018 -PCM en donde se define la seguridad Digital en el ámbito nacional, el Decreto Legislativo N° 1412-2018 que aprueba la Ley de Gobierno Digital entre otros.

El problema de investigación se centra en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (en adelante UNTRM), donde se percibe una falta de cultura de Risk management para los activos de información, la ausencia de políticas de seguridad, el factor humano de la organización desconocen los derechos y responsabilidades relacionados con el mal uso de la tecnología; Todos estos problemas contribuyen a la generación de vulnerabilidades que podrían ser explotadas por diferentes amenazas y por lo tanto impactarían significativamente la continuidad de los procesos comerciales y afectarían los principios de seguridad de la información.

Es importante que la UNTRM sensibilice a su personal sobre la importancia de la Risk management para los activos de información, ya que permitirá la evaluación e identificación pertinente de las vulnerabilidades que podrían ser explotadas por diferentes amenazas, principalmente afectando la Continuidad empresarial y principios de seguridad de la información en la Universidad.

A esta realidad se formula la siguiente interrogante. ¿De qué manera un Modelo de gestión de riesgos mejorará la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas?, y cuyos problemas específicos se expresan en las siguientes preguntas: ¿Empleados de la UNTRM conoce la importancia de recursos de información?, ¿Los responsables de TI comunican oportunamente las políticas de seguridad al personal de la UNTRM? ¿Sabe cómo identificar los activos de información que necita proteger en función a su importancia y criticidad?, ¿Sabe cómo identificar las amenazas potenciales que pueden surgir para atacar un activo de información?, ¿Los departamentos de la universidad conocen las políticas de seguridad?, ¿la universidad invierte recursos económicos en la seguridad de la información de la UNTRM?

El proyecto tuvo como justificación teórica contribuir al conocimiento científico con un instrumento para mejorar la seguridad de la información en la UNTRM y con ello la efectividad y calidad de los servicios críticos en la universidad. El análisis e interpretación de los resultados, así como la construcción de la propuesta contribuirán en la generación de cambios en la cultura de la seguridad de la UNTRM. También servirá de ayuda y orientación para realizar, posteriores investigaciones.

Por otro lado, la justificación metodológica estuvo orientada a la implementación de un Risk Management Model para mejorar la security of the information, el mismo que pueden aplicar las universidades para mejorar la seguridad de la información en la universidad y contribuir con la calidad y efectividad de los servicios críticos de la universidad: el servicio de admisión, matrícula, registros, grados y títulos, tesorería y contabilidad. Además, este modelo, permitirá a través de las normas y procedimientos, gestionar incidentes de seguridad reduciendo

los impactos negativos en procesos que puedan ocasionar caídas de los activos tecnológicos, y por consecuencia pérdida de imagen institucional.

Finalmente, en su justificación práctica, la investigación se justificó porque se deseaba garantizar la security of the information en la UNTRM, también porque brindaría información útil a las autoridades y a los directores de la universidad para analizar resultados en la mejora de la seguridad de la información y por ende de la calidad y efectividad de los servicios que brinda.

La investigación tuvo como objetivo general proponer un modelo de gestión de riesgos para mejorar la seguridad de la información en la UNTRM, y los objetivos específicos que determinarán este objetivo son: Realizar un diagnóstico de los procesos de la UNTRM que utilizan tecnologías y sistemas de información, para identificar procesos críticos; evaluar la security of the information en la UNTRM; diseñar el modelo de gestión de riesgos para mejorar la seguridad de la información en la UNTRM; y validar el modelo de gestión de riesgos para mejorar la seguridad de la información de la UNTRM. La hipótesis a defender presentó el siguiente enunciado (Hi): Si se diseña un Modelo de Gestión de Riesgos entonces logrará mejorar la seguridad de la información en la UNTRM – Chachapoyas.

II. MARCO TEÓRICO

El marco referencial recoge experiencias previas sobre el problema de investigación, las mismas que van a contribuir a reconocer aspectos que necesitan de mayor profundización investigativa, e identificar tendencias teóricas y metodológicas que orienten el logro de los propósitos de la investigación.

Entre los antecedentes que se relacionan a mi investigación de manera internacional esta; Anchundia-Betancourt, C.E (2017) tuvo como objetivo en su artículo examinar el estado actual del conocimiento en ciberseguridad en contextos universitarios con ciertas implicaciones en Ecuador; se realizó una revisión documental con buscadores en bases de datos de documentos científicos como Sciencedirect y Google Academic, entre otros. A pesar de que existe poca literatura científica sobre el tema de la ciberseguridad en el ámbito universitario, esto impide un análisis en profundidad de la situación en el contexto universitario; sin embargo, dado que la ciberseguridad es un contexto global y está generalizada a todo tipo de organizaciones, pueden extrapolar las amenazas a la educación superior. Además, menciona que la universidad debe ser líder en cultura de ciberseguridad, basada en cultura de seguridad y defensa dentro de la Universidad.

Altamirano-Yupanqui & Bayona-Oré, (2017) en su artículo efectuaron una revisión sistemática de la literatura científica, para encontrar teorías de investigación relacionadas con el cumplimiento de las políticas de seguridad, cuyos resultados fueron comprender el comportamiento humano a través de la teoría psicológica.

Gutiérrez & Sánchez-Ortiz, (2018) en su trabajo científico propusieron un Risk Management Model basado en el estándar ISO 31000: 2012 para docencia de pregrado de la Universidad Católica del Norte de Chile. El modelo propuesto permitió favorecer los procesos de acreditación para mejorar la eficiencia de los procesos docentes, creando matrices de riesgo y determinando indicadores clave de riesgo (KRI). Los resultados obtenidos de la aplicación del modelo

fueron definir los riesgos inherentes y remanentes en los procesos docentes, así como el control de los procesos críticos.

Correa Henao et al., (2017) en su investigación se plantearon el objetivo de gestionar los riesgos en el entorno empresarial colombiano, a través de buenas prácticas en cultura organizacional, analizando las metodologías aceptadas para llevar a cabo el proceso de 'análisis e identificación de riesgos en el campo corporativo y organizacional. A medida que la cultura de la gestión de riesgos evolucione en las organizaciones y la dirección de las organizaciones invierta en la gestión de riesgos, les ayudará a mejorar la organización y por tanto fortalecer gradualmente la competitividad de la empresa. Las organizaciones colombianas han aplicado la gestión de riesgos como política en sus modelos de negocio posibilitando la creación de una cultura de responsabilidad corporativa, mejora continua y competitividad, esto ha permitido a las empresas diseñar estrategias de mejora generando sistemas de control interno que permitan el cumplimiento. con sus objetivos misioneros, todo ello en base a la normativa vigente y los estándares internacionales que las organizaciones deben respetar para su certificación en gestión de riesgos.

Por su parte, Miranda Cairo et al., (2016) se propusieron en su producción científica el objetivo de implementar la gestión automatizada de controles de seguridad de TI, utilizando una metodología que permitió la integración de diferentes modelos, estándares, herramientas y buenas prácticas, fusionando diversos métodos orientados a la gestión de riesgos con miras a la automatización durante las etapas de operación, seguimiento y revisión de un sistema de gestión de seguridad informática. El resultado de su investigación fue hacer de la gestión de la seguridad de TI un proceso simple y eficiente; Estos resultados fueron validados por un análisis estadístico que muestra la reducción de la complejidad y el aumento de la eficiencia en términos de tiempo y esfuerzo que requiere el proceso, con un factor cercano al 90% en ambos casos.

Education Cybersecurity Report (2018), menciona que un tercio de los ataques cibernéticos son realizadas a las instituciones de educación superior, tal como lo que ha ocurrido a inicios del 2019 con más de 20 universidades norteamericanas.

Por otro lado, Don Welch, (2019), Chief Información Security Officer de la Universidad de Pennsylvania, menciona que los líderes de seguridad cibernética en educación superior, dedican poco tiempo a desarrollar una estrategia de seguridad, siendo las universidades pequeñas ciudades que manejan diversos tipos de datos críticos y confidenciales. Así mismo menciona que la ciberseguridad no es solo una función de los responsables de TI, que es más bien una función institucional, por lo tanto, todos los miembros de la comunidad universitaria tienen un papel muy importante que desempeñar y deben actuar en concordancia con la estrategia de ciberseguridad.

De acuerdo con el Center for Digital Education los principales retos que afrontas las universidades respecto a la ciberseguridad son: Phishing. La educación del usuario es importante ya que tanto los docentes, estudiantes y personal administrativo de las universidades están ocupados con las actividades académicas y por ende cuentan con un mínimo tiempo para preocuparse por la ciberseguridad, la seguridad en la nube, compromiso de las autoridades con la estrategia de la seguridad, la inversión en tecnologías de seguridad de última generación, la gestión de la identidad y acceso a aplicaciones que las universidad maneja, la gobernanza de la seguridad de datos; así mismo varias universidades no disponen de una gestión de datos centralizada y por ende es difícil gobernar la seguridad de los datos.

En Perú existe preocupación en materia de ciberseguridad, por lo que en 2019 se presentan al Congreso de la República dos proyectos de ley, uno tiene que ver con la seguridad informática en Perú y la conformación de un Consejo Nacional de ciberseguridad, cuyo objetivo del proyecto de ley es promover la seguridad informática en todo el territorio nacional de acuerdo con los principios de: colaboración multidisciplinar, multisectorial e interinstitucional, respeto a los derechos humanos y desde un enfoque basado sobre gestión de riesgos. (García, 2019).

Así mismo, el reporte de Ciberseguridad 2020, publicado por el Banco Interamericano de Desarrollo (BID), muestra que Perú tiene una inadecuada gestión de riesgos y respuestas ante la protección de la infraestructura crítica,

falta de contenidos claves en la política y estrategias de ciberseguridad, bajos estándares en adquisiciones de tecnologías y un reducido mercado nacional de tecnologías de ciberseguridad.(ComexPerú, 2020).

Celi-Arévalo & Diaz-Plaza, (2017) , en su tesis doctoral, establece evaluar los elementos que influyen en el comportamiento de los usuarios de TI, y desarrollar un modelo conceptual que identifique estos factores, intencionales o no, por el incumplimiento de políticas y estándares de seguridad de la información en sector microfinanciero, el aporte de esta investigación consiste en evaluar factores concernientes con su comportamiento, la influencia del entorno y percepción del control establecido. Para la recolección de datos utilizó el cuestionario, instrumento creado por los investigadores y validado por un piloto utilizando las estadísticas alfa de Conbrach. La muestra estuvo compuesta por 133 usuarios de TI de 8 empresas de microfinanzas, 110 de los cuales eran válidos para el procesamiento de datos. Se aplicó un análisis de correlación y se encontró que los elementos asociados con la conducta pretendida tuvieron un coeficiente de correlación de 0,695 con respecto al cumplimiento de los lineamientos de seguridad de la información, mientras que los elementos asociados con la conducta no intencionada tuvieron un coeficiente de correlación de 0,564. Por tanto, concluye que los resultados del cumplimiento de las políticas de seguridad de la información son 63,9% para el comportamiento de los usuarios de tecnologías de la información consistente en comportamientos intencionales y no intencionales.

Zevallos, M. (2019), en su artículo científico Model of Information Security Risk Management, realiza una revisión literaria de marcos, modelos y metodologías de Risk Management para identificar actividades, elementos y componentes a desarrollar para la elaboración de un Risk Management model orientado a la seguridad de la información, en el artículo citado se aplica el estado del arte relativo a los Risk Management models orientados a la security of the information; También especifica que la implementación de un Risk Management model alineado con los requisitos de una organización, influye en la reducción de costos, plazos, hace que los procesos de una organización sean más predecibles, permite que la alta dirección tome mejores decisiones, comunique

y resuelva sus riesgos de manera efectiva. También indica que las organizaciones enfrentan diferentes tipos de riesgos, por lo que no se recomienda copiar y aplicar un estándar existente y usarlo como práctica estándar. El objetivo de la Risk Management es desarrollar un análisis detallado de la organización, sus operaciones, activos, procesos e interrelaciones existentes con el fin de establecer una lista integral de riesgos, que consiste en identificar, analizar y ofrecer alternativas de tratamiento con riesgos reales y potenciales.

Rayme, R. (2007), en su disertación, Gestión de la seguridad de la información y servicios críticos en las universidades, propone estrategias de gestión para la seguridad de la información y su impacto en la calidad y eficiencia de los servicios críticos (admisión, registros, grados y títulos, tesorería, tramite documental) de las universidades. Su muestra estuvo formada por 30 expertos en TIC que trabajan en la UNMSM, UNFV y Universidad Privada San Juan Bautista (UPSB). Se aplicó una encuesta en línea para evaluar sus opiniones sobre la gestión de la seguridad y los servicios esenciales; los resultados obtenidos fueron principalmente la estrategia para el desarrollo de políticas de seguridad: UNMSM 37%, UNFV 19% y UPSB 24%; como segunda estrategia está la formación de personal, para lo cual los especialistas consultados indicaron el interés de participar: UNMSM 60%, UNFV 70% y UPSB 24% y como tercera estrategia tenemos la protección de los recursos de información en la que el 38% de los especialistas dijeron que sus centros de datos carecen de equipos de protección contra cortes de energía. Con la implementación de estas estrategias, según los expertos consultados, se obtendrá un 50% en relación a una mejor protección de la información y un 27% en términos de mejora de la calidad del servicio a los estudiantes y un 27% en relación a docentes. Asimismo, se minimizarán los riesgos de información: la UNMSM en cuanto a la infección por virus informáticos es del 56%, la universidad con un porcentaje elevado en comparación con otras universidades consultadas. En cuanto a los incidentes de seguridad (modificación no autorizada, divulgación ilícita y robo de información), los resultados muestran que el 70% son causados por trabajadores, imprudencia en su conocimiento de la seguridad y hechos delictivo. Según los resultados de esta investigación, se recomienda que las autoridades universitarias desarrollen

y apliquen políticas de seguridad de la información, ya que esto representa una base de seguridad. También se recomienda realizar un programa de capacitación a los trabajadores en temas de seguridad de la información y finalmente existe la necesidad de reestructurar las redes informáticas mediante la aplicación de tecnologías de prevención y detección de intrusos.

Los aportes teóricos y enfoques que favorecen la consistencia científica del objeto de estudio están centrada en la Teoría General de sistemas, Teoría de la Información y Enfoque basado en Riesgos. Así mismo, para Tamayo, A (1999), menciona que la Teoría general de sistemas se orienta hacia la formulación de principios elementales que permitan combinar el conocimiento de toda la amplia gama de sistemas vivos y no vivos. Tamayo lo considera como un método orientado a estudiar el sistema en su conjunto, integrado con sus componentes como base y analizando las relaciones e interrelaciones que existen entre las partes, conduciendo a una comprensión general del sistema. La teoría general de sistemas permite la elaboración de modelos y predecir cómo se comportarán antes de la puesta en servicio mediante procesos de simulación, seleccionando la mejor opción para el problema analizado.

Según Aladro Vico, E. (2011), señala en su artículo que la teoría de la información surgió de la teoría del periodismo y la teoría de la noticia, esta teoría fue adaptada a las teorías matemáticas y cibernéticas que se dieron sobre los fenómenos comunicativos. Por otro lado, la teoría de la información está relacionada con las leyes matemáticas que gobiernan la transferencia y procesamiento de la información; es una disciplina que trata sobre cómo almacenar y transferir información entre dispositivos.

Respecto al enfoque basado en riesgos, Ambrústolo et al., (2020), en su disertación menciona que la implementación del enfoque basado en riesgos permitió desarrollar un enfoque proactivo, bajo un enfoque estructurado, sistémico y estandarizado que tiene en cuenta la integridad de las actividades de la organización. Asimismo, el enfoque basado en riesgos según la ISO 9001 tiene como objetivo principal identificar los efectos de las incertidumbres comerciales y determinar los riesgos como base para la planificación.

Según el D.L. N° 1412, (2018), que aprueba la Ley del Gobierno Digital, en su capítulo VI, articulo 30 define la Seguridad Digital a nivel nacional como la etapa de confianza en el entorno digital, estado de confianza que se obtiene a partir de la administración y aplicación de reglas proactivas y reactivas a Risks que perjudican la seguridad de las personas, el activo económico y social, la seguridad nacional y los objetivos nacionales, con articulación de representantes del sector público, privado y otros que apoyan la ejecución de controles, acciones y medidas**.** Es decir, la Digital Security se encarga de las medidas de Security of the information procesada, transmitida, almacenada o contenida en el entorno digital, buscando generar confianza, administrando los Risks que perturban la seguridad de las personas y los activos económicos y sociales.

Por otro lado, según el D.S-N-050-2018-PCM (2018), define la Digital Security a nivel nacional como la etapa de confianza en el entorno digital, estado de confianza que se obtiene a partir de la administración y aplicación de reglas proactivas y reactivas a Risks que perjudican la seguridad de las personas, el activo económico y social, la seguridad nacional y los objetivos nacionales, con articulación de representantes del sector público, privado y otros que apoyan la ejecución de controles, acciones y medidas

Según Figueroa Suárez et al., (2017) Security of the information es aquella:

> “[…] Que tiene como objetivo proteger los activos de información independientemente de su forma o estado, utilizando metodologías, estándares, técnicas, herramientas, estructuras organizativas, tecnologías y otros elementos, para el Aplicación y gestión de las medidas de seguridad adecuadas en cada caso. Por tanto, cubre la seguridad informática "

Por lo tanto, cuando hablamos de Security of the information, estamos hablando de protegerla de Risks que afecten a más de una de las tres propiedades fundamentales: (1) la confidencialidad es decir la información solo debe estar disponible o pública para quienes están autorizados, (2) integridad, es decir, la información debe conservarse correcta y (3) la disponibilidad consiste en que la

información debe estar siempre disponible para aquellos que están autorizados. (González et al., 2015, p.14)

La información es el activo más importante que las organizaciones deben proteger. Por lo tanto, el activo es todo lo que tiene valor para la organización y, por lo tanto, debe protegerse. (NTP-ISO/IEC 27005, 2018, p. 19). Por otro lado para González et al., (2015), considera que el activo es cualquier recurso de la empresa necesario para realizar las actividades diarias y cuya indisponibilidad o deterioro representa una pérdida o costo.

El Departamento Administrativo de la Función Pública de Colombia, (2018), considera como Activos las aplicaciones de la empresa, servicios web, redes, hardware, información física o digital, recursos humanos, etc., que la empresa utiliza para desenvolverse en su entorno Digital.

Los Risk management models se utilizan para implementar un proceso lógico y sistemático utilizado para la toma de decisiones y para perfeccionar la eficiencia y eficacia de las empresas. (Hernández Díaz et al., 2013, p.61). Un Management model es un marco de referencia para la gestión de una entidad que se puede aplicar tanto en negocios y empresas privadas como en la administración pública.

Según Valencia et al., (2016) la Risk management es:

> "[…] Un método sistemático mediante el cual los risks asociados a una actividad, función o proceso pueden ser planificados, identificados, analizados, evaluados, manejados y monitoreados con la finalidad que la organización pueda disminuir pérdidas y aumentar sus oportunidades, en este caso las Actividades, funciones, procesos y recursos que forman parte de las TIC".

Para González et al., (2015), la Risk management se considera como actividades cuyo objetivo es mantener el riesgo por debajo del umbral fijado por la empresa, para ello las organizaciones deben realizar dos tareas principales: (1) Análisis de riesgo que consiste en conocer el nivel de Risk que asume la empresa, por lo

que esta tarea sugiere realizar un inventario de los activos donde se determinen las amenazas, la probabilidad de su ocurrencia y los posibles efectos. (2) Tratamiento de riesgos para los riesgos que se encuentran por encima del umbral establecido.

Según ISO 31000: 2018, la Risk management lo considera como las acciones coordinadas para conducir y controlar la empresa en relación con los Risk; para la gestión tiene en cuenta el contexto interno y externo de la empresa, incluido el los factores culturales y el comportamiento humano. (ISO, 2018)

ISO 31000: 2009, herramienta que nos brinda los principios, marco y proceso para una adecuada gestión de riesgos, esta norma es utilizada por todas las organizaciones públicas o privadas, y que ayuda a las organizaciones a lograr sus metas, mejorar la identificación de oportunidades, amenazas, distribución y uso de recursos para la gestión de riesgos. (Lizarzaburu Bolaños et al., 2019).
Referente al risk management model de TI para mejorar la seguridad de la información en la UNTRM, se basa en la Norma ISO 31000 cuyo enfoque está orientado a la mejora continua y a los procesos operacionales que maneja la Universidad, por lo que se asume como dimensiones las siguientes fases:

Fase de Establecimiento del contexto: Según Ramírez-Castro & Ortíz-Bayona, (2011), esta fase consiste en conocer internamente y de manera integral a la organización, es decir, protegerla y cómo se va a realizar esta protección, para determinar el grado de aceptación del riesgo, determinado el alcance y restricciones existentes.

En esta fase se toma en cuenta dos contextos: (1) el contexto interno que tiene que ver con lo cultural es decir el comportamiento en cuanto a los actores (estudiantes, docentes, administrativos y autoridades) que pertenecen a la universidad, la interrelación que se establecen entre los actores dando lugar a los procesos académicos y administrativos soportados por las TICs, la estructura universitaria, recursos (activos: servidores, tecnologías de información, equipos de cómputo, de red, sistemas de protección eléctrica, etc) y las metas y objetivos referente a calidad educativa y la acreditación universitaria. (2) Contexto externo:

entornos empresariales, elementos externos a la universidad que puedan afectar su desempeño, sociales y culturales, referentes al estilo de vida, contexto geográfico y demográfico, etc. relacionados con estudiantes, empresas, gobiernos locales y regionales, estándares de acreditación y cumplimiento de estándares de calidad, financieros y políticos.

Fase de Identificación de activos, en esta fase se hace una (1) clasificación de los activos según: procesos de negocio (proceso de matrícula, gestión académica, investigación, gestión de biblioteca, tutoría, bienestar universitario, gestión virtual, gestión de convalidación), servicios (gestión académica, Campus virtual, correo electrónico, Wiffi, Acceso a internet, Conferencia, Audiovisuales, catálogo de biblioteca en Online), aplicaciones (Sistema de Gestión de Base de Datos, Gestión: académica, administrativo, personal, e investigación, los sistemas de: biblioteca virtual, tutoría, finanzas, logística, continua y bolsa de trabajo), soporte de TI (Servidor web, servidores de bases de datos, servidor de seguridad, servidor de comunicaciones, etc.). (2) subordinación de activos, (3) estimación de los activos.

Fase de Análisis del riesgo, aquí se determina la probabilidad de que ocurra el riesgo, el impacto del riesgo y evaluamos el nivel de riesgo. (Casares San José-Martí & Lizarzaburú Bolaños, 2016)

Fase de valoración del riesgo, aquí se identifican los activos a proteger, para la valoración de los activos se toman en cuenta los activos en cuestión así como: procesos, información, datos y activos de soporte, estos activos de soporte que incluyen costos de adquisición, renovación o remplazo, mantenimiento y factores de depreciación.(Ramírez Castro & Ortíz Bayona, 2011)

En la Fase de tratamiento y gestión de riesgos se definen las medidas que se deben implementar para hacer frente a un riesgo, aceptando, evitando, mitigando y compartir el riesgo.

Según Ramírez-Castro & Ortíz-Bayona, (2011), menciona que en esta fase se establecen y ejecutan acciones para mitigar los riesgos encontrados y alcanzar los riesgos residuales aceptables para la organización.

III. METODOLOGÍA

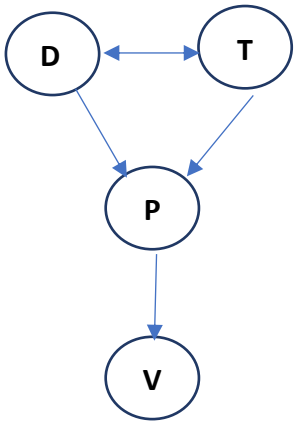
3.1. Tipo y diseño de investigación

La investigación según su finalidad se enmarcada en una investigación básica, porque su propósito es construir y ampliar la base de conocimiento teórico de una disciplina.(Müggenburg & Pérez, 2007)

Por su carácter, es descriptiva-propositiva, porque describe teóricamente las características de un fenómeno en base a sus variables, especificando características de los riesgos y propone un risk management model para mejorar la seguridad de la información. (Cabezas Mejía et al., 2018)

El diseño del estudio es cuantitativo de tipo no experimental, porque se van a evaluar los datos de manera numérica con ayuda de la estadística para poder analizar los datos con posterioridad.(Sanca Tinta, 2011)

A continuación, se presenta el esquema del diseño de la investigación:



LEYENDA

D : Diagnostico

T : **Teoría**

P : **Propuesta**

V : **Validación**

3.2. Variables y operacionalización.

Variable dependiente: Seguridad de la información

Definición conceptual

Según Figueroa Suárez et al., (2017) seguridad de la información es aquella:

> "[…] Que tiene como objetivo proteger los activos de información independientemente de su forma o estado, utilizando

metodologías, estándares, técnicas, herramientas, estructuras organizativas, tecnologías y otros elementos, para el Aplicación y gestión de las medidas de seguridad adecuadas en cada caso. Por tanto, cubre la seguridad informática "

.

Definición operacional

Es un conjunto de medidas anticipadas y reactivas que protegen y salvaguardar la información sobre el patrimonio de la universidad, es decir, son las políticas de uso y medidas que alteran el tratamiento de los datos utilizados en la universidad.

Variable independiente: Modelo de Gestión de Riesgos

Definición conceptual

Según Valencia et al., (2016) la gestión de Riesgos es:

“[…] Un método sistemático mediante el cual los riesgos asociados a una actividad, función o proceso pueden ser planificados, identificados, analizados, evaluados, manejados y monitoreados para que la organización pueda reducir pérdidas y aumentar sus oportunidades, en este caso las Actividades, funciones, procesos y recursos que forman parte de las TIC”.

Definición Operacional

Instrumento de gestión teórico-práctico orientado a identificar, evaluar y minimizar todos los posibles riesgos informáticos asociados a las actividades, operaciones y activos de la universidad, permitiendo así a la universidad definir y ejecutar estrategias que prevengan y reduzcan riesgos para garantizar la continuidad del negocio.

3.3. Población y muestra

Toledo Diaz de Leon, (2015). plantea que la población o el universo está “conformado por todos los elementos involucrados en el fenómeno definido y delimitado a través del análisis del problema de investigación. La población del trabajo estará conformada por los docentes (247) y Personal administrativo (235) nombrados y contratados de la UNTRM.

Tabla 1: Persona docente y administrativo de la UNTRM

Trabajadores	Modalidad	Subtotal	Total
Docentes	Nombrados	103	247
	Contratados	144	
Administrativos	Nombrados	45	235
	Contratados	190	
Total		482	482

Fuente: RR.HH. de la UNTRM

"La muestra es un subgrupo de la población o universo cuya selección refleja las características de la población y la muestra también debe ser proporcional al tamaño de la población que se selecciona mediante procedimientos aleatorios o probabilísticos" (Toledo Diaz de Leon, 2015). La muestra estará constituida por 40 trabajadores entre docentes y administrativos.

Tabla 2: Personal seleccionado para la muestra

Trabajadores	**Total**
Docentes de Sistemas	15
Administrativos de DAYRA	5
Administrativos del área de TI	5
Administrativos de DGCA	7
Administrativos Pos Grado	4
Alta Dirección	4
Total	40

Fuente: Elaboración Propia

“El muestreo es el proceso de extraer una muestra de la población, cuyo proceso fundamental es identificar la población que estará representada en el estudio. (Toledo Diaz de Leon, 2015). Con respecto a los docentes y administrativos serán seleccionados con el muestreo no probabilístico por conveniencia.

Criterios de inclusión. Docentes y personal administrativo de la UNTRM.

Criterios de exclusión. Aquellos docentes y administrativos que se encuentran al margen del proceso de investigación. Entre ellos el personal que estuvieron de vacaciones o permiso o ya no son contratados.

3.4. Técnicas e instrumentos de recolección de datos

Técnica de gabinete. Para contrastar la información se utilizará la técnica de análisis documental, y el gestor bibliográfico Mendeley para poder gestionar, sistematizar, analizar y evaluar información de documentos digitales como artículos, tesis, libros, etc. mientras que para el análisis de la información impresa se utilizará la técnica de fichaje teniendo en cuenta las citas de acuerdo a las normas APA 7.

“La técnica de la encuesta es muy utilizada como procedimiento de investigación, ya que permite obtener y procesar datos de manera rápida y eficiente” (Casas Anguita et al., 2003). Esta técnica permitirá la recolección de la información sustancial y pertinente de los docentes y administrativos de la UNTRM, proporcionándonos su opinión sobre la seguridad de la información. Su implementación se realizará mediante un cuestionario.

Cuestionario. “Es el instrumento que acopia de manera organizada los indicadores de las variables involucradas en el objetivo de la encuesta” (Casas Anguita et al., 2003). Instrumento elaborado con 30 ítems correspondientes a la variable Seguridad de la Información, clasificado en 3 dimensiones, teniendo como propósito recoger el grado de conocimiento de los docentes y administrativos sobre la seguridad de la información.

Para la validación del instrumento se aplicó la técnica de Juicio de expertos los mismos que evaluarán la estructura y contenido de la misma, serán especialistas y profesionales capacitados en Gestión Pública. La validación es “la capacidad de un instrumento para poder medir la variable para la cual

ha sido deseñado, la misma que tiene una validez lógica, de contenido, de criterio y de constructo" (Villavicencio Caparó et al, 2018)

"La confiabilidad del instrumento muestra hasta qué punto los resultados obtenidos con la aplicación de un instrumento son realmente útiles, sólidos y consistentes" (Martínez & March, 2015). Se realizará a través de la aplicación del coeficiente Alfa de Cronbach, cuyos resultados estimarán un +índice de fiabilidad en base a la correlación y consistencia interna de sus indicadores.

3.5. Procedimiento

El procedimiento que se realizará para recolectar datos, parte de la elaboración y aplicación de un cuestionario congruente con el marco teórico, las dimensiones e indicadores de la variable dependiente, el mismo que será socializado y administrado a los docentes y administrativos de la UNTRM para recoger la información real de la variable dependiente Seguridad de la Información.

Las acciones a desarrollar para la ejecución del instrumento online comprenden: coordinaciones virtuales previas con los funcionarios y agentes participantes para sensibilizar sobre la intención de la investigación, desarrollo del cuestionario en forma simultánea e intermitente (se respetará la predisposición de tiempo de los sujetos), asignación de un tiempo razonable, recojo digital, verificación del llenado de los ítems y procesamiento análisis e interpretación de los resultados.

3.6. Métodos de análisis de datos

El método de análisis es cuantitativo. El análisis estadístico de los datos se realizará a través de la técnica de la tabulación de datos, que permitirá ordenar y organizar los resultados en tablas y figuras, para realizar el análisis e interpretación de la información obtenida en forma objetiva con respecto al objeto de estudio.

Recogidos los datos, estos serán ingresados, agrupados y procesados en un ordenador o software estadístico aplicativo (SPSS versión 21), para agilizar el agrupamiento y análisis de los mismos para dar solución a los objetivos planteados. Esto, permitirá visualizar los resultados en tablas de una y dos

entradas con respecto a la seguridad de la información en sus 3 dimensiones, también se determinarán estadísticos descriptivos y de dispersión con la finalidad de determinar los niveles o categorías de la variable en estudio.

3.7. Aspectos éticos

Para realizar la presente investigación, se tendrá en cuenta las normas del comité de ética de la Universidad Cesar Vallejo, respetando los estándares de rigor científico, responsabilidad y honestidad. Se mantendrá la confidencialidad de la información desde la medición de línea base hasta la medición final.

Los docentes y administradores de la UNTRM Amazonas considerados en la muestra representativa del estudio serán informados de manera oportuna de los objetivos y la confidencialidad de la investigación para tener su aceptación mediante la firma del documento de consentimiento informado, además, se garantizará que la participación en la aplicación del instrumento de recolección de datos sea consciente y voluntaria.

El estudio incluye principios éticos básicos; Se pondrán en práctica los principios de honestidad y respeto a los derechos de terceros, así mismo, las decisiones que se tomen en el contexto del proceso de investigación estarán sujetas al cumplimiento de los aspectos legales pertinentes y a garantizar la calidad de la investigación. Por lo tanto, bajo la Ley 27444 de Procedimiento Administrativo General, la investigación cumplirá con los estándares internacionales de citas y referencias de las fuentes consultadas; Asimismo, los datos e información presentados en su contenido se beneficiarán de la originalidad, objetividad, autenticidad y veracidad. (Ministerio de Justicia y Derechos Humanos, 2017).

IV. RESULTADOS

Tabla 1: Resultados en la dimensión Confidencialidad de la security of the information en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas

N°	Confidencialidad	Nunca	Casi nunca	Algunas Veces	Casi Siempre	Siempre
1	La UNTRM invierte presupuesto en ciberseguridad.	10,3%	20,7%	37,9%	20,7%	10,3%
2	La UNTRM prioriza dentro de sus gastos en TI la protección de sus activos informáticos.	6,9%	20,7%	37,9%	27,6%	6,9%
3	La UNTRM selecciona y contrata personal especializado idóneo para el departamento de Seguridad informática.	10,3%	27,6%	44,8%	13,8%	3,4%
4	La UNTRM propone e implementa políticas de seguridad para el adecuado manejo de la información	3,4%	10,3%	48,3%	34,5%	3,4%
5	La UNTRM capacita a la comunidad universitaria sobre la política de seguridad de la información.	24,1%	31,0%	37,9%	3,4%	3,4%
6	La UNTRM capacita a los trabajadores sobre la clasificación de los activos de información y su importancia.	24,1%	37,9%	31,0%	3,4%	3,4%
7	Usted resguarda la información de la universidad en medios seguros.	6,9%	0%	17,2%	31,0%	44,8%
8	Los Archivos que usted comparte en carpetas cuenta con permisos de acceso solo para las personas autorizadas.	0%	13,8%	17,2%	17,2%	51,7%
9	Las contraseñas que usted genera para el uso de los sistemas generalmente son contraseñas complejas.	0%	6,9%	24,1%	27,6%	41,4%
10	La UNTRM implementa políticas y controles eficientes que determinen la conducta inapropiada que tiene un empleado, respecto a la seguridad de la información.	10,3%	34,5%	27,6%	13,8%	13,8%
11	El departamento de TI de la UNTRM, utiliza Antivirus, Firewall, AntiSpyware, Antimalware, sistemas de detección de intrusos u otra herramienta para mantener seguro la red informática de la universidad.	3,4%	13,8%	20,7%	34,5%	27,6%
12	El área de TI de la UNTRM realiza prueba de seguridad en sus redes informáticas.	6,9%	27,6%	24,1%	27,6%	13,8%
13	Existen accesos restringidos a el área de TIC de la UNTRM	3,4%	24,1%	17,2%	31,0%	24,1%

Fuente: Aplicación de instrumentos a personal de TI y administrativos de la UNTRM

En la Tabla 1 referente a la confidencialidad; se observa que el 10.3% de los encuestados manifiesta que nunca la UNTRM invierte en ciberseguridad, un 20.7% casi nunca, un 37,9% algunas veces, un 20.7% casi siempre y un 10.3% siempre, aspecto que muestra el escaso presupuesto que se invierte en

ciberseguridad. Sobre la priorización del gasto en protección de sus activos informáticos, el 6.9% manifiesta que nunca, 20.7% casi nunca, 37.9% algunas veces, 27.6% casi siempre y un 6.9% siempre, indicador en la que se visualiza poca priorización del gasto en la protección de los activos informáticos. En lo referente a la selección y contratación del personal especializado para el departamento de seguridad informática, el 10.3% manifiesta que nunca, 27,6% casi nunca, 44,8% algunas veces y un 13.8% casi siempre, observándose que la selección del personal no siempre es el especializado para el departamento de seguridad. En lo referente a si la UNTRM propone e implementa políticas de seguridad para el adecuado manejo de la información, un 3,4% manifiesta que nunca, 10,3% casi nunca, 48,3% algunas veces, un 34.5.% casi siempre y un 3.4% siempre, aspecto que hace visible la carencia de políticas seguridad para el adecuado manejo de la información. Respecto a Capacitación sobre la política de seguridad de la información a la comunidad universitaria, el 24.1% respondió que nuca, 31,0% casi nunca, 37.9% algunas veces, y un 3,4% casi siempre y siempre, indicador que la que se percibe que algunas veces se capacita a los miembros de la comunidad universitaria respecto a las políticas de seguridad de la información. Respecto a Capacitación a los trabajadores sobre clasificación de los activos de información y su importancia, se observa que el 24.1.% afirma que nuca, el 37.9% casi nunca, 31.0% algunas veces y un 3,4% casi siempre y siempre, aspecto que manifiesta la insuficiente capacitación a los trabajadores sobre la clasificación de los activos de información. Sobre el resguardo de la información en medios seguros, el 6,9% afirma que nunca lo realiza, 17,2% algunas veces, 31,0% casi siempre y un 51.7% siempre, indicador en la que afirma que más de la mitad si resguarda la información en medios seguros. Referente a los archivos que comparte y si cuenta con permisos de acceso solo para personas autorizadas, un 17,2% responde casi siempre, y un 51.7% siempre, los que se observa aquí, es que la mayoría comparte carpetas con permisos de acceso solo para personas autorizadas. Así mismo, sobre las contraseñas complejas que genera para el uso de los sistemas, el 27.6% respondió casi siempre y un 41,4% siempre, quedando claro menos de la mitad de los encuestados usa contraseñas complejas para el uso de los sistemas. Referente a la implementación de políticas y controles eficientes que determinen la conducta inapropiada de un empleado respecto a la seguridad de la

información, un 10,3% manifiesta que nunca, 34,5% casi nunca, 27.6% algunas veces, y el 13.8% casi siempre y siempre, observándose en este indicador que las políticas y controles que permitan determinar la conducta inapropiada de un empleado es ineficiente. El departamento de TI utiliza antivirus, Firewall, AntiSpyware, Antimalware, sistema de detección de intrusos para mantener seguro la red informática, 3,4% respondió nunca, 13.8% casi nunca, 20.7% algunas veces, 34,5% casi siempre y un 27,6% siempre, aquí se observa que el departamento de TI casi siempre utiliza herramientas para mantener seguro la red informática de la universidad. El área de TI realiza pruebas de seguridad en sus redes informáticas, el 6.9% manifiesta que nunca, 27.6% casi nunca, 24.1% algunas veces y un 13.8% siempre, observándose que algunas veces se realiza pruebas de seguridad, pruebas que son muy importantes realizar para evitar que los intrusos aprovechen las vulnerabilidades que pueden estas libres. Existe acceso restringido al área de TIC, el 3,4% afirma que nuca, 24.1% casi nunca, 17,2% algunas veces, 31.0% casi siempre y 24,1% siempre, observándose que no siempre el acceso a las TIC no es en la mayoría restringido. Finalmente, en esta dimensión se constató que la información que manejan los trabajadores es insegura, debido a que no se implementan adecuadas políticas de seguridad de la información, del mismo modo no se capacita al personal en estos temas referente a la seguridad de la información y por ende no se prioriza dentro del gasto de TI de la UNTRM la protección de sus activos de información, exponiendo la divulgación no autorizada de la información de la UNTRM.

Tabla 2: Resultados en la dimensión Integridad de datos en la security of the information en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas.

Item	Integridad de datos	Nunca	Casi nunca	Algunas Veces	Casi Siempre	Siempre
14	Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de la misma.	3,4%	13,8%	10,3%	20,7%	51,7%
15	Realiza cambios periódicos de contraseña para ingresar a su equipo de cómputo.	6,9%	20,7%	17,2%	20,7%	34,5%
16	La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave.	3,4%	24,1%	13,8%	27,6%	31,0%
17	El antivirus instalado en su equipo es actualizado continuamente.	6,9%	10,3%	20,7%	27,6%	34,5%
18	Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia.	20,7%	24,1%	10,3%	24,1%	20,7%
19	Realizan periódicamente mantenimientos a su equipo de cómputo	13,8%	3,4%	27,6%	27,6%	27,6%
20	La UNTRM realiza capacitaciones sobre ataques informáticos en sus diversas modalidades.	24,1%	44,8%	20,7%	6,9%	3,4%
21	Has tenido algún problema con Malware, Virus, Gusano, Troyano, Spyware, Adware, o Ranssonware.	13,8%	24,1%	51,7%	10,3%	0%
22	Se evalúa el nivel de educación y conocimiento sobre seguridad de la información que tiene un trabajador de la UNTRM.	24,1%	34,5%	27,6%	6,9%	6,9%

Fuente: Aplicación de instrumentos a personal de TI y administrativos de la UNTRM

En la Tabla 2 respecto a la Integridad de datos, se observa que el 3,4% manifiesta que nunca realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de la misma, 13.8% casi nuca, 10.3.% algunas veces, 20,7% casi siempre y un 51,7% siempre, esto nos indica que existe un porcentaje reducido de los encuestados que algunas veces realiza el bloqueo, y más de la mitad de los encuestado mencionan que siempre realizan el bloque al retirarse de su equipo de cómputo. El mayor porcentaje de las personas encuestadas

afirman que realizan cambios periódicos de contraseñas para ingresar a su equipo de cómputo, así tenemos que el 34.5% afirma que siempre, 20.7% casi siempre, 17,2% algunas veces, 20,7% casi nunca y un 6.9% nunca, por lo tanto, los usuarios realizan cambios periódicos de contraseñas. Un alto porcentaje de los encuestados afirma que la documentación en físico que maneja se encuentra resguardada en un lugar seguro y bajo llave, así tenemos que el 31,0% afirma que siempre, 27.6% casi siempre, 13.8% algunas veces, 24,1% casi nunca y un 3,4% nunca, esto indica que existe aún un cierto porcentaje de encuestados que afirman que casi nunca la documentación física que maneja se encuentra resguardada en un lugar seguro y bajo llave. Respecto a si se mantienen continuamente actualizado los antivirus, el 6,9% afirma que nunca, 10.3% casi nunca, 20.7% algunas veces, 27,6% casi siempre y un 34.5% siempre, aspecto que indica que un porcentaje promedio del 16 % de los encuestados afirman que no se mantiene actualizado los antivirus en los equipos de cómputo. Ante cortes eléctricos e imprevistos, cuenta con medidas de contingencia, el 20.7% menciona que nuca, 24,1% casi nunca, 10.3% algunas veces, 24.1% casi siempre y 20.7% siempre, esto indica que existe un porcentaje de los encuestados que afirma que no se cuenta con las medidas de contingencias ante cortes eléctricos. Realizan mantenimientos periódicos a su equipo de cómputo, el 13.8% respondió que nunca, 3,4% casi nunca, 27,6% algunas veces, casi siempre y siempre, esto nos da a conocer que la gran mayoría afirma que si realizan el mantenimiento periódico a su equipo de cómputo y quedando un porcentaje reducido que afirma que nunca o casi nunca realiza el mencionado mantenimiento. Referente a las capacitaciones sobre ataques informáticos en sus diversas modalidades, el 24,1% afirma que nunca, 44,8% casi nunca, 20,7% algunas veces, 6,9% casi siempre y un 3,4% siempre, aspecto que nos indica que no se cuenta con las capacitaciones sobre ataques informáticos, capacitaciones necesarias para poder prevenir los ataques y proteger la información que maneja cada usuario en su PC. Respecto a problemas con malwares, virus, gusanos, troyanos, spyware, adware o Ranssonware, el 13.8% sostiene que nunca, 24,1% casi nunca, 51,7% algunas veces y un 10,3% casi siempre, esta pregunta nos afirma que un gran porcentaje si ha tenido problemas con virus, malware, etc. Respecto a si se evalúa el nivel de educación y conocimiento sobre seguridad de información que debe tener un trabajador de la

universidad, el 24.1% afirma que nunca, 34,5% casi nunca, 27,6% algunas veces, 6,9% casi siempre y siempre, esto nos afirma lo importante que es la evaluación de los trabajadores respecto al nivel de educación y conocimiento sobre seguridad de la información. Finalmente, en esta dimensión se constató que tan importante es los cambios periódicos de contraseña, resguardar la información bajo llave, mantener los equipos con antivirus actualizados, contar con medidas de contingencias ante cortes eléctricos y el conocimiento que debe tener el trabajador sobre temas de seguridad de la información, para que de esta manera se mantenga integra la información, previniendo modificaciones no autorizadas de la misma.

Tabla 3:Resultados en la dimensión Disponibilidad de la security of the information en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas.

Item	Disponibilidad	Nunca	Casi nunca	Algunas Veces	Casi Siempre	Siempre
23	Para evitar olvidar la contraseña de su sistema, acostumbra copiarlo en un Post-it y lo pega en la pantalla del computador.	79,3%	10,3%	10,3%	0%	0%
24	Se encuentra disponible la información que requiere para desarrollar su trabajo.	6,9%	0%	17,2%	44,8%	31,0%
25	Los sistemas con los que cuenta la UNTRM son rápidos	6,9%	0%	55,2%	24,1%	13,8%
26	El tiempo de recuperación de un sistema ente una incidencia es rápida.	3,4%	20,7%	37,9%	34,5%	3,4%
27	Usted realiza periódicamente una copia de seguridad de la información que usted maneja.	3,4%	17,2%	20,7%	24,1%	34,5%
28	Cuenta en todo momento con acceso a la información que requiere para realizar sus labores.	0%	0%	24,1%	48,3%	27,6%
29	La página web institucional de la UNTRM se encuentra activa en todo momento.	0%	0%	10,3%	34,5%	55,2%
30	Usted conoce los procedimientos que se debe seguir en caso de detectar alguna falla o amenaza en los equipos de cómputo.	13,8%	6,9%	17,2%	27,6%	34,5%

Fuente: Aplicación de instrumentos a personal de TI y administrativos de la UNTRM.

En la Tabla 3, nos muestra información referente a la disponibilidad de la información, el 79,3% afirma que nunca acostumbra copiar la contraseña en un

Post-it y lo pega en la pantalla de su computador, asimismo el 10,3% casi nunca, y algunas veces, aspecto que nos muestra que la gran mayoría de los encuestados no expone sus claves. Respecto a si se encuentra disponible la información que requiere para desarrollar su trabajo, el 6,9% afirma que nunca, 17,2% algunas veces, 44.8% casi siempre y un 31,0% siempre, esto nos afirma que siempre se encuentra disponible la información para que pueda realizar su trabajo en las áreas correspondientes. Los sistemas con los que cuenta la universidad son rápidos, el 6,9% manifiesta que nunca, 55,2% algunas veces, 24,1% casi siempre y 13,8% siempre, esto nos confirma que existe un alto porcentaje que afirma que no son rápidos los sistemas. El tiempo de recuperación de un sistema ante una incidencia es rápida, el 3,4% afirma que nunca, 20,7% casi nunca, 37,9% algunas veces, 34,5% casi siempre y 3.4 siempre, este indicador nos muestra que el tiempo de recuperación no es la adecuada. Referente a, si realiza periódicamente una copia de seguridad de la información que maneja, el 3,4% manifiesta que nuca, 17,2% casi nunca, 20,7% algunas veces, 24,1% casi siempre y un 34,5% siempre, esto nos indica que aún existe un porcentaje de los encuestados que no realiza periódicamente copias de seguridad de su información. Cuenta en todo momento con acceso a la información que requiere para realizar sus labores, el 24,1% afirma que algunas veces, 48,3% casi siempre y un 27,6% siempre, esto nos confirma que la mayoría de los encuestados manifiesta que si cuenta con acceso a la información para realizar sus labores. Respecto a, si la página institucional de la universidad se encuentra activa en todo momento, el 10,3% afirma que algunas veces, 34,5% casi siempre y un 55,2% siempre, esto nos confirma que la pagina institucional de la universidad siempre se encuentra activa. Respecto al procedimiento que se debe seguir el trabajador en caso de detectar alguna falla o amenaza en los equipos de cómputo, el 13,8% afirma que no conoce, 6,9% casi no conoce, 17,2% algunas veces, 27,6% casi siempre y 34,5% siempre, esto nos confirma que existe un porcentaje reducido que no conoce el procedimiento que debe seguir ante alguna falla o amenaza en los equipos de cómputo. Finalmente, en esta dimensión se ve la importancia de no exponer las claves de acceso a los sistemas escribiéndola en post-it, que los sistemas sean rápidos, que la información sea accesible y segura, que ante una falla de los sistemas estos sean restablecidos rápidamente y la importancia de realizar las copias de

seguridad periódicamente, conocer los procedimientos que se debe seguir al detectar alguna falla o amenaza, previniendo de esta manera las interrupciones no autorizadas de los recursos informáticos.

Tabla 4: Nivel de la security of the information en la Universidad Nacional Toribio Rodríguez de Mendoza -Chachapoyas.

Dimensión	Niveles	Frecuencia	Porcentaje
Confidencialidad	Baja	2	6,9
	Regular	20	69,0
	Alta	7	24,1
Integridad de datos	Baja	4	13,8
	Regular	19	65,5
	Alta	6	20,7
Disponibilidad	Baja	1	3,4
	Regular	17	58,6
	Alta	11	37,9

Fuente: Aplicación de instrumentos a personal de TI y administrativos de la UNTRM

En la Tabla 4 se muestra el nivel de security of the information en la UNTRM, recogida desde la comunidad de universitaria, específicamente de la alta dirección, administrativos de DGCA, DAYRA, DTIC, donde se observó que la dimensión de confidencialidad se encuentra en un nivel regular de 69,0%, esto indica que la confidencialidad es inadecuada. Referente a la dimensión de integridad de los datos, el 65,5 % manifiesta en un nivel regular, esta dimensión nos indica que los trabajadores no previenen adecuadamente las modificaciones de la información. Respecto a la dimensión de disponibilidad el 58,6% manifiesta que se encuentra en un nivel regular, indicador que nos muestra que existen deficiencias en la disponibilidad de acceso a la información a usuarios autorizados, es decir que existen interrupciones no autorizados de los recursos informáticos.

V. DISCUSIÓN

El propósito de la investigación estuvo enfocado en la construcción de un Risk Management Model, propuesta que pretende contribuir en mejorar la Security of the information en la UNTRM – Chachapoyas, teniendo en cuenta el involucramiento de la alta dirección en establecer el presupuesto adecuado para que se invierta en seguridad de la información, creando el área de ciberseguridad articulada a la DTIC para que esta se encargue de elaborar las políticas de seguridad para la UNTRM, capacitando a la comunidad universitaria en temas de seguridad de la información, seleccionado al personal idóneo para el área de ciberseguridad , y de esta manera establecer una cultura en seguridad de la información y por ende una cultura en gestión de riesgos. Teniendo en cuenta a Anchundia-Betancourt, C.E (2017) en la que menciona que la universidad debe ser líder en cultura de ciberseguridad.

En ese sentido, para alcanzar el objetivo general se realizó un análisis situacional para evaluar la seguridad de la información en la UNTRM, mediante instrumentos confiables y válidos. Entre los hallazgos encontramos escaso presupuesto que la UNTRM destina para la ciberseguridad, tal como se aprecia en la tabla 1 referente a la confidencialidad; que el 10.3% de los encuestados manifiesta que nunca la UNTRM invierte en ciberseguridad, un 20.7% casi nunca, un 37,9% algunas veces, un 20.7% casi siempre y un 10.3% siempre. Asimismo, el estudio Anchundia-Betancourt, C.E (2017) determina que la ciberseguridad está generalizada a todo tipo de organizaciones, y que pueden extrapolar las circunstancias desfavorables a la educación superior. Además, menciona que la universidad debe ser líder en cultura de ciberseguridad.

Por otro lado, Altamirano-Yupanqui & Bayona-Oré, (2017) reafirman que la ciberseguridad, resultan ser parte del comportamiento humano a través de la teoría psicológica, en su estudio efectuaron una investigación

sistemática de la literatura científica, encontrando teorías de investigación relacionadas con el cumplimiento de las políticas de seguridad.

En relación a si la UNTRM propone e implementa políticas de seguridad para el apropiado manejo de la información en la Universidad los encuestados mencionan que un 3,4% manifiesta que nunca, 10,3% casi nunca, 48,3% algunas veces, un 34.5.% casi siempre y un 3.4% siempre, aspecto que hace visible la carencia de políticas seguridad para el adecuado manejo de la información. Respecto a Capacitación sobre la política de seguridad de la información en la comunidad universitaria, el 24.1% respondió que nuca, 31,0% casi nunca, 37.9% algunas veces, y un 3,4% casi siempre y siempre, indicador en la que se percibe que algunas veces se capacita a la comunidad universitaria respecto a las Information Security Policies, esto nos muestra el desinterés por cuidar adecuadamente el activo de la información en la UNTRM, exponiendo de esta manera a que puedan ser atacados tal como lo afirma el Education Cybersecurity Report (2018), en la que menciona que un tercio de los ataques cibernéticos son realizadas a las instituciones de educación superior, tal como lo que ha ocurrido a inicios del 2019 con más de 20 universidades norteamericanas.

Por otro lado, Don Welch, (2019), Chief Información Security Officer de la Universidad de Pennsylvania, menciona que la ciberseguridad no es solo una función de los responsables de TI, que es más bien una función institucional, por lo tanto, todos los miembros de la universidad tienen un papel muy importante que desempeñar y deben actuar en concordancia con la estrategia de ciberseguridad.

Respecto al primer objetivo específico de diagnóstico de los procesos de la UNTRM que utilizan tecnologías y sistemas de información, para identificar procesos críticos.

El área de TI realiza pruebas de seguridad en sus redes informáticas, el 6.9% manifiesta que nunca, 27.6% casi nunca, 24.1% algunas veces y un

13.8% siempre, observándose que algunas veces se realiza pruebas de seguridad, pruebas que son muy importantes realizar para evitar que los intrusos aprovechen las vulnerabilidades que pueden estas libres.

De lo expuesto, se puede manifestar Gutiérrez & Sánchez-Ortiz, (2018) en la que menciona que la gestión de riesgos basado en el estándar ISO 31000: 2012 para docencia de pregrado de la Universidad de Chile. El modelo propuesto permitió favorecer los procesos de acreditación para mejorar la eficiencia de los procesos docentes, creando matrices de riesgo y determinando indicadores clave de riesgo (KRI). Se definieron los riesgos inherentes y remanentes en los procesos docentes, así como el control de los procesos críticos.

Asimismo, Correa Henao et al., (2017) propusieron las buenas prácticas en cultura organizacional, analizando las metodologías aceptadas para llevar a cabo el proceso de identificación y análisis de riesgos en el campo organizacional, por lo tanto con una buena cultura de la gestión de riesgos mejorar la organización y fortalecer gradualmente la competitividad de la empresa. Así mismo en esta dimensión se constató que tan importante es los cambios periódicos de contraseña, resguardar la información bajo llave, mantener los equipos con antivirus actualizados, contar con medidas de contingencias ante cortes eléctricos y el conocimiento que debe tener el trabajador sobre temas de seguridad de la información, para que de esta manera se mantenga integra la información, previniendo modificaciones no autorizadas de la misma.

En relación al segundo objetivo específico: diseñar el Risk Management Model para mejorar la security of the information en la UNTRM.
Se obtiene que la UNTRM propone e implementa políticas de seguridad para el adecuado manejo de la información, un 3,4% manifiesta que nunca, 10,3% casi nunca, 48,3% algunas veces, un 34.5.% casi siempre y un 3.4% siempre, aspecto que hace visible la carencia de políticas de seguridad para la adecuada administración de la información.

Se tiene el estudio de Rayme, R. (2007), en su disertación, Gestión de la seguridad de la información y servicios críticos en las universidades, propone estrategias de gestión para la security of the information y su impacto en la eficiencia y calidad de los servicios críticos (admisión, registros, grados y títulos, tesorería, tramite documental) de las universidades.

Por otro lado, Ramírez-Castro & Ortíz-Bayona, (2011) menciona lo importante de conocer internamente y de manera integral a la organización, es decir, protegerla y cómo se va a realizar esta protección, para determinar el grado de aceptación del riesgo, determinado el alcance y restricciones existentes.

Del mismo modo Correa Henao et al., (2017) en su investigación se plantearon el objetivo de gestionar los riesgos en el entorno empresarial colombiano, a través de buenas prácticas en cultura organizacional, analizando las metodologías aceptadas para llevar a cabo el proceso de 'análisis e identificación de riesgos en el campo corporativo y organizacional. A medida que la cultura de la gestión de riesgos evolucione en las organizaciones y la dirección de las organizaciones invierta en la gestión de riesgos, les ayudará a mejorar la organización y por tanto fortalecer gradualmente la competitividad de la empresa. Las organizaciones colombianas han aplicado la gestión de riesgos como política en sus modelos de negocio posibilitando la creación de una cultura de responsabilidad corporativa, mejora continua y competitividad, esto ha permitido a las empresas diseñar estrategias de mejora generando sistemas de control interno que permitan el cumplimiento. con sus objetivos misioneros, todo ello en base a la normativa vigente y los estándares internacionales que las organizaciones deben respetar para su certificación en gestión de riesgos.

Por otro lado, Zevallos, M. (2019), en su artículo científico Model of Information Security Risk Management, especifica que la implementación de un Risk Management model alineado con los requisitos de una

organización, influye en la reducción de costos, plazos, hace que los procesos de una organización sean más predecibles, permite que la alta dirección tome mejores decisiones, comunique y resuelva sus riesgos de manera efectiva. También indica que las organizaciones enfrentan diferentes tipos de riesgos, por lo que no se recomienda copiar y aplicar un estándar existente y usarlo como práctica estándar. El objetivo de la Risk Management es desarrollar un análisis minucioso de la organización, sus operaciones, activos, procesos e interrelaciones existentes con el fin de establecer una lista integral de riesgos, que consiste en identificar, analizar y ofrecer alternativas de tratamiento con riesgos reales y potenciales.

Podemos mencionar que para el diseño del Risk Management Model se debe tener cuentas las normas, leyes nacionales e internacionales, basada en las teorías, enfoques, y principios que establezca la UNTRM, el mencionado modelo debe permitir que los responsables de la ciberseguridad de la UNTRM, elaboren políticas, capaciten constantemente a la comunidad universitaria en temas de seguridad de la información, supervise y gestione los riesgos a los que se expone la UNTRM, cultivando de esta manera una cultura en seguridad de la información y por ende una cultura en la gestión de riesgos, ya que para que se pueda lograr esto todos los miembros de la comunidad universitaria colabores ya que esto es un trabajo en equipo, que involucra desde los directivos de la alta dirección hasta el personal de limpieza, tal como lo menciona Don Welch, (2019), Chief Information Security Officer de la Universidad de Pennsylvania, menciona que la ciberseguridad no es solo una función de los responsables de TI, que es más bien una función institucional, por lo tanto, todos los miembros de la UNTRM tienen un papel muy importante que desempeñar y deben actuar en concordancia con la estrategia de ciberseguridad.

El Tercer objetivo específico: validar el Risk Management Model para mejorar la security of the information de la UNTRM.

Se obtiene los resultados con respecto a capacitación a los trabajadores sobre clasificación de los activos de información y su importancia, se observa que el 24.1.% afirma que nuca, el 37.9% casi nunca, 31.0% algunas veces y un 3,4% casi siempre y siempre, aspecto que manifiesta la insuficiente capacitación a los trabajadores sobre la clasificación de los activos de información.

A esto podemos indicar que según Ramírez-Castro & Ortíz-Bayona, (2011), menciona que en esta fase se establecen y ejecutan acciones para mitigar los riesgos encontrados y alcanzar los riesgos residuales aceptables para la organización

Asimismo, (Casares San José-Martí & Lizarzaburú Bolaños, 2016) afirman que es necesario implementar un modelo que esté al nivel de la empresa se determina la probabilidad de que ocurra el riesgo, el impacto del riesgo y evaluamos el nivel de riesgo, donde se identifiquen activos a proteger, para la valoración de los activos.

Y por último (Ramírez Castro & Ortíz Bayona, 2011) también están de acuerdo que cada empresa o institución debe diseñar modelos con procesos, información, datos y activos de soporte, que incluyen costos de adquisición, renovación o remplazo, mantenimiento y factores de depreciación.

VI. CONCLUSIONES

1. Se diagnosticó el estado actual de los procesos de la UNTRM que utilizan tecnologías y sistemas de información, para identificar procesos críticos; en la cual, esto permitió identificar los procesos críticos sobre los cuales se realizó la evaluación de los escenarios de riesgo obteniendo un listado de procesos académicos y administrativos críticos de la UNTRM.
2. El proceso de evaluación diagnostica de la security of the information en la UNTRM, en base a la percepción de docentes y administrativos de la UNTRM se encuentra en un nivel regular con 69% referente a la confidencialidad, y en nivel regular con un 65,5 % respecto a la integridad de los datos y la disponibilidad de la información se encuentra en un nivel regular con un 58,6%, todo esto nos indica que los trabajadores no tiene una cultura en la gestión de riesgos, no conocen las políticas de seguridad de la información y por ende no se les capacita en estos temas, debido a que la UNTRM no invierte mucho presupuesto en ciberseguridad
3. Se diseñó el modelo de gestión de riesgos para mejorar la seguridad de la información en la UNTRM, aquí se toma en cuenta el contexto interno que tiene que ver con lo cultural es decir el comportamiento en cuanto a los actores (estudiantes, docentes, administrativos y autoridades) que pertenecen a la universidad, la interrelación que se establecen entre los actores dando lugar a los procesos académicos y administrativos soportados por las TICs.
4. La validación consistió en la evaluación de la estructura y profundidad del contenido realizada por personas expertas en gestión pública, quienes estudiaron y analizaron en forma rigurosa la originalidad, coherencia, pertinencia e interrelación entre los diversos componentes investigativos. Este proceso de revisión permitió recoger aportes y sugerencias, para ajustar y orientar los procedimientos y acciones de los stakeholder con el fin de garantizar la efectividad de la gestión de riesgos y resguardar adecuadamente la información de la UNTRM.

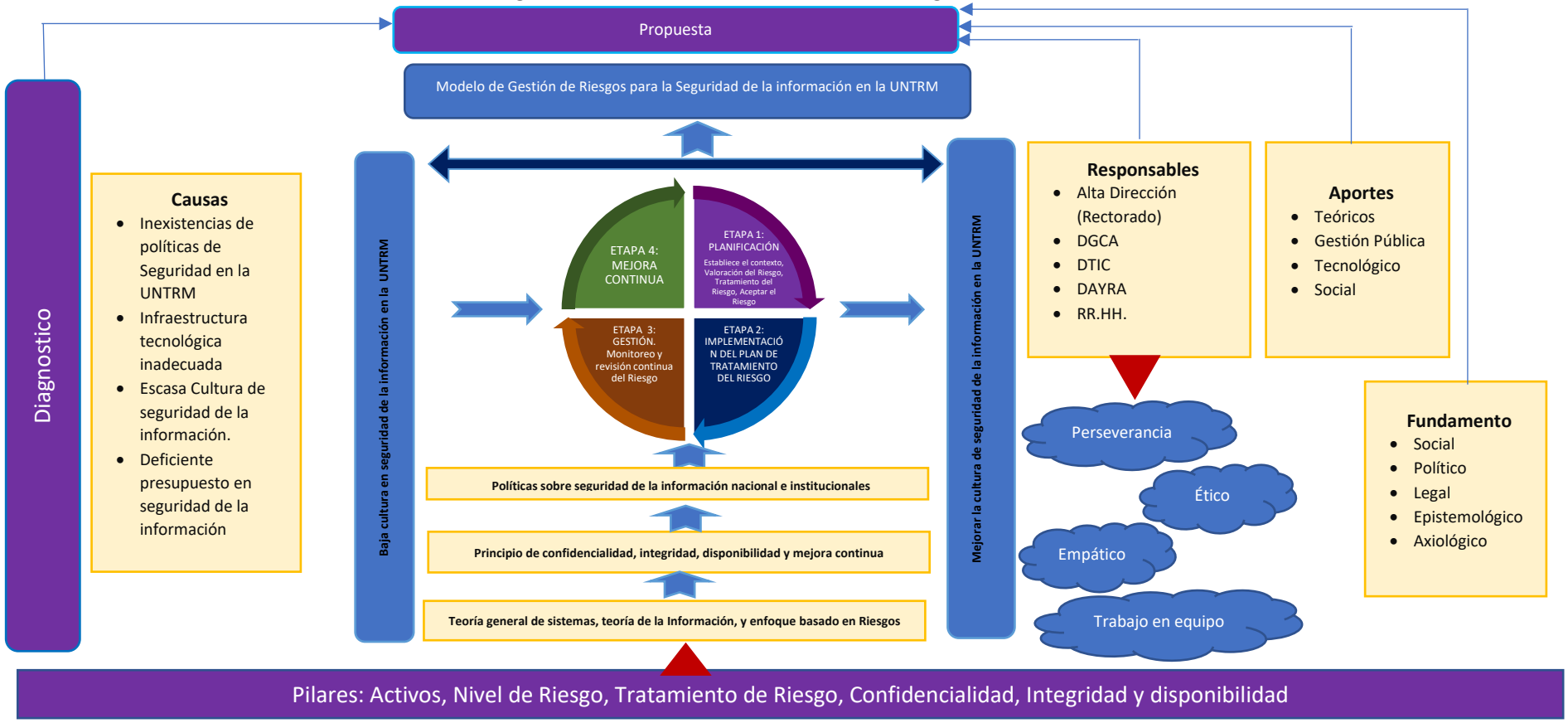
VII. RECOMENDACIONES

1. Se sugiere a la Alta Dirección de la UNTRM crear el área de Ciberseguridad articulada a la DTIC de la UNTRM. Esta área debe ser un área encargada de toda la seguridad de TI que se encargue de la gestión de los riesgos en la UNTRM, elaborando e implementado políticas de gestión de riesgos haciendo uso de herramientas tecnológicas innovadoras que contribuyan a la toma de decisiones en aspectos de gestión de riesgos, así como el Big Data y machine learning, es decir desarrollar herramientas que brinden información de carácter predictivo.
2. Se sugiere a los involucrados de la UNTRM empoderar e institucionalizar el Risk Management Model con la finalidad de poner en práctica los principios y los lineamientos estratégicos y fomentar la cultura en gestión de riesgos en la UNTRM.
3. Se sugiere que se desarrollen y apliquen políticas de seguridad de la información, ya que esto representa una base de seguridad. También se recomienda realizar un programa de capacitación a los trabajadores en temas de seguridad de la información y finalmente existe la necesidad de reestructurar las redes informáticas mediante la aplicación de tecnologías de prevención y detección de intrusos
4. Se recomienda al vicerrectorado académico y administrativo en tener en cuenta una herramienta que nos brinda los principios, marco y proceso para una adecuada gestión de riesgos, en la cual ayude a lograr sus metas, mejorar la identificación de oportunidades, amenazas, distribución y uso de recursos para la Risk management..

VIII. PROPUESTA

Propuesta: Modelo de gestión de riesgos para la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza, Chachapoyas

Figura 1. Modelo de Gestión de Riesgos



Fuente: Ñañez, 0. (2021). Investigador. Representación del Modelo teórico.

Descripción del Modelo

El modelo propuesto sobre Risk management para la security of the information en la UNTRM, se basado en la norma ISO/IEC 31000, la ISO/IEC 27005, y la NTP-ISO/IEC 27005:2018, respaldadas en la Teoría General de sistemas, Teoria de la información, el enfoque basado en Riesgos de TI, teniendo como pilares las dimensiones de la investigación, para la adecuada gestión del riesgo de la security of the information en la UNTRM.

Así mismo la propuesta parte de un diagnóstico de la UNTRM, teniendo en cuenta la causas, los responsables de la alta dirección, responsables de las áreas (DGCA, DTIC, DAYRA Y RR.HH.) de la UNTRM, los cuales deben cultiva los valores de la perseverancia, la ética, la empatía y algo muy fundamental el trabajo en equipo, ya que esta nos va permitir lograr implantar la cultura en seguridad de la información en la UNTRM, del mismo modo el modelo brindará aportes teóricos, aportes en gestión Pública, tecnológico y social, el cual tiene un fundamento social, político, legal, epistemológico y axiológico.

Por otro lado el modelo contempla 4 etapas: Planificación, implementación, gestión y mejora continua.

La etapa de planificación se constituye estableciendo el contexto que tiene que ver con la determinación y definición de los objetivos de la universidad, considerando que la Risk management debe poder integrarse en el contexto interno (cultura organizacional, recursos de la organización, procesos y objetivos organizacionales) y externo. (aspectos sociales, políticos y económicos, legislativos, entre otros) de la universidad. Asimismo, en esta etapa se considera la fase de valoración de riesgos en la cual se debe identificar, describir cuantitativa o cualitativamente y priorizar en relación a los criterios y objetivos de evaluación de riesgos notables para la universidad, esta contiene la fase de análisis la misma que está conformada por la identificación del Risk y la estimación del Risk, en la valoración del Risk de Security of the information se deberán identificar los activos de información primarios (Procesos o subprocesos, información, acciones y procesos de negocio) y de soporte (hardware, software, redes, personal, sitio y estructura organizativa) por proceso de evaluación. La estimación del riesgo tiene como objetivo determinar la probabilidad de los Risks y el impacto de sus consecuencias, clasificarlos y evaluarlos para obtener información y determinar el nivel de Risk, su priorización

y estrategia de tratamiento. La valoración de riesgo de la información es cualitativa y genera una comparación entre el análisis de la probabilidad de ocurrencia del riesgo contra sus efectos. En el tratamiento de los Security risks, el director del SGSI y su equipo de trabajo presentarán un plan anual del tratamiento de los Risks de seguridad de la información identificados.

La etapa de implementación del Plan de Tratamiento de Riesgos, en esta etapa se define el manejo de riesgos, especificando qué medidas se implementarán y quién es el responsable de esta implementación; Aquí se debe indicar claramente cada acción, fase y procedimiento que se va a realizar para ser monitoreados y hacer un seguimiento de su ejecución.

La etapa de gestión concierne al monitoreo continuo y revisión de riesgos, esta etapa consiste en revisar periódicamente el valor de los activos, impacto, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que requieren la evaluación iterativa de riesgos de security of the information. Este monitoreo es importante ya que los riesgos son tan dinámicos como la propia universidad y pueden cambiar radicalmente sin previo aviso. En esta etapa, se deben definir cronogramas de monitoreo y medición del SGRSI que ayude a contextualizar la toma de decisiones oportuna.

Finalmente, la etapa de mejora continua, consiste en mantener y mejorar el proceso de la Risk management en la security of the information, que se logra revisando periódicamente el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios.

Fundamentación:

El propósito de este modelo es crear una cultura de prevención contra los Risks que pueden estar expuestos los activos de información de la UNTRM en el día a día, con base en un enfoque de la Risk management, se intenta implementar una táctica que permite diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afecten a los activos de información e implementar contramedidas en el Management system de TI para reducir la probabilidad de que ocurran.

El sustento epistemológico se basa en la construcción de conocimientos referidos a la cultura que deben tener los trabajadores de la UNTRM referente a la security of the information, el actuar que deben tener los trabajadores frente a

los activos de información que estos manejen, y manejar las técnicas adecuadas para mitigar los riesgos de security of the information.

En referencia al marco normativo, el MGRSI presenta como base jurídica las siguientes leyes, políticas, normas y decretos: Ley N° 27658 (Ley Marco de Modernización de la Gestión del Estado) Ley N° 29733 (Ley de Protección de Datos Personales), Decreto legislativo N° 1412, que aprueba la Ley de gobierno digital, La Política Nacional de Ciberseguridad, Política de la seguridad de la información del MINEDU, NTP-ISO/IEC 27005:2018 (Gestión de riesgos de seguridad de la información), NTP-ISO/IEC 17799-2007 (Tecnología de la información), Norma ISO/IEC 31000 y la Norma ISO/IEC 27005.

REFERENCIAS

Aladro Vico, E. (2011). La Teoría de la Información ante las nuevas tecnologías de la comunicación. *CIC: Cuadernos de Información y Comunicación*, *16*, 83–93. http://dialnet.unirioja.es/servlet/articulo?codigo=3746797&info=resumen&idioma=SPA

Altamirano Yupanqui, J. R., & Bayona Oré, S. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *RISTI - Revista Iberica de Sistemas e Tecnologias de Información*, *25*, 112–134. https://doi.org/10.17013/risti.25.112-134

Ambrústolo, M. B., Di Lorio, A. H., Migueles, M., Trigo, S., Berardi, M. B., & Greco, F. (2020). *Enfoque basado en riesgos aplicado a un Laboratorio de Informática Forense Enfoque basado en riesgos aplicado a un Laboratorio de Informática Forense*. *November*, 1–12.

Anchundia-Betancourt, C. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de Las Ciencias*, *3*, 200–217. https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.200-217

Cabezas Mejía, E. D., Andrade Naranjo, D., & Torres Santamaía, J. (2018). *Introducción a la metodología de la investigación científica*.

Casares San José-Martí, I., & Lizarzaburú Bolaños, E. R. (2016). *Introducción a la Gestión Integral de Riesgo Enpresarial Enfoque:ISO 31000* (Primera ed). https://fundacioninade.org/sites/inade.org/files/web_libro_3_la_gestion_integral_de_riesgos_empresariales.pdf

Casas Anguita, J., Repullo Labrador, J. R., & Donado Campos, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Atencion Primaria*, *31*(8), 527–538. https://doi.org/10.1157/13047738

Celi Arévalo, E. K., & Diaz Plaza, R. J. A. (2017). *Políticas de Seguridad de la información en función del comportamiento de los usuarios de tecnologías de la Información en el sector microfinanciero de Lambayeque* [Universidad Nacional Pedro Ruiz Gallo]. http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/1365/BC-TES-

TMP-201.pdf?sequence=1&isAllowed=y

ComexPerú. (2020). La Ciberseguridad en el Perú:Reto para la transformación Digital. In *Agosto 07, 2020*. https://www.comexperu.org.pe/articulo/la-ciberseguridad-en-el-peru-reto-para-la-transformacion-digital

Correa Henao, G. J., Rios González, E. M., & Acevedo Moreno, J. C. (2017). Evolución de la cultura de la gestión de riesgos en el entorno empresarial colombiano. *ENGINEERING AND TECHNOLOGY*, *6*, 22–45. https://doi.org/10.22507//jet.v6n1a2

Departamento Administrativo de la Función Pública. (2018). *Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital* (pp. 1–94). http://www.funcionpublica.gov.co/documents/418548/34150781/Guía+para+la+administración+del+riesgo+y+el+diseño+de+controles+en+entidades+públicas+-+Riesgos+de+gestión%2C+corrupción+y+seguridad+digital+-+Versión+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f

Don Welch. (2019). *Creating a Cybersecurity Strategy for Higher Education*. 20 Mayo 2019. https://er.educause.edu/articles/2019/5/creating-a-cybersecurity-strategy-for-higher-education

Education Cybersecurity Report 2018. (2018). *2018 Education Cybersecurity Report*. https://securityscorecard.com/resources/2018-education-report

Figueroa Suárez, J. A., Rodríguez Andrade, R. F., Bone Obando, C. C., & Saltos Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. *Polo Del Conocimiento*, *2*, 145–155. https://doi.org/10.23857/pc.v2i12.420

García, V. (2019). ¿Cómo está avanzando la ciberseguridad en el Perú? Breve aproximación al Marco Normativo. *Actualidad Jurídica Uría Menéndez*, *52*, 176–179. https://www.uria.com/documentos/publicaciones/6687/documento/foro-latam14.pdf?id=8972

Guía para la Gestión de Riesgos de Seguridad de la Información, 1 (2020) (testimony of Gobierno Electrónico). https://www.mendeley.com/reference-manager/reader/10dff920-0ab2-361e-8320-02c309d26dfa/6b3d4593-a604-9ec1-368d-4d38dce780f3

González, M., Guzmán, A., & Trujillo, M. A. (2015). Gestión de riesgos. Una guía

de aproximación para el empresario. In *INCIBE* (pp. 1–22). https://doi.org/10.2307/j.ctv180h6pk.9

Gutiérrez, Y. E., & Sánchez Ortiz, A. (2018). Diseño de un Modelo de Gestión de Riesgos basado en ISO 31.000:2012 para los Procesos de Docencia de Pregrado en una Universidad Chilena. *Formación Universitaria*, *11*(4), 15–32. https://doi.org/10.4067/s0718-50062018000400015

Hernández Díaz, N., Yelandy Leyva, M., & Cuza García, B. (2013). Modelos causales para la Gestión de Riesgos. *Revista Cubana de Ciencias Informáticas*, *7*(4), 58–74.

ISO. (2018). ISO 31000:2018 - Risk management. In *Documento de consulta* (pp. 1–18). https://www.iso.org/obp/ui/es/#iso:std:iso:31000:ed-2:v1:en

Lizarzaburu Bolaños, E. R., Barriga, G., Burneo, K., & Noriega, E. (2019). Gestión Integral de Riesgos y Antisoborno : Un enfoque operacional desde la perspectiva iso 31000 e iso 37001. *Universidad y Empresa*, *21*(36), 79–118. https://doi.org/http://dx.doi.org/10.12804/revistas.urosario.edu.co/empresa/a.6089 *

Martínez, M., & March, T. (2015). Caracterización de la validez y confiabilidad en el constructo metodológico de la inestigación social. *Revista de Humanidades, Educací´ón y Comunicación Social*, *53*(9), 107–127.

Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R., & Sánchez Zequeira, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, *10*, 14–26. http://scielo.sld.cu/scielo.php?pid=S2227-18992016000200002&script=sci_arttext&tlng=en

Müggenburg, M. C., & Pérez, I. (2007). Tipos de estudio en el enfoque de investigación cuantitativa. *Revista Enfermería Universitaria ENEO-UNAM*, *4*(1), 35–38. http://www.redalyc.org/pdf/3587/358741821004.pdf

D.S-N-050-2018-PCM. Aprueba la Definición de Seguridad Digital en el Ámbito Naconal, 3 (2018). https://cdn.www.gob.pe/uploads/document/file/155527/D.S-N_-050-2018-PCM.pdf

D.L. N° 1412, que aprueba la Ley de Gobierno Digital, 4 (2018). https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-

que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf

Ramírez Castro, A., & Ortíz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios and ISO 27005 , and its contribution to business operation continuity. *Ingeniería*, *16*(2), 56–66. https://dialnet.unirioja.es/servlet/articulo?codigo=4797252

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

Sanca Tinta, D. M. (2011). *Revista de Actualización Clínica*. *09*.

Solano Cárdenas, L. J., Martínez Ardila, H., & Becerra Ardila, L. E. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El Profesional de La Información*, *25*(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Tamayo Alzate, A. (1999). Metodología Teoría General de Sistemas. *Revista Del Departamento de Ciencias*, *8*, 84–89. http://www.bdigital.unal.edu.co/57900/1/teoriageneraldesistemas.pdf

NTP-ISO/IEC 27005:2018, (2018). https://es.scribd.com/document/433791085/28431-NTP-ISO-IEC-27005

Tellez Carvajal, E. (2018). TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS. *IUS Et. Scientia*, *4*, 19–39.

Toledo Diaz de Leon, N. (2015). Universidad autònoma del estado de mèxico. In *Poblacion y Muestra* (pp. 1–34).

Valencia, F. J., Marulanda, C. E., & López Trujillo, M. (2016). Gobierno y Gestión de Riesgos de Tecnologías de Información y aspectos diferenciadores con el Riesgo Organizacional. *Revista Gerencia Tecnológica Informática*, *15*(November), 65–77. https://www.researchgate.net/publication/311206737_Gobierno_y_gestion_de_riesgos_de_tecnologias_de_informacion_y_aspectos_diferenciadores_con_el_riesgo_organizacional

Villavicencio Caparó, E., Ruiz García, V., & Cabrera Duffaut, A. (2018). Validación De Cuestionarios. *Odontología Activa Revista Científica*, *1*(3),

71–76. https://doi.org/10.31984/oactiva.v1i3.200

Zevallos Morales, M. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista Peruana de Computación y Sistemas*, *2*(1), 43–60.

ANEXOS

Anexo 01. Matriz de operacionalización de variables

Variable	Definición (conceptual y operacional)	Dimensiones	Indicador	Escala de medición
Modelo de gestión de riesgos	**Definición conceptual** Según Valencia et al., (2016) la gestión de Riesgos es: "[…] Un método sistemático mediante el cual los riesgos asociados a una actividad, función o proceso pueden ser planificados, identificados, analizados, evaluados, manejados y monitoreados para que la organización pueda reducir pérdidas y aumentar sus oportunidades, en este caso las Actividades, funciones, procesos y recursos que forman parte de las TIC". **Definición Operacional** Instrumento de gestión teórico-práctico orientado a identificar, evaluar y minimizar todos los posibles riesgos informáticos asociados a las actividades, operaciones y activos de la universidad, permitiendo así a la universidad definir y ejecutar estrategias que prevengan y reduzcan riesgos para garantizar la continuidad del negocio.	Activos	Nivel de efectividad para identificar activos críticos	Guía de observación (Malo, regular y bueno)
			Nivel de efectividad para priorizar activos	
		Escenario de riesgo	Número de amenazas identificadas y valoradas	
			Número de vulnerabilidades identificadas y valoradas	
		Nivel de riesgo	Efectividad para la valoración de impactos	
			Efectividad para la valoración de ocurrencia	
		Tratamiento del riesgo	Número de controles necesarios para la mitigación de riesgos no tolerables	
Seguridad de la Información	**Definición conceptual** **Según** Figueroa Suárez et al., (2017) seguridad de la información es aquella: "[…] Que tiene como objetivo proteger los activos de información independientemente de su forma o	Confidencialidad	Cantidad de Presupuesto en Ciberseguridad	**Escala ordinal**
			Porcentaje de gasto en TI para proteger los activos informáticos	
			Selección Personal especializado	
			Políticas de seguridad	
			Número de capacitación sobre seguridad	
			Número de capacitaciones sobre clasificación de activos de información	

Variable	Definición (conceptual y operacional)	Dimensiones	Indicador	Escala de medición
	estado, utilizando metodologías, estándares, técnicas, herramientas, estructuras organizativas, tecnologías y otros elementos, para el Aplicación y gestión de las medidas de seguridad adecuadas en cada caso. Por tanto, cubre la seguridad informática " . **Definición operacional** Es un conjunto de medidas anticipadas y reactivas que protegen y salvaguardar la información sobre el patrimonio de la universidad, es decir, son las políticas de uso y medidas que alteran el tratamiento de los datos utilizados en la universidad.		Nivel de resguardo de información en medios seguros	**Cuestionario** Nunca (1) Casi Nunca (2) A Veces (3) Casi Siempre (4) Siempre (5).
			Permisos de acceso a información que comparte	
			Complejidad del uso de contraseñas	
			Conducta inapropiada de los empleados respecto a la seguridad de la información	
			Cantidad de herramientas eficientes en la detección de intrusos	
			Número de pruebas en redes informáticas	
			Acceso restringido al área de TIC	
		Integridad	Bloqueo de sesión de usuario	
			Frecuencia de cambios de contraseñas	
			Información física resguardada	
			Frecuencia de actualización de antivirus	
			Medidas de contingencia	
			Frecuencia de Mantenimiento de equipo	
			Número de capacitaciones sobre ataques informáticos	
			Problemas con software malicioso	
			Nivel educación sobre seguridad de la información	
		Disponibilidad	Nivel de Seguridad en las contraseñas del o sistema que maneja	
			Tiempo en obtener la información requerida	
			Velocidad de los sistemas	
			Recuperación de sistemas ante incidencias	
			Copias de seguridad de la información	
			Porcentaje de Acceso a la información	
			Tiempo de indisponibilidad de los sistemas	
			Nivel de conocimiento de los procedimientos ante fallas o amenazas.	

Anexo 02.

UNIVERSIDAD CÉSAR VALLEJO

DOCTORADO EN GESTIÓN PÚBLICA Y GOBERNABILIDAD

CUESTIONARIO PARA RECOGER INFORMACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRIGUEZ DE MENDOZA DE AMAZONAS

Objetivo*:* Este cuestionario tiene por finalidad recoger información sobre la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, teniendo en cuenta a las personas que trabajan en las áreas administrativas, en este sentido pido a usted su colaboración respondiendo cada ítem de manera sincera y veraz, dicha información es anónima y confidencial. Se agradece anticipadamente su colaboración.

Instrucciones: Lee comprensivamente cada uno de los enunciados y elije la opción valorativa con la que estés de acuerdo o que se aproxime más a su opinión, y coloque un aspa (X) dentro del recuadro correspondiente. El llenado tendrá los siguientes criterios de evaluación: **Nunca** (1), **Casi nunca** (2), **Algunas veces** (3), **Casi siempre** (4) y S**iempre** (5).

Ítems	**Valoración**				
	1	**2**	**3**	**4**	**5**
CONFIDENCIALIDAD	**N**	**CN**	**AV**	**CS**	**S**
1. La UNTRM invierte presupuesto en ciberseguridad.					
2. La UNTRM prioriza dentro de sus gastos en TI la protección de sus activos informáticos.					
3. La UNTRM selecciona y contrata personal especializado idóneo para el departamento de Seguridad informática.					
4. La UNTRM propone e implementa políticas de seguridad para el adecuado manejo de la información					
5. La UNTRM capacita a la comunidad universitaria sobre la política de seguridad de la información.					
6. La UNTRM capacita a los trabajadores sobre la clasificación de los activos de información y su importancia.					
7. Usted resguarda la información de la universidad en medios seguros.					
8. Los Archivos que usted comparte en carpetas cuenta con permisos de acceso solo para las personas autorizadas.					
9. Las contraseñas que usted genera para el uso de los sistemas generalmente son contraseñas complejas.					
10. La UNTRM implementa políticas y controles eficientes que determinen la conducta inapropiada que tiene un empleado, respecto a la seguridad de la información.					
11. El departamento de TI de la UNTRM, utiliza Antivirus, Firewall, AntiSpyware, Antimalware, sistemas de detección de intrusos u otra herramienta para mantener seguro la red informática de la universidad.					
12. El área de TI de la UNTRM realiza prueba de seguridad en sus redes informáticas.					
13. Existen accesos restringidos a el área de TIC de la UNTRM					
INTEGRIDAD DE DATOS	**N**	**CN**	**AV**	**CS**	**S**
14. Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de la misma.					

15. Realiza cambios periódicos de contraseña para ingresar a su equipo de cómputo.					
16. La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave.					
17. El antivirus instalado en su equipo es actualizado continuamente.					
18. Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia.					
19. Realizan periódicamente mantenimientos a su equipo de cómputo					
20. La UNTRM realiza capacitaciones sobre ataques informáticos en sus diversas modalidades.					
21. Has tenido algún problema con Malware, Virus, Gusano, Troyano, Spyware, Adware, o Ranssonware.					
22. Se evalúa el nivel de educación y conocimiento sobre seguridad de la información que tiene un trabajador de la UNTRM.					
DISPONIBILIDAD	**N**	**CN**	**AV**	**CS**	**S**
23. Para evitar olvidar la contraseña de su sistema, acostumbra copiarlo en un Post-it y lo pega en la pantalla del computador.					
24. Se encuentra disponible la información que requiere para desarrollar su trabajo.					
25. Los sistemas con los que cuenta la UNTRM son rápidos					
26. El tiempo de recuperación de un sistema ente una incidencia es rápida.					
27. Usted realiza periódicamente una copia de seguridad de la información que usted maneja.					
28. Cuenta en todo momento con acceso a la información que requiere para realizar sus labores.					
29. La página web institucional de la UNTRM se encuentra activa en todo momento.					
30. Usted conoce los procedimientos que se debe seguir en caso de detectar alguna falla o amenaza en los equipos de cómputo.					
Sub total					
Total					
Valoración					

FICHA TÉCNICA INSTRUMENTAL

1. **Nombre del instrumento:**

   Cuestionario para recoger información sobre la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas

2. **Autor original.**

   Creado por

   Mg. Oscar Ñañez Campos

3. **Objetivo instrumento.**

   Analizar y evaluar la realidad sobre la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza a través de las dimensiones: confiabilidad, integridad de los datos y disponibilidad de la información.

4. **Estructura y aplicación.**

   4.1. El cuestionario está estructurado en 30 ítems, los cuales se distribuyen de la siguiente manera: 13 ítems correspondiente a la dimensión de confidencialidad, 9 ítems a la dimensión de integridad de los datos, y 8 pertenecen a la dimensión de disponibilidad; cuyos criterios de valoración son: (1) Nunca, (2) Casi nunca, (3) Algunas veces, (4) casi siempre, (5) siempre, los mismos que tienen relación con los indicadores de la variable: Seguridad de la información.

   4.2. Los trabajadores de la universidad deben de desarrollar el cuestionario en forma individual, consignando los datos requeridos de acuerdo a las indicaciones para el desarrollo de dicho instrumento de evaluación.

   4.3. El cuestionario se aplicará en forma online a 40 trabajadores de la Universidad y oficinas relacionadas de la Universidad.

   4.4. Su aplicación tendrá como duración 20 minutos aproximadamente

5. Estructura detallada

Dimensiones	Indicadores	Ítems
Confidencialidad	Cantidad de Presupuesto en Ciberseguridad	Ítems 1
	% de gasto en TI para proteger los activos informáticos	Ítems 2
	Selección Personal especializado	Ítems 3
	Políticas de seguridad	Ítems 4
	Número de capacitación sobre seguridad	Ítems 5
	Número de capacitaciones sobre clasificación de activos de información	Ítems 6
	Nivel de resguardo de información en medios seguros	Ítems 7
	Permisos de acceso a información que comparte	Ítems 8
	Complejidad del uso de contraseñas	Ítems 9
	Conducta inapropiada de los empleados respecto a la seguridad de la información	Ítems 10
	Cantidad de herramientas eficientes en la detección de intrusos	Ítems 11
	Número de pruebas en redes informáticas	Ítems 12
	Acceso restringido al área de TIC	Ítems 13
Integridad de los datos	Bloqueo de sesión de usuario	Ítems 14
	Frecuencia de cambios de contraseñas	Ítems 15
	Información física resguardada	Ítems 16
	Frecuencia de actualización de antivirus	Ítems 17
	Medidas de contingencia	Ítems 18
	Frecuencia de Mantenimiento de equipo	Ítems 19
	Número de capacitaciones sobre ataques informáticos	Ítems 20
	Problemas con software malicioso	Ítems 21
	Nivel educación sobre seguridad de la información	Ítems 22
Disponibilidad	Nivel de Seguridad en las contraseñas del o sistema que maneja	Ítems 23
	Tiempo en obtener la información requerida	Ítems 24
	Velocidad de los sistemas	Ítems 25
	Recuperación de sistemas ante incidencias	Ítems 26
	Copias de seguridad de la información	Ítems 27
	Porcentaje de Acceso a la información	Ítems 28
	Tiempo de indisponibilidad de los sistemas	Ítems 29
	Nivel de conocimiento de los procedimientos ante fallas o amenazas.	Ítems 30

6. Escala.

6.1 Escala general.

Escala	SIGLA	Puntaje	Rango
Siempre	S	5	[130 - 150]
Casi siempre	CS	4	[104- 129)
Algunas veces	AV	3	[80 - 104)
Casi nunca	CN	2	[55 – 79)
Nunca	N	1	[30 – 54)

6.2 Escala específica.

Escala	Dimensiones		
	Confidencialidad	**Integridad**	**Disponibilidad**
Siempre	[57 - 65]	[41 - 45]	[36 - 65]
Casi siempre	[46 - 56)	[33 - 40)	[29 - 35)
Algunas veces	[35 - 45)	[25 - 32)	[22 - 28)
Casi nunca	[24- 34)	[17 - 24)	[15 - 21)
Nunca	[13 - 23)	[09 - 16)	[08 - 14)

7. Validación:

Por juicio de expertos, y a través de la estadística de fiabilidad con el Alfa de Cronbach.

Confiabilidad de instrumento

Método de análisis de fiabilidad Alfa de Cronbach

Informe de validación – Modelo Alfa de Cronbach – coeficiente de correlación de Pearson

Resumen de procesamiento de casos

		N	%
Casos	Válido	29	100,0
	Excluido[a]	0	,0
	Total	29	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,930	,927	30

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
Item01	95,28	327,064	,563	,927
Item02	95,21	326,956	,627	,926
Item03	95,55	329,970	,589	,927
Item04	95,03	333,963	,552	,928
Item05	95,97	328,892	,591	,927
Item06	96,03	326,892	,660	,926
Item07	94,14	328,337	,642	,926
Item08	94,21	328,599	,525	,928
Item09	94,24	326,833	,666	,926
Item10	95,41	318,680	,720	,925
Item11	94,59	328,608	,522	,928
Item12	95,14	323,623	,618	,926
Item13	94,79	319,599	,699	,925
Item14	94,24	332,047	,395	,930
Item15	94,72	320,278	,606	,927
Item16	94,69	319,079	,678	,925
Item17	94,55	321,685	,628	,926
Item18	95,28	322,778	,494	,929
Item19	94,76	322,690	,566	,927
Item20	96,07	330,067	,552	,927
Item21	95,69	355,293	-,141	,934
Item22	95,90	325,525	,594	,927
Item23	96,97	356,106	-,205	,934
Item24	94,28	334,707	,491	,928
Item25	94,83	337,076	,450	,929
Item26	95,14	332,123	,553	,927
Item27	94,59	320,180	,677	,926
Item28	94,24	336,833	,524	,928
Item29	93,83	339,005	,473	,928
Item30	94,66	321,877	,549	,928

Estadísticas de escala

Media	Varianza	Desviación estándar	N de elementos
98,28	351,421	18,746	30

Validación de contenido por juicio de expertos

UNIVERSIDAD CÉSAR VALLEJO

INFORME DE VALIDACIÓN DEL INSTRUMENTO

I. **TÍTULO DE LA INVESTIGACIÓN:**

Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas

II. **NOMBRE DEL INSTRUMENTO:**

Cuestionario dirigido a los docentes y administrativos para obtener información sobre la seguridad de la información en la Universidad.

III. **TESISTA:**

Mg. Oscar Ñañez Campos

IV. **DECISIÓN:**

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

I. **DECISIÓN:**

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

OBSERVACIONES: Apto para su aplicación

APROBADO: SI [X] NO [ ]

Chachapoyas, 18 de enero del 2021

Firma

Experto Dr. José Alex López Castro

DNI. 33431904

UNIVERSIDAD CÉSAR VALLEJO

INFORME DE VALIDACIÓN DEL INSTRUMENTO

I. **TÍTULO DE LA INVESTIGACIÓN:**

Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas

II. **NOMBRE DEL INSTRUMENTO:**

Cuestionario dirigido a los docentes y administrativos para obtener información sobre la seguridad de la información en la Universidad.

III. **TESISTA:**

Mg. Oscar Ñañez Campos

IV. **DECISIÓN:**

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

I. **DECISIÓN:**

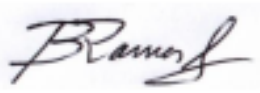
Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

OBSERVACIONES: Apto para su aplicación

APROBADO: SI [X] NO [ ]

Chachapoyas, 18 de enero del 2021

Firma



Experto

Dr. Benjamin Ramos Saavedra

D.N.I 16574376

UNIVERSIDAD CÉSAR VALLEJO

INFORME DE VALIDACIÓN DEL INSTRUMENTO

I. **TÍTULO DE LA INVESTIGACIÓN:**

Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas

II. **NOMBRE DEL INSTRUMENTO:**

Cuestionario dirigido a los docentes y administrativos para obtener información sobre la seguridad de la información en la Universidad.

III. **TESISTA:**

Mg. Oscar Ñañez Campos

IV. **DECISIÓN:**

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

I. **DECISIÓN:**

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

OBSERVACIONES: Apto para su aplicación

APROBADO: SI [X] NO [ ]

Chachapoyas, 18 de enero del 2021

Firma

Experto Dr. Luis Santiago García Merino

Anexo 03: Propuesta

Modelo de gestión de riesgos

Descripción del Modelo

El modelo propuesto sobre Risk management para la security of the information en la UNTRM, se basado en la norma ISO/IEC 31000, la ISO/IEC 27005, y la NTP-ISO/IEC 27005:2018, respaldadas en la Teoría General de sistemas, Teoria de la información, el enfoque basado en Riesgos de TI, teniendo como pilares las dimensiones de la investigación, para la adecuada gestión del riesgo de la security of the information en la UNTRM.

Así mismo la propuesta parte de un diagnóstico de la UNTRM, teniendo en cuenta la causas, los responsables de la alta dirección, responsables de las áreas (DGCA, DTIC, DAYRA Y RR.HH.) de la UNTRM, los cuales deben cultiva los valores de la perseverancia, la ética, la empatía y algo muy fundamental el trabajo en equipo, ya que esta nos va permitir lograr implantar la cultura en seguridad de la información en la UNTRM, del mismo modo el modelo brindará aportes teóricos, aportes en gestión Pública, tecnológico y social, el cual tiene un fundamento social, político, legal, epistemológico y axiológico.

Por otro lado el modelo contempla 4 etapas: Planificación, implementación, gestión y mejora continua.

La etapa de planificación se constituye estableciendo el contexto que tiene que ver con la determinación y definición de los objetivos de la universidad, considerando que la Risk management debe poder integrarse en el contexto interno (cultura organizacional, recursos de la organización, procesos y objetivos organizacionales) y externo. (aspectos sociales, políticos y económicos, legislativos, entre otros) de la universidad. Asimismo, en esta etapa se considera la fase de valoración de riesgos en la cual se debe identificar, describir cuantitativa o cualitativamente y priorizar en relación a los criterios y objetivos de evaluación de riesgos notables para la universidad, esta contiene la fase de análisis la misma que está conformada por la identificación del Risk y la estimación del Risk, en la valoración del Risk de Security of the information se deberán identificar los activos de información primarios (Procesos o subprocesos, información, acciones y procesos de negocio) y de soporte (hardware, software, redes, personal, sitio y estructura organizativa) por proceso de evaluación. La estimación del riesgo tiene como objetivo determinar la

probabilidad de los Risks y el impacto de sus consecuencias, clasificarlos y evaluarlos para obtener información y determinar el nivel de Risk, su priorización y estrategia de tratamiento. La valoración de riesgo de la información es cualitativa y genera una comparación entre el análisis de la probabilidad de ocurrencia del riesgo contra sus efectos. En el tratamiento de los Security risks, el director del SGSI y su equipo de trabajo presentarán un plan anual del tratamiento de los Risks de seguridad de la información identificados.

La etapa de implementación del Plan de Tratamiento de Riesgos, en esta etapa se define el manejo de riesgos, especificando qué medidas se implementarán y quién es el responsable de esta implementación; Aquí se debe indicar claramente cada acción, fase y procedimiento que se va a realizar para ser monitoreados y hacer un seguimiento de su ejecución.

La etapa de gestión concierne al monitoreo continuo y revisión de riesgos, esta etapa consiste en revisar periódicamente el valor de los activos, impacto, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que requieren la evaluación iterativa de riesgos de security of the information. Este monitoreo es importante ya que los riesgos son tan dinámicos como la propia universidad y pueden cambiar radicalmente sin previo aviso. En esta etapa, se deben definir cronogramas de monitoreo y medición del SGRSI que ayude a contextualizar la toma de decisiones oportuna.

Finalmente, la etapa de mejora continua, consiste en mantener y mejorar el proceso de la Risk management en la security of the information, que se logra revisando periódicamente el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios.

Fundamentación:

El propósito de este modelo es crear una cultura de prevención contra los Risks que pueden estar expuestos los activos de información de la UNTRM en el día a día, con base en un enfoque de la Risk management, se intenta implementar una táctica que permite diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afecten a los activos de información e implementar contramedidas en el Management system de TI para reducir la probabilidad de que ocurran.

El sustento epistemológico se basa en la construcción de conocimientos referidos a la cultura que deben tener los trabajadores de la UNTRM referente a la security of the information, el actuar que deben tener los trabajadores frente a los activos de información que estos manejen, y manejar las técnicas adecuadas para mitigar los riesgos de security of the information.

En referencia al marco normativo, el MGRSI presenta como base jurídica las siguientes leyes, políticas, normas y decretos: Ley N° 27658 (Ley Marco de Modernización de la Gestión del Estado) Ley N° 29733 (Ley de Protección de Datos Personales), Decreto legislativo N° 1412, que aprueba la Ley de gobierno digital, La Política Nacional de Ciberseguridad, Política de la seguridad de la información del MINEDU, NTP-ISO/IEC 27005:2018 (Gestión de riesgos de seguridad de la información), NTP-ISO/IEC 17799-2007 (Tecnología de la información), Norma ISO/IEC 31000 y la Norma ISO/IEC 27005.

I. Objetivos y principios

El modelo de gestión de riesgos para la seguridad de la información en la UNTRM ha sido desarrollado con el objetivo de proporcionar una herramienta sistémica que brinde los lineamientos necesarios para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, que permitan una adecuada toma de decisiones para reducir la probabilidad de que una amenaza se materialice o reducir la vulnerabilidad del sistema o el posible impacto en la Universidad

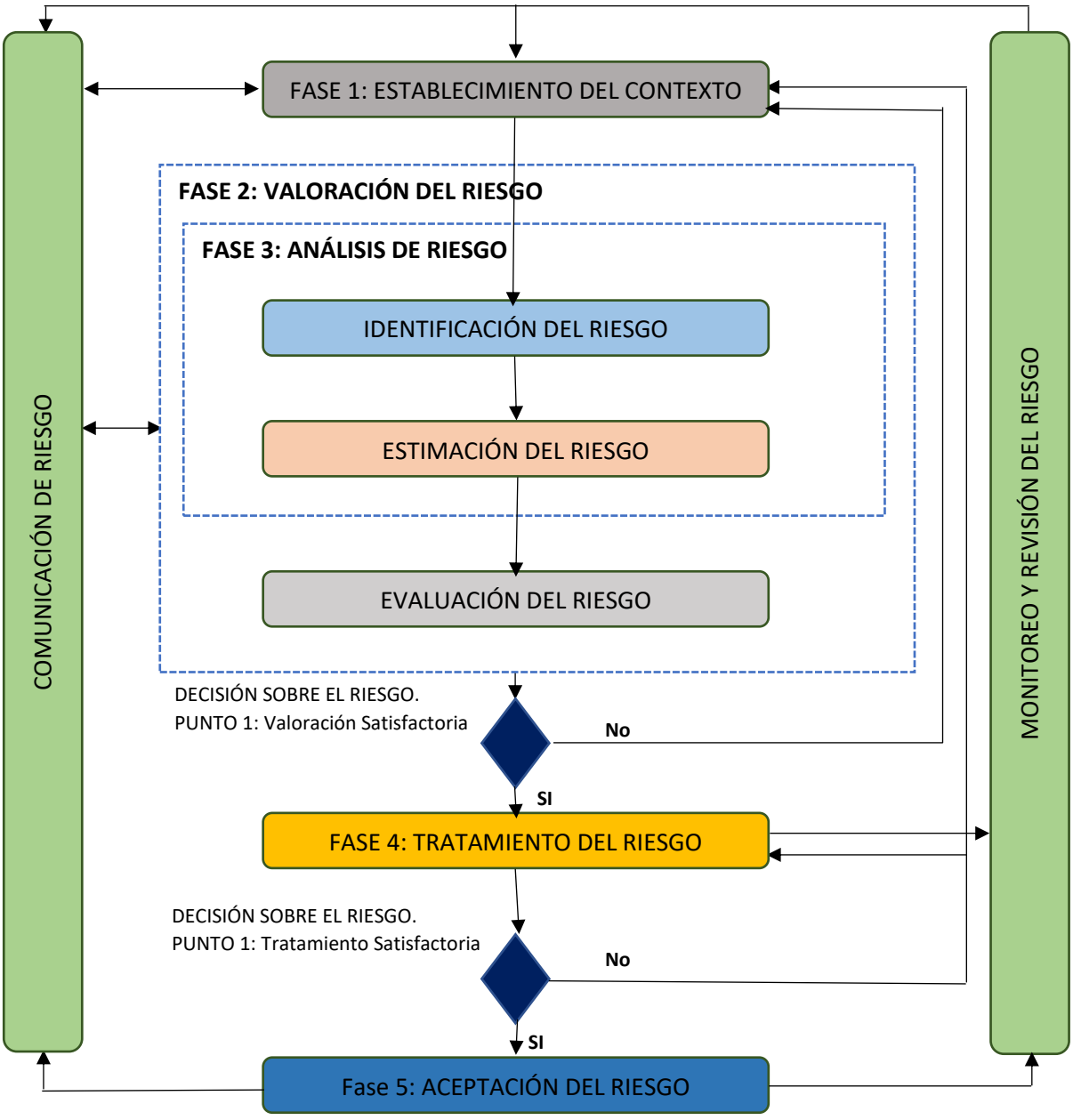
II. Alcance

El modelo de gestión de riesgos de seguridad de la información y su tratamiento se puede aplicar a cualquier proceso de la UNTRM, a través de los principios básicos y metodológicos para la gestión de riesgos de seguridad de la información, así como las técnicas, actividades y formas que permitan y faciliten el desarrollo de los pasos de reconocimiento de contexto, identificación de riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o gestión de riesgos según el área de riesgo; también incluye pautas y recomendaciones para su seguimiento y evolución.

III. Componentes del MGRSI

Etapa 1: Planificación

Figura 2: Visión del proceso de riesgo de seguridad de información



Fuente: Norma ISO/IEC 27005

En la figura 2 el proceso de gestión de riesgos para la seguridad de la información en la UNTRM, es interactivo para las actividades de valoración del riesgo y/o el tratamiento del mismo.

El contexto se establece como primera fase, aquí se determina las condiciones tanto internas (cultura, recursos, procesos y objetivos) y externas (social, económico o legislativo) que define el marco de trabajo, luego se lleva a cabo la fase de valoración del riesgo, en la que se establecen los riesgos que se van a controlar a través de la identificación, análisis y evaluación; y si esta provee información suficiente para poder determinar efectivamente qué medidas son necesarias para modificar los riesgos a un nivel aceptable entonces culmina la gestión de riesgos y continua el tratamiento del riesgo, y si este es satisfactorio, pasa a la fase de aceptación del riesgo, caso contrario regresa a establecimiento del contexto. Si la información no es suficiente, se realiza otra interacción de la valoración del riesgo teniendo en cuenta los criterios de evaluación de riesgos y los criterios de aceptación de riesgos.

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo, y el tratamiento del riesgo puede no producir inmediatamente un nivel aceptable de riesgo residual en esta situación y puede ser necesaria otra iteración de la valoración del riesgo con cambios en los parámetros de contexto.

La fase de aceptación del riesgo debe garantizar que los riesgos residuales son aceptados explícitamente por la alta dirección de la Universidad, lo cual es importante en una situación en la que la implementación de los controles se omite o se retrasa debido a los costos. En esta fase es importante detallar criterios de aceptación (criterios del negocio, aspectos legales y reglamentarios, operaciones, tecnología, finanzas, factores sociales y humanitarios) del riesgo que dependen con frecuencia de las políticas, metas, objetivos de la Universidad y de los stakeholders. Así mismo la universidad debe definir sus propias escalas para los niveles de aceptación del riesgo.

Tabla 5: Fases del proceso riesgo de seguridad de la información

Fases	Pasos
Establecimiento del contexto	1. Consideraciones Generales- levantamiento de información inicial. 2. Establecer criterios básicos para la gestión del riesgo 3. Definir el alcance y límites de la Gestión del Riesgo. 4. Establecer una organización para SGRSI
Valoración del Riesgo y Análisis del Riesgo	5. Identificar activos de información 6. Identificar las amenazas y vulnerabilidades. 7. Identificar los controles existentes. 8. Identificar consecuencias 9. Valorar las consecuencias 10. Valorar los incidentes 11. Determinar el nivel de estimación del riesgo. 12. Evaluar el riesgo
Tratamiento del Riesgo	13. Seleccionar controles
Aceptación del Riesgo	14. Aceptación del Riesgo
Comunicación del Riesgo	15. Comunicar el Riesgo
Monitoreo y Revisión del Riesgo	16. Monitorear y revisar los riesgos

Fuente: (*Guía para la Gestión de Riesgos de Seguridad de la Información*, 2020)

Tabla 6: Desarrollo de la Etapa de Planificación de PRSI

Etapa	Actividad	Meta	Entregable	Plazo	Avance
Planificación	Realizar diagnostico del estado actual del manejo de Riesgos de la información	Determinar el grado de madurez del PRSI	Documento con levantamiento de riesgos identificados en la actualidad		
	Realiza un diagnostico de riesgos de revisión y valoración de los riesgos actuales	Actualiza el formato con los riesgos actuales identificando el nivel de riesgo actual	Formato de Riesgo Actualizado		
	Establecer los periodos y actividades a desarrollar para el seguimiento de los riesgos	Elaborar documentos con directrices de control y seguimiento de riesgo	Documento con políticas de manejo de Riesgos		

Fuente: Elaboración propia

Etapa 2: Implementación

Se define el manejo de riesgos, especificando qué medidas se implementarán y quién es el responsable de esta implementación; Aquí se debe indicar claramente cada acción, fase y procedimiento que se va a realizar para ser monitoreados y hacer un seguimiento de su ejecución.

Según Norma ISO 3100:2018, menciona que las organizaciones deben de implementar el marco de referencia para la gestión del riesgo mediante un plan apropiado incluyendo plazos y recursos.

Tabla 7: Desarrollo de la fase de implementación del PRSI

Etapa	Actividad	Meta	Entregable	Plazo	Avance
Implementación	Revisión PRSI en grupo primario Riesgos de Seguridad de información (PR)	Presentación de PRSI a la DTI de la UNTRM	Documento de PRSI aprobado por la alta dirección		
	Elaboración de estrategias de control de riesgos.	Establecer cronograma de actividades y control de riesgos	Cronograma de seguimiento y control de Riesgos		
	Configurar en los equipos de seguridad las reglas de anti-span, antivirus y prevención de intrusos	Implementación de controles para la infraestructura informática	Controles establecidos y en operación		
	Llevar al formato de gestión de riesgos, todas las amenazas y vulnerabilidades que requieren control	Formato actualizado con nivel de riesgos.	Formato entregado y aprobado por la DGCA		

Fuente: Elaboración propia

Etapa 3: Gestión

En esta etapa se determina periódicamente la efectividad de las actividades realizadas utilizando diversas estrategias como: auditorias internas y externas, monitoreo de controles puntuales, medición del desempeño, reportes de gestión, etc. Los riesgos son dinámicos como la propia universidad por tanto podrán cambiar de forma o manera radical sin previo aviso, es por ello que es necesaria una supervisión continua que descubra: nuevos activos o modificaciones en el

valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos e incidentes de seguridad de la información; todo esto se consigue definiendo esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permita contextualizar una toma decisiones de manera oportuna.

Tabla 8: Desarrollo de la Etapa de Gestión del PRSI

Etapa	Actividad	Meta	Entregable	Plazo	Avance
Gestión	Revisar el comportamiento de los controles establecidos	Determinar el grado de efectividad de los controles	Documento con acción es a realizar para mejorar los controles a los riesgos		

Fuente: Elaboración propia

Etapa 4: Mejora Continua

Esta etapa consiste en mantener y mejorar el proceso de la gestión del riesgo en la seguridad de la información, esto se consigue revisando periódicamente el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios.

Etapa	Actividad	Meta	Entregable	Plazo	Avance
Mejora continua	Revisar el comportamiento de los controles establecidos	Determinar el grado de efectividad de los controles	Documento con acción es a realizar para mejorar los controles a los riesgos		

IV. Implementación metodológica

Para llevar a cabo la implementación del Modelo de Gestión de Riesgos para la Seguridad de la Información (MGRI) en la UNTRM, se toma como base la metodología de PHVA (Planear, hacer, verificar y actuar), y los lineamientos emitidos por la Presidencia del Consejo de Ministros (PCM), a través de los decretos emitidos, y las Políticas Nacionales referente a la Ciberseguridad y seguridad de la información, a partir de eso se definen las fases de implementación del MGRSI (Planear, hacer, verificar y actuar).

Tabla 9: Alineamiento del MGRSI y el Proceso de gestión del riesgo de Seguridad de la Información

Modelo Gestión Riesgos de Seguridad de la información / metodología (PHVA)	**Proceso de Gestión del Riesgo de Seguridad de la Información**
Planificación (Plan)	Establecer el contexto. Evaluar el riesgo. Desarrollar el plan de tratamiento del riesgo. Aceptar el riesgo.
Implementación (Hacer)	Implementar el plan de tratamiento del riesgo.
Gestión (Verificar)	Monitoreo y revisión continuos de los riesgos.
Mejora continua (Actuar)	Mantener y mejorar el Proceso de Gestión del Riesgo en Seguridad de la Información.

Fuente: (NTP-ISO/IEC 27005, 2009)

V. Evaluación

El sistema de evaluación de la propuesta consiste en una evaluación sistémica y holística, cuya finalidad consiste en identificar las potencialidades y limitaciones de MGRSI, de tal manera que permuta que se tomen medidas correctivas oportuna, así mismo el enfoque sistémico de evaluación tiene como objetivo mantener un cuidadoso seguimiento y control de los las distintas etapas del MGRSI, permite verificar que la funcionalidad de la propuesta logra los resultados esperados; ayuda contra inconvenientes, imprevistos e irregularidades. El mencionado modelo tiene carácter holístico porque articula e integra con cada etapa de los procesos de la propuesta, abstrae racionalmente as debilidades y fortalezas de cada una de las etapas del modelo y evalúa los impactos internos y externos que se podría ocasionar si es que no se gestionan adecuadamente los riesgos.

Validación de la propuesta

INSTRUMENTO PARA VALIDAR LA PROPUESTA POR EXPERTOS

I. DATOS GENERALES Y AUTOEVALUACIÓN DE LOS EXPERTOS

Respetado profesional: Dr. José Alex López Castro

De acuerdo a la investigación que estoy realizando, relacionada con la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas me resultará de gran utilidad toda la información que al respecto me pudiera brindar, en calidad de experto en la materia.

Objetivo: Valorar su grado de experiencia en la temática referida.

En consecuencia, solicito muy respetuosamente, responda a las siguientes interrogantes:

1. **Datos generales del experto encuestado:**
   - **1.1. Años de experiencia en gestión pública: 20 años**
   - **1.2. Cargo que ha ocupado:** Docente Tiempo completo del IESPP "Toribio Rodríguez de Mendoza"
   - **1.3. Institución Educativa donde labora actualmente:** IESPP "Toribio Rodríguez de Mendoza"
   - **1.4. Especialidad:** Licenciado en educación
   - **1.5. Grado académico alcanzado: Doctor en Gestión Pública y Gobernabilidad**

2. **Test de autoevaluación del experto:**

   2.1 Señale su nivel de dominio acerca de la esfera sobre la cual se consultará, marcando con una cruz o aspa sobre la siguiente escala (Dominio mínimo = 1 y dominio máximo= 10)

1	2	3	4	5	6	7	8	9	10

   2.2 Evalué la influencia de las siguientes fuentes de argumentación en los criterios valorativos aportados por usted:

Fuentes de argumentación	Grado de influencia en las fuentes de argumentación		
	Alto	Medio	Bajo
Análisis teóricos realizados por Ud.	x		
Su propia experiencia.	x		
Trabajos de autores nacionales.	x		
Trabajos de autores extranjeros.	x		
Conocimiento del estado del problema en su trabajo propio.	x		
Su intuición.	x		

II. EVALUACIÓN DE LA PROPUESTA POR LOS EXPERTO

Nombres y apellidos del experto	Dr. José Alex López Castro

Se ha elaborado un instrumento para que se evalúe el Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza -Chachapoyas

Por las particularidades del indicado Trabajo de Investigación es necesario someter a su valoración, en calidad de experto; aspectos relacionados con la variable de estudio: Modelo de gestión de riesgos.

Mucho le agradeceré se sirva otorgar según su opinión, una categoría a cada ítem que aparece a continuación, marcando con una **X** en la columna correspondiente. Las categorías son:

Muy adecuado (MA)
Bastante adecuado (BA)
Adecuado (A)
Poco adecuado (PA)
Inadecuado (I)

Si Ud. considera necesario hacer algunas recomendaciones o incluir otros aspectos a evaluar, le agradezco sobremanera.

2.1. ASPECTOS GENERALES:

N°	Aspectos a evaluar	MA	BA	A	PA	I
1	Nombre del Modelo.	x				
2	Representación gráfica del Modelo.	x				
3	Secciones que comprende.	x				
4	Nombre de estas secciones.	x				
5	Elementos componentes de cada una de sus secciones.	x				
6	Relaciones de jerarquización de cada una de sus secciones.	x				
7	Interrelaciones entre los componentes estructurales de estudio.	x				

2.2. CONTENIDO

N°	Aspecto a evaluar	MA	BA	A	PA	I
1	Nombre del Modelo.					
2	Las estrategias están bien elaboradas para el modelo.	x				
3	Programaciones de capacitación con profesionales.	x				
4	Coherencia entre el título y la propuesta de modelo	x				
5	Existe relación entre las estrategias programadas y el tema.	x				
6	Guarda relación el Modelo con el objetivo general.	x				
7	El objetivo general guarda relación con los objetivos específicos.	x				
8	Relaciones de los objetivos específicos con las actividades a trabajar.	x				
9	Las estrategias guardan relación con el modelo.	x				
10	El organigrama estructural guarda relación con el modelo.	x				
11	Los principios guardan relación con el objetivo.	x				
12	El tema tiene relación con la propuesta del Modelo.	x				
13	La fundamentación tiene sustento para la propuesta de modelo.	x				

N°	Aspecto a evaluar	MA	BA	A	PA	I
14	El modelo contiene viabilidad en su estructura	x				
15	El monitoreo y la evaluación del modelo son adecuados	x				
16	Los contenidos del modelo tienen impacto académico y social.	x				
17	La propuesta tiene sostenibilidad en el tiempo y en el espacio	x				
18	La propuesta está insertada en la investigación.	x				
19	La propuesta del modelo cumple con los requisitos.	x				
20	La propuesta del modelo contiene fundamentos teóricos	x				

2.3. VALORACIÓN INTEGRAL DE LA PROPUESTA

N	Aspectos a evaluar	MA	BA	A	PA	I
1	Pertinencia.	x				
2	Actualidad: La propuesta del modelo tiene relación con el conocimiento científico del tema de investigación.	x				
3	Congruencia interna de los diversos elementos propios del estudio de investigación.	x				
4	El aporte de validación de la propuesta favorecerá el propósito de la tesis para su aplicación.	x				

Lugar y fecha: Chiclayo, 05/07/2021

Firma del experto
DNI N°: 33431904

Agradezco su gratitud por sus valiosas consideraciones:

Nombres: Dr. José Alex López Castro

Dirección electrónica: jose.lopez@untrm.edu.pe

Teléfono: 915153814

Gracias por su valiosa colaboración.

INSTRUMENTO PARA VALIDAR LA PROPUESTA POR EXPERTOS

I. DATOS GENERALES Y AUTOEVALUACIÓN DE LOS EXPERTOS

Respetado profesional: Dr. Luis Santiago García Merino

De acuerdo a la investigación que estoy realizando, relacionada con la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas me resultará de gran utilidad toda la información que al respecto me pudiera brindar, en calidad de experto en la materia.

Objetivo: Valorar su grado de experiencia en la temática referida.

En consecuencia, solicito muy respetuosamente, responda a las siguientes interrogantes:

1. **Datos generales del experto encuestado:**
   - **1.1. Años de experiencia en gestión pública: 15 años**
   - **1.2. Cargo que ha ocupado:** Docentes Universitario, PDTE CONSEJO DIRECTIVO IITEGC
   - **1.3. Institución Educativa donde labora actualmente:** Universidad Alas Peruana
   - **1.4. Especialidad:** Ingeniero Informático y Sistemas
   - **1.5. Grado académico alcanzado:** Doctor en Ciencias de la Computación y Sistemas

2. **Test de autoevaluación del experto:**

   2.1 Señale su nivel de dominio acerca de la esfera sobre la cual se consultará, marcando con una cruz o aspa sobre la siguiente escala (Dominio mínimo = 1 y dominio máximo= 10)

1	2	3	4	5	6	7	8	9	10

   2.2 Evalué la influencia de las siguientes fuentes de argumentación en los criterios valorativos aportados por usted:

Fuentes de argumentación	Grado de influencia en las fuentes de argumentación		
	Alto	Medio	Bajo
Análisis teóricos realizados por Ud.	x		
Su propia experiencia.	x		
Trabajos de autores nacionales.	x		
Trabajos de autores extranjeros.	x		
Conocimiento del estado del problema en su trabajo propio.	x		
Su intuición.	x		

II. EVALUACIÓN DE LA PROPUESTA POR LOS EXPERTO

Nombres y apellidos del experto	Dr. Luis Santiago García Merino

Se ha elaborado un instrumento para que se evalúe el Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza -Chachapoyas

Por las particularidades del indicado Trabajo de Investigación es necesario someter a su valoración, en calidad de experto; aspectos relacionados con la variable de estudio: Modelo de gestión de riesgos.

Mucho le agradeceré se sirva otorgar según su opinión, una categoría a cada ítem que aparece a continuación, marcando con una **X** en la columna correspondiente. Las categorías son:

Muy adecuado (MA)
Bastante adecuado (BA)
Adecuado (A)
Poco adecuado (PA)
Inadecuado (I)

Si Ud. considera necesario hacer algunas recomendaciones o incluir otros aspectos a evaluar, le agradezco sobremanera.

2.1. ASPECTOS GENERALES:

N°	Aspectos a evaluar	MA	BA	A	PA	I
1	Nombre del Modelo.	x				
2	Representación gráfica del Modelo.	x				
3	Secciones que comprende.	x				
4	Nombre de estas secciones.	x				
5	Elementos componentes de cada una de sus secciones.	x				
6	Relaciones de jerarquización de cada una de sus secciones.	x				
7	Interrelaciones entre los componentes estructurales de estudio.	x				

2.2. CONTENIDO

N°	Aspecto a evaluar	MA	BA	A	PA	I
1	Nombre del Modelo.					
2	Las estrategias están bien elaboradas para el modelo.	x				
3	Programaciones de capacitación con profesionales.	x				
4	Coherencia entre el título y la propuesta de modelo	x				
5	Existe relación entre las estrategias programadas y el tema.	x				
6	Guarda relación el Modelo con el objetivo general.	x				
7	El objetivo general guarda relación con los objetivos específicos.	x				
8	Relaciones de los objetivos específicos con las actividades a trabajar.	x				
9	Las estrategias guardan relación con el modelo.	x				
10	El organigrama estructural guarda relación con el modelo.	x				
11	Los principios guardan relación con el objetivo.	x				
12	El tema tiene relación con la propuesta del Modelo.	x				
13	La fundamentación tiene sustento para la propuesta de modelo	x				

N°	Aspecto a evaluar	MA	BA	A	PA	I
14	El modelo contiene viabilidad en su estructura	x				
15	El monitoreo y la evaluación del modelo son adecuados	x				
16	Los contenidos del modelo tienen impacto académico y social.	x				
17	La propuesta tiene sostenibilidad en el tiempo y en el espacio	x				
18	La propuesta está insertada en la Investigación.	x				
19	La propuesta del modelo cumple con los requisitos.	x				
20	La propuesta del modelo contiene fundamentos teóricos	x				

2.3. VALORACIÓN INTEGRAL DE LA PROPUESTA

N	Aspectos a evaluar	MA	BA	A	PA	I
1	Pertinencia.	x				
2	Actualidad: La propuesta del modelo tiene relación con el conocimiento científico del tema de Investigación.	x				
3	Congruencia interna de los diversos elementos propios del estudio de Investigación.	x				
4	El aporte de validación de la propuesta favorecerá el propósito de la tesis para su aplicación.	x				

Lugar y fecha: Chiclayo, 05/07/2021

Firma del experto

Agradezco su gratitud por sus valiosas consideraciones:

Nombres: Dr. Luis Santiago García Merino

Dirección electrónica: itcaperu@gmail.com

Teléfono: 947049345

Gracias por su valiosa colaboración.

INSTRUMENTO PARA VALIDAR LA PROPUESTA POR EXPERTOS

I. DATOS GENERALES Y AUTOEVALUACIÓN DE LOS EXPERTOS

Respetado profesional: Dr. Benjamín Ramos Saavedra

De acuerdo a la investigación que estoy realizando, relacionada con la seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas me resultará de gran utilidad toda la información que al respecto me pudiera brindar, en calidad de experto en la materia.

Objetivo: Valorar su grado de experiencia en la temática referida.

En consecuencia, solicito muy respetuosamente, responda a las siguientes interrogantes:

1. **Datos generales del experto encuestado:**
   - **1.1. Años de experiencia en gestión pública: 20 años**
   - **1.2. Cargo que ha ocupado:** Docente Tiempo completo del IESPP "Toribio Rodríguez de Mendoza"
   - **1.3. Institución Educativa donde labora actualmente:** IESPP "Toribio Rodríguez de Mendoza"
   - **1.4. Especialidad:** Licenciado en educación
   - **1.5. Grado académico alcanzado: Doctor en Gestión Pública y Gobernabilidad**

2. **Test de autoevaluación del experto:**

   2.1 Señale su nivel de dominio acerca de la esfera sobre la cual se consultará, marcando con una cruz o aspa sobre la siguiente escala (Dominio mínimo = 1 y dominio máximo= 10)

1	2	3	4	5	6	7	8	9	10

   2.2 Evalué la influencia de las siguientes fuentes de argumentación en los criterios valorativos aportados por usted:

Fuentes de argumentación	Grado de influencia en las fuentes de argumentación		
	Alto	Medio	Bajo
Análisis teóricos realizados por Ud.	x		
Su propia experiencia.	x		
Trabajos de autores nacionales.	x		
Trabajos de autores extranjeros.	x		
Conocimiento del estado del problema en su trabajo propio.	x		
Su intuición.	x		

II. EVALUACIÓN DE LA PROPUESTA POR LOS EXPERTO

Nombres y apellidos del experto	Dr. Benjamin Ramos Saavedra

Se ha elaborado un instrumento para que se evalúe el Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza -Chachapoyas

Por las particularidades del indicado Trabajo de Investigación es necesario someter a su valoración, en calidad de experto; aspectos relacionados con la variable de estudio: Modelo de gestión de riesgos.

Mucho le agradeceré se sirva otorgar según su opinión, una categoría a cada ítem que aparece a continuación, marcando con una **X** en la columna correspondiente. Las categorías son:

Muy adecuado (MA)
Bastante adecuado (BA)
Adecuado (A)
Poco adecuado (PA)
Inadecuado (I)

Si Ud. considera necesario hacer algunas recomendaciones o incluir otros aspectos a evaluar, le agradezco sobremanera.

2.1. ASPECTOS GENERALES:

N°	Aspectos a evaluar	MA	BA	A	PA	I
1	Nombre del Modelo.	x				
2	Representación gráfica del Modelo.	x				
3	Secciones que comprende.	x				
4	Nombre de estas secciones.	x				
5	Elementos componentes de cada una de sus secciones.	x				
6	Relaciones de jerarquización de cada una de sus secciones.	x				
7	Interrelaciones entre los componentes estructurales de estudio.	x				

2.2. CONTENIDO

N°	Aspecto a evaluar	MA	BA	A	PA	I
1	Nombre del Modelo.					
2	Las estrategias están bien elaboradas para el modelo.	x				
3	Programaciones de capacitación con profesionales.	x				
4	Coherencia entre el título y la propuesta de modelo	x				
5	Existe relación entre las estrategias programadas y el tema.	x				
6	Guarda relación el Modelo con el objetivo general.	x				
7	El objetivo general guarda relación con los objetivos específicos.	x				
8	Relaciones de los objetivos específicos con las actividades a trabajar.	x				
9	Las estrategias guardan relación con el modelo.	x				
10	El organigrama estructural guarda relación con el modelo.	x				
11	Los principios guardan relación con el objetivo.	x				
12	El tema tiene relación con la propuesta del Modelo.	x				
13	La fundamentación tiene sustento para la propuesta de modelo.	x				

N°	Aspecto a evaluar	MA	BA	A	PA	I
14	El modelo contiene viabilidad en su estructura	x				
15	El monitoreo y la evaluación del modelo son adecuados	x				
16	Los contenidos del modelo tienen impacto académico y social.	x				
17	La propuesta tiene sostenibilidad en el tiempo y en el espacio	x				
18	La propuesta está insertada en la investigación.	x				
19	La propuesta del modelo cumple con los requisitos.	x				
20	La propuesta del modelo contiene fundamentos teóricos	x				

2.3. VALORACIÓN INTEGRAL DE LA PROPUESTA

N	Aspectos a evaluar	MA	BA	A	PA	I
1	Pertinencia.	x				
2	Actualidad: La propuesta del modelo tiene relación con el conocimiento científico del tema de Investigación.	x				
3	Congruencia interna de los diversos elementos propios del estudio de Investigación.	x				
4	El aporte de validación de la propuesta favorecerá el propósito de la tesis para su aplicación.	x				

Lugar y fecha: Chiclayo, 05/07/2021

Firma del experto
DNI N°: 16574375

Agradezco su gratitud por sus valiosas consideraciones:

Nombres: Dr. Benjamín Ramos Saavedra

Gracias por su valiosa colaboración.

Anexo 04: Constancia de autorización para aplicación de instrumentos de recolección de datos .

UNIVERSIDAD NACIONAL
TORIBIO RODRÍGUEZ DE
MENDOZA DE AMAZONAS

Rectorado

"Año del Bicentenario del Perú: 200 años de Independencia"

Chachapoyas, 24 de junio de 2021.

SEÑORES:
ESCUELA DE POSGRADO
Universidad César Vallejo – Sede Chiclayo
CHICLAYO

Mediante la presente, reciba un cordial saludo a nombre de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas y en atención a la carta s/n. de fecha 24 de mayo del 2021, comunica a usted que la Oficina de Rectorado de nuestra casa superior de estudios, **AUTORIZA** al Mg. **OSCAR ÑANEZ CAMPOS** de la escuela de Posgrado del VI ciclo del Doctorado en Gestión Pública y Gobernabilidad de la Universidad Privada Cesar Vallejo – Sede Chiclayo, para que desarrolle la aplicación de su Proyecto de Tesis denominado "Modelo Gestión de Riesgo para la Seguridad de la Información, Universidad Nacional Toribio Rodríguez de Mendoza Chachapoyas", a partir de la fecha hasta culminar su estudio estructural.

Aprovecho la oportunidad para expresarle los sentimientos de mi especial consideración y estima.

UNIVERSIDAD NACIONAL
TORIBIO RODRIGUEZ DE MENDOZA DE AMAZONAS

Polycarpio Chauca Valqui Dr.
RECTOR

Campus Universitario, Sede Administrativa, Calle Higos Urco N° 342-350-356
Teléfono 041-478581, Anexo N° 4002 Chachapoyas, Perú
Email: rectorado@untrm.edu.pe / www.untrm.edu.pe