UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

Facultad de Ingeniería

Escuela Profesional de Ingeniería de Sistemas e Informática

TESIS

"Riesgos de seguridad de la información y la calidad de servicio en la Universidad Tecnológica de los Andes, Abancay 2021"

Presentado por:

Br. PEDRO MIGUEL CHIRINOS PALOMINO

Para optar el título profesional de:

INGENIERO DE SISTEMAS E INFORMÁTICA

Abancay – Apurímac - Perú

2023

Tesis

“Riesgos de Seguridad de la Información y la Calidad de Servicio en la Universidad Tecnológica de los Andes, Abancay 2021”

Línea de Investigación:

Informática, Sociedad y Gestión de Conocimiento

Asesor:

Mg. Marleny Peralta Ascue

UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO EN LA UNIVERSIDAD TECNOLÓGICA DE LOS ANDES, ABANCAY 2021"

Presentado por el bachiller **Pedro Miguel Chirinos Palomino**, para obtener el Título Profesional de**: Ingeniero de Sistemas e informática**

Sustentado y aprobado el 02 de octubre del 2023 ante el jurado:

Presidente	: Mg. EDUARDO CHAVEZ VASQUEZ
Primer Miembro	: Mg. YULIANA M. TOMAYLLA GUTIERREZ
Segundo Miembro	: Mg. NILTON MARURI MALPARTIDA
Asesor	: Mg. MARLENY PERALTA ASCUE

Riesgos de Seguridad de la Información y la Calidad de Servicio en la Universidad Tecnológica de los Andes, Abancay 2021

INFORME DE ORIGINALIDAD

17%	17%	2%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.utea.edu.pe Fuente de Internet	5%
2	Submitted to Universidad Tecnologica de los Andes Trabajo del estudiante	3%
3	upc.aws.openrepository.com Fuente de Internet	2%
4	hdl.handle.net Fuente de Internet	1%
5	repositorio.une.edu.pe Fuente de Internet	1%
6	Submitted to Colegio San Agustín Trabajo del estudiante	1%
7	repositorio.unheval.edu.pe Fuente de Internet	1%
8	Submitted to City University of New York System	<1%

DEDICATORIA

Dedico mi Tesis a mis padres, **Braulio** y **Patricia**, quienes con su amor, paciencia y arduo trabajo me permitieron alcanzar un sueño más en mi vida, gracias por infundirme el ejemplo de trabajo y valentía.

Finalmente, me gustaría dedicar mi investigación a toda mi familia, que con sus consejos y palabras de aliento me han hecho una mejor persona y que siempre me acompañaron en las buenas y en las malas para lograr mis metas.

AGRADECIMIENTO

Gracias a mi esposa **María Jesús** y a mis dos amores, **Fernanda y Rodrigo**, por su amor y apoyo incondicional, y por estar conmigo en este proceso, eternamente agradecido.

ÍNDICE DE CONTENIDOS

CAPÍTULO IV

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

TIC: Tecnología de información y comunicación.

IA: Inteligencia artificial

IoT: Internet de las cosas.

RSI: Riesgos de seguridad de información.

CS: Calidad de servicio.

Big Data: Volumen de datos.

UTEA: Universidad Tecnológica de los Andes.

EPISI: Escuela Profesional de Ingeniería de Sistemas e Informática.

FI: Facultad de ingeniería.

OTI: Oficina de tecnología de información.

CCI: Centro de cómputo e informática.

EP: Escuelas profesionales.

SERVQUAL: Service of quality

COVID-19: Enfermedad generada por el coronavirus

GAP: Análisis de brechas seguridad.

NTP-ISO/IEC 27001:2014: Norma Técnica Peruana, técnicas de seguridad. Sistemas de gestión de seguridad de la información.

SW: Software.

HW: Hardware.

RESUMEN

En consideración a la naturaleza de los fenómenos estudiados, el objetivo general planteado fue *"Identificar el nivel de concordancia entre los riesgos de seguridad de la información y la calidad de servicio en la Universidad Tecnológica de los Andes, Abancay 2021"*.

En esa línea la investigación fue de enfoque cuantitativo, tipo básica, alcance correlacional-descriptivo y con un diseño no experimental-correlacional-transversal; contando con 3271 sujetos de población a partir de los cuales por el método probabilístico aleatorio simple e intencionado se consideró una muestra de 359 unidades de análisis, aplicando la encuesta como técnica y el cuestionario como instrumento para el logro de la información, generando resultados consistentes permitiendo la validación de la hipótesis de investigación por *r* de Pearson. Concluyendo que, los riesgos de seguridad de la información y la calidad de servicio presentan un nivel de relación significativo positivo moderado en la Primera Casa Superior de Estudios investigada, Abancay 2021, toda vez que la correlación de *r* Pearson dio 0.160** y el *p*-valor logrado de α=0.002, que es inferior al error de 5.0% (Sig. bilateral α=0.002 < 0.05), escenario señalado por los entornos físicos, técnicos y organizativas de los riesgos de seguridad de la información en la universidad se encuentran concordantes con la empatía, la confianza, los componentes tangibles, la capacidad de respuesta y seguridad de los servicios académicos-administrativos que proporcionan y perciben los usuarios discentes a lo largo de su formación profesional.

Palabras clave: Riesgos de seguridad de la información y calidad de servicio.

ABSTRACT

Considering the nature of the phenomena studied, the general objective was "Identify the level of agreement between information security risks and the quality of service at the Technological University of the Andes, Abancay 2021".

In this line, the research was of a quantitative approach, basic type, correlational-descriptive scope and with a non-experimental-correlational-transversal design; counting with 3271 population subjects from which by the simple and intentional random probabilistic method a sample of 359 units of analysis was considered, applying the survey as a technique and the questionnaire as an instrument for the achievement of information, generating consistent results allowing validation of the research hypothesis by Pearson's r. Concluding that the information security risks and the quality of service present a moderate positive significant relationship level in the First Superior House of Studies investigated, Abancay 2021, since the correlation of r Pearson gave 0.160** and the p-Achieved value of α=0.002, which is less than the error of 5.0% (Sig. bilateral α=0.002 < 0.05), a scenario indicated by the physical, technical and organizational environments of the information security risks in the university. consistent with the empathy, trust, tangible components, response capacity and security of the academic-administrative services provided and perceived by student users throughout their professional training.

Key words: Information security risks and quality of service.

INTRODUCCIÓN

Con el avance de la tecnología y sobre todo la criticidad de la información que se llegan a procesar hoy en día en las organizaciones a nivel mundial, donde las mismas están afrontando una problemática de poder evaluar el resguardo de los datos y los riesgos que puedan tener estos, tendientes a implementar, ejecutar y llevar adelante de manera efectiva y que debe formar parte de una mejora continua de la productividad organizacional (Álvarez, 2017).

Situación manifiesta, que en los últimos tiempos se puede advertir una evidente transformación y visualización de las organizaciones sobre las conceptualizaciones de asistencia y/o servicios. Toda vez que la parte significativa de la “calidad de servicio” crece de manera exponencial todos los días, de donde la calidad se encuentra desde la visualización del usuario y de acuerdo a su percepción marcará la diferencia entre sus expectativas y el servicio recibido.

En esa línea, las organizaciones de hoy en día frente a la alta dependencia de los sistemas y las TIC, sobre todo la enmarañada administración de la información intrínseca y extrínseca, de manera espontánea y constante enfrentan inconmensurables amenazas donde posiblemente manifiestan sus deficiencias vulnerables, su integración, disposición y confidencia de la información en la institución, siendo de prioridad para el incremento de la competitividad, siendo responsables para resguardar sus sistemas y tecnologías, si desean continuar brindando un servicio de calidad a sus usuarios y clientes, y llegar a implementar procesos de seguridad de los datos, los componentes necesarios y pertinentes controles en la institución educativa superior (Pacheco y Rodríguez, 2019).

En consecuencia, la investigación está sistematizada en capítulos a saber:

Capítulo I: El plan de la investigación; constituida por situación del problema latente, la respectiva visualización e identificación del problema, el planteamiento del problema general y específicos, así como la justificación del estudio, la

respectiva delimitación espacial, la temporal, social y conceptual, además de la viabilidad y limitaciones de la investigación.

Capítulo II: El marco teórico; considera los antecedentes de investigaciones previas tanto internacional, nacional y regional y/o local, seguido de las bases teóricas de cada variable, y culmina en su marco teórico conceptual.

Capítulo III: la metodología de investigación; conformada por el planteamiento de la hipótesis general e hipótesis específicas, del respectivo método utilizado en el tratamiento de datos, el tipo, alcance y su pertinente diseño del estudio, la población participante, el tamaño de la muestra y el muestreo de las unidades de análisis, las técnicas aplicadas para el logro de los datos, así como el instrumento; además de los aspectos éticos, el procedimiento estadístico, la presentación de los resultados y finalizar con el análisis e interpretación de la información alcanzada.

Capítulo IV: Resultados y discusión; se parte de los resultados alcanzados de las variables, las respectivas discusiones, así como la contrastación de la hipótesis general y específicas y al final las conclusiones, recomendaciones y los anexos que sostienen información adicional sobre la ejecución de la investigación.

CAPÍTULO I

PLAN DE INVESTIGACIÓN

1.1 Descripción de la realidad problemática

Las organizaciones actualmente viven ambientes de constante competitividad productiva, quienes que para lograr sus objetivos se encuentran encaminadas hacia la digitalización de sus procesos operacionales, donde con el uso masivo de sistemas, y tecnologías de información y comunicación (TIC), las redes e internet, la aplicación de la inteligencia artificial (IA), así como Big Data, inclusive la internet de la cosas (IoT), les permiten gestionar la información de manera oportuna pero lamentablemente se encuentran expuestas a riesgos constantes de seguridad en su infraestructura, tecnológicos, humanos y entre otros, las mismas requieren escenarios de seguridad inteligentes. (Comisión Económica para América Latina y el Caribe [CEPAL], 2021)

Con el avance de la tecnología y sobre todo la criticidad de la información que se llegan a procesar hoy en día en las organizaciones a nivel mundial, donde las mismas están afrontando una problemática de poder evaluar el resguardo de datos y sus respectivos riesgos tendiente a implementar, ejecutar y llevar adelante de

manera efectiva y que debe formar parte de una mejora continua de la productividad organizacional.

Situación manifiesta, que en los últimos tiempos se puede advertir una evidente transformación y visualización de las organizaciones sobre las conceptualizaciones de asistencia y/o servicios. Toda vez que la parte significativa de la “calidad de servicio” crece de manera exponencial todo los días, de donde la calidad se encuentra desde la visualización del usuario y de acuerdo a su percepción marcará la diferencia entre sus expectativas y el servicio recibido.

Es así que la empresas de hoy en día frente a la alta dependencia de las TIC, y la enmarañada administración de datos intrínseca y extrínseca de manera espontánea y constante que enfrentan inconmensurables amenazas ddonde posiblemente manifiestan sus deficiencias vulnerables, su integración, disposición y confidencia de la información institucional, siendo de prioridad para el incremento de la competitividad, siendo responsables para resguardar sus sistemas y tecnologías, si desean continuar brindando un servicio de calidad a sus usuarios y clientes, y llegar a implementar procesos de protección de los datos, los componentes necesarios y pertinentes controles en la organización (Pacheco & Rodríguez, 2019).

Por cuanto, es de mucha importancia analizar los riesgos posibles para que las organizaciones identifiquen las vulneraciones a los cuales se encuentra expuestos sus activos y recursos concretos y abstractos, con la intensión de valorar la revolución que generaría los servicios que proporciona. Sumado a lo manifestado es de significativa importancia realizar un análisis de los riesgo a los cuales se

encuentra expuesto la información la misma es determinante para la operatividad y desarrollo de sus servicios y del sistema de la administración del resguardo de los datos, además del impacto en los servicios que brinda la organización (Mujica y Álvarez, 2009, p. 34).

Tal es así, que ante el cambiante escenario de las sistemas tecnológicos, las organizaciones requieren tomar decisiones significativas en relación al riesgo del resguardo de datos, de que tecnología implementar y cuáles evitarlas, además del servicio de calidad que se debe proporcionar; por cuanto los procesos de controles de seguridad frágiles en los sistemas tecnológicos, tienden a generar falencias de procesamientos o de las transferencias desautorizadas (Deloitte, 2016, párr. 1).

Por cuanto el presente estudio permitió reflejar la realidad latente de los fenómenos objeto de investigación, partiendo de los respectivos análisis de los riesgos como el foco central de toda institución educativa, sobre la seguridad de los datos y la asociación con el servicio de calidad que brinda la primera Casa Superior de Estudios, Abancay 2021, permitiendo conocer y determinar el adecuado nivel de resguardo de datos, en que toda entidad visiona para proteger sus recursos tangibles e intangibles, asumiendo de manera responsable los criterios a establecer sobre la administración de los riesgos del resguardo de datos y del servicio de calidad que los proporciona en el bienestar de los usuarios discentes de la sede Abancay, filial Cusco y Andahuaylas, la misma permitirá diseñar y proporcionar estrategias metodológicas propias de análisis de riesgo, para llegar a discernir acciones base para implantar, monitorear, revisar, mejorar y controlar los

sistemas de información acorde al servicio de calidad que hoy exige la nueva educación superior en el Perú.

1.2 Identificación y formulación de problema

La ejecución del diagnóstico de la realidad problemática es sustancial, la misma permitió observar y analizar los riesgos que pueden atravesar los componentes sustanciales de los fenómenos estudiados y establecer la concordancia entre los fenómenos que se desarrolla en la entidad objeto de estudio, toda vez que identificado los riesgos y el nivel de los servicios, el impacto potencial que se está generando, toda vez que la pérdida o destrucción de los datos, deben ser controladas, siendo estas generalmente muy ineficientes en la entidad, que inciden en la frecuencia de ocurrencia, la apreciación del usuario sobre la prestación y el servicio aceptado, además de para las decisiones oportunas, eficientes y efectivas que deben realizar las autoridades universitarias.

1.2.1 Problema general

¿Cuál es el nivel de concordancia entre riesgos de seguridad de la información y la calidad de servicio en la Universidad Tecnológica de los Andes, Abancay 2021?

1.2.2 Problema específicos

pe1. ¿De qué manera se asocia los riesgos físicos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021?

Pe2. ¿De qué manera se asocia los riesgos técnicos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021?

Pe3. ¿De qué manera se asocia los riesgos organizativos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021?

1.3 Justificación de la investigación

1.3.1 Justificación social

El estudio consintió observar el ambiente natural de los riesgos para el mejoramiento de los estándares del resguardo de datos y el servicio de calidad que reciben los aprendientes en la entidad objeto de estudio, Abancay; que repercutirá de significativamente en el benefició de la sociedad estudiantil y de la cultura organizacional de la entidad en su conjunto, toda vez que las exposiciones del resguardo de datos no tiende a ser un procedimiento tedioso, a partir del cual permitió conocer, comprender y aprender los elementos y/o factores que se articulan para aplicar las medidas de protección de la información y los escenarios que repercuten en la calidad de servicio que brinda la universidad.

1.3.2 Justificación teórica

La procesos operativos de los riesgos del resguardo de los datos y calidad de servicio que se vienen ejecutando en la entidad educativa superior a lo largo del desarrollo académico de los discentes, estuvieron sostenidas en las bases teóricas existentes y los conocimientos pertinentes, las que son una necesidad y de gran importancia en la operatividad de la información y las actividades formativas académicas y administrativas de la UTEA, sede Abancay; la misma que como efecto repercute en los riesgos que deben ser considerados, relacionados al resguardo de la información basados en los escenarios físicos,

técnicos y organizacionales, así como los escenarios, estructurales y la proporcionalidad del servicio de calidad para establecer aprendizajes significativos de los aprendientes uteinos.

1.3.3 Justificación metodológica

Parte de una utilidad metodológica que brindó datos consistentes acerca la significancia y escenarios que se estuvieron presentando sobre las inseguridades del manejo de los datos, en cuanto a los insumos, materiales y especialmente del impacto que tenía sobre la organización en el servicio que proporcionaba la organización a los discentes, así como de observar las incidencias que se encontraban afectando a la seguridad de la información a partir de llegar a establecer la categoría de los sistemas tecnológicos, considerando las dimensiones de la seguridad, como físicos, técnicos y organizativos asociados a los procesos operativos del servicio de calidad en la UTEA, Abancay 2021. Donde estos escenarios permitirán identificar el grado de concordancia que existe entre las variables estudiadas y brindar escenarios de la realidad, para los administradores de los datos y del servicio, deban mejorar en su trabajo de manera eficiente y efectiva para la competitividad de la universidad.

1.3.4 Justificación práctica

Fue muy favorable desarrollar la investigación, la misma concurrió a que el talento humano de la institución educativa superior mejore el nivel de las alarmas del resguardo de datos y que la calidad del servicio sean más significativos, toda vez que la información es un activo intangible que se debe

proteger de forma adecuada en la entidad, frente a la pérdida, accidental o provocada y de accesos no autorizados, tanto externos como internos, así como en la modificación de la información, que estuvo relacionada al bienestar del servicio académico y administrativos dentro la actividad diaria que se brinda, por cuanto resulta inadmisible que personas ajenas al negocio accedan a la documentación y/o información donde muchas veces los responsables de OTI, administrativos y autoridades universitarias no lo prestan atención a los datos que son almacenados en sus equipos informáticos.

1.4 Objetivos de la investigación

1.4.1 Objetivo General

Identificar el nivel de concordancia entre los riesgos de seguridad de la información y la calidad de servicio en la UTEA, Abancay 2021.

1.4.2 Objetivos específicos

oe1. Determinar la asociación entre los riesgos físicos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021.

oe2. Identificar la asociación entre los riesgos técnicos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021.

oe3. Determinar la asociación entre los riesgos organizativos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021.

1.5 Delimitación de la investigación

1.5.1 Espacial

Se desarrolló el estudio en la UTEA, Abancay; fundamentalmente en la oficina de tecnología de información (OTI), además del centro de cómputo e

informática (CCI) y las diez (10) escuelas profesionales (EP) de la sede central de la universidad citada de manera precedente. Donde la UTEA se encuentra ubicada en la Av. Perú N° 700, del distrito y provincia de Abancay, Apurímac.

1.5.2 Temporal

La investigación se inició en septiembre de 2021 y culminó en junio de 2022.

1.5.3 Social

La misma estuvo constituida por el talento humano de OTI, el CCI y los estudiantes pertenecientes a las diez escuelas profesionales (EP) de la UTEA, de la sede Abancay.

1.5.4 Conceptual

Se partieron del análisis de los elementos y bases teóricas-científicas de los fenómenos objeto de investigación, las que permitieron observar oportunamente los escenarios de la realidad latente en cuanto al resguardo de los datos y sobre el servicio de calidad de la UTEA-Abancay, y arribar a conjeturas consistentes, determinando e identificando el nivel de concordancia entre ambos fenómenos, con la finalidad de proponer acciones de mejora continua en las decisiones oportunas consideradas para el manejo de las inseguridades en cuanto a la seguridad informática y la calidad de las atenciones que brinda la entidad educativa superior, además la información repercutirá para futuros estudios.

1.6 Viabilidad de la investigación

El desarrollo de la investigación fue exitoso, donde de manera oportuna se consideró todos los recursos necesarios, los mismos se encontraban disponibles, tales como económicos o financieros, humanos o sociales, materiales o técnicos y entre otros.

Es así que, para la viabilidad económica, se contó con el financiamiento respectivo que se invirtió en los materiales e insumos a ser necesarios hasta la concreción de la investigación.

De otra parte, presenta la viabilidad social, toda vez que se buscó satisfacer las necesidades operativas del manejo de la información al interior y exterior de la comunidad académica estudiantil universitaria, para el cual se observó el desempeño de los responsables de las respectivas unidades administrativas de la oficina de TIC y entre otras de la UTEA, en el manejo de los riesgos del resguardo de la informática y del servicio de calidad brindado.

La viabilidad técnica, se partió de la existencia de recursos concretos suficientes y necesarios como tecnológicos, materiales, insumos y de las unidades de análisis para la obtención de la información y arribar a resultados pertinentes para la determinación del objetivo de la investigación.

1.7 Limitaciones de la investigación

Existieron ciertas limitaciones, que generaron durante todo el ciclo del presente estudio, como las limitaciones en el tiempo para su desarrollo, soporte, autorización y apoyo de los administradores de OTI, autoridades universitarias y los aprendientes de la UTEA, sede Abancay; así mismo del escaso acceso a la

información a nivel local, sobre todo a nivel físico y el apoyo oportuno de los aprendientes para la ejecución de los cuestionarios por la situación social del país a efecto de la pandemia del COVID-19.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de investigación

2.1.1 A nivel internacional

Partiendo de Rodríguez y Torres (2019), en su investigación *"Análisis de riesgos de seguridad de la información del área it de la empresa royal services S.A."*. Universidad Católica de Colombia, Bogotá-Colombia; donde concluyen que se deben considerar de manera obligatoria los procesos operacionales y analizar los riesgos informáticos, toda vez que si no se tienen los conocimientos respectivos sería muy complicado afrontar posibles contingencias en el resguardo de datos, para la protección de datos y que de no sr así implicaría impactos negativos para la organización, ameritando una planificación para poner a buen recaudo los datos institucionales (p. 42).

Fajardo (2017), en su investigación: *"Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano"*. Institución Universitaria Politécnico Gran Colombiano, Bogotá-Colombia. Quién concluye que existen fisuras asociadas al diseño y manejo del software, además de las debilidades en la infraestructura tecnológica que

adquiere, procesa, envía y almacena los datos, haciendo notorio de la gran necesidad de implementar un plan para el monitoreo de riesgos interesados a borrar y/o reducir las contingencias que corren la información institucional. Toda vez que la seguridad encontrada son de criticidad “Alta” (p. 69-70).

Por su parte Calderón (2015), en la investigación *“Análisis de riesgos informáticos y desarrollo de un plan de seguridad de la información para el gobierno autónomo descentralizado municipal de Catamayo”*. Universidad Nacional de Loja, Loja-Ecuador; que concluye que los procesos de Octave, permitirá desarrollar la evaluación de inseguridades de forma precisa, debido a sus etapas precisas hacia todos las unidades de la empresa, siendo de significación que los datos no corran riesgo alguna, por qué no se prestan los cuidados adecuados en la conservación de la tecnología computacional; así mismo por qué no se llegan a establecer canales base para la disposición física y lógica por la carencia de tecnología que garanticen el resguardo de las interconexiones a los embates de los virus informáticos, tales como los troyanos, gusanos y entre otros ataques del ciberespacio (p. 108-109).

En su investigación de Vaca (2019), titulada *“Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del ecuador*”. Universidad Técnica de Ambato, Ambato-Ecuador; quién llega a la conclusión que, por intermedio del manejo de las técnicas pentesting identificó las vulnerabilidades y amenazas expuestas los componentes informáticos y la información sensible obtenida, almacenada y distribuida; manifestando que son los usuarios finales que presentan la

vulnerabilidad por el desconocimiento de la forma de comportarse en un escenario de una amenaza (p. 160).

Al final, Pilla (2019), en su estudio *"Diseño de una política de seguridad de la información para el área de tecnología de la información de la cooperativa de ahorro y crédito Chibuleo Ltda., basado en la norma ISO/IEC 27002:2013"*. Universidad Internacional SEK, Quito-Ecuador; llegando a la conclusión, que se identificaron fragilidad y la presencia de escenarios débiles del resguardo de los datos, y además reconoció controles significativos tendientes a la reducción de incidencias referentes al resguardo de datos en la institución. (p. 116).

2.1.2 Nivel nacional

Según la investigación de Maquera (2022), titulada *"Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya*". Universidad Privada de Tacna, Tacna-Perú; donde concluye que, de acuerdo a la prueba de Pearson cuyo valor 0,540, siendo p=0,000); determinando el sistema de administración del resguardo de datos presenta una influencia directa y significativa con la calidad de servicio en la entidad municipal (p. 70).

Por su parte Mendez (2021), en el estudio *"Diseño de un sistema de gestión de seguridad de información para proteger los activos de información del servicio de administración tributaria de la zona norte del Perú".* Universidad Privada del Norte, Trujillo-Perú; concluye que, existe brechas de seguridad, detectadas por el análisis GAP, donde el grado de manejo de la NTP-ISO/IEC

27001:2014 es 25%, señalando de la no existencia de un cumplimiento a las exigencias mínimas para ejecutar la administración del resguardo de datos, además existe un nivel del 30% en los controles por que no se encuentran referenciados en la políticas de seguridad (p. 76).

Además, Huaura (2019), en su estudio *"Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones"*. Universidad Nacional Mayor de San Marcos, Lima-Perú; concluyendo que una adecuada administración de los peligros del resguardo de datos, permitirá mejorar las decisiones tomadas por el ápice estratégico. Siendo preocupante la fuga de datos por intermedio de dispositivos extraíbles (51.2%), seguido del 26.8% por tecnología móvil, además del 13.4% por el manejo en la nube de dichos servicios, además del 7.3% por SW de monitoreo de escritorio y al final un 1.2% por otros medios como redes sociales, correos electrónicos, documentación impresa, y entre otros dispositivos y herramientas (p. 100-101).

Considerando a Machicao (2019), quién ejecutó la investigación *"Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) –UNA Puno 2018"*. Universidad Nacional del Altiplano, Puno-Perú; llega a la conclusión, que se identificaron doce riesgos de grado alto, veintiocho con medio y ciento cincuenta y uno con bajo riesgo, existiendo diferentes amenazas internas y externas que puedan violentar los datos que procesa la oficina de tecnología de información, quienes deben sostener su integración, confidencia y disposición de la información, toda vez que las políticas de seguridad que debe tener la información, garantizará las medidas

de seguridad y llegará a manipular técnicamente la información relevante de la entidad (p. 81).

Gonzales (2017), realizó la investigación *"Calidad de servicio y satisfacción de los estudiantes usuarios con la atención administrativa en la facultad ciencias contables y administrativas, UNA-Puno, 2017"*. Universidad Nacional del Altiplano, Puno-Perú; quién concluye que los servicios de calidad que proporciona los trabajadores es apreciada por los discentes regularmente, toda vez que los administrativos asumen eventualmente sus responsabilidades por encargo. Además, señala que los clientes están medianamente satisfechos con el servicio recibido, al final afirma que el servicio proporcionado presenta una asociación positiva (r=0.493) con las necesidades de los aprendientes, manifestando que el bienestar de los discentes se encuentran concatenado significativamente con el servicio de calidad que recibe de los administrativos (p. 70).

2.1.2 Nivel regional y local

En la investigación de Camapaza (2019), titulado *"Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la municipalidad del centro poblado de Salcedo – Puno"*. Universidad Andina del Cusco, Cusco-Perú, donde llega a concluir, que el diseñó generado y aplicado permite mitigar o disminuir el impacto de los riesgos a los que están expuestos los activos de información de la Municipalidad en estudio, para los cuales deben poseer políticas claras y controles pertinentes para las amenazas y riesgos que son necesarios en la actualidad en las instituciones (p. 104).

Por su parte Schiavonne (2022), en su estudio *"Propuesta de mitigación de riesgos en el sistema facturación de la empresa pale consultores haciendo uso de la adaptación de las metodologías pentesting standart y nist-sp 800-30-2022"*. Universidad Andina del Cusco, Cusco-Perú. Llega a la conclusión, que La metodología aplicada ayuda eficientemente en el desarrollo de análisis de vulnerabilidades basadas en herramientas y protocolos que enfocan inseguridades, pero estás se encuentran orientadas a entorno web en vista, dificultando las respectivas herramientas en entornos de aplicación de escritorio (p. 100).

2.2 Bases Teóricas

2.2.1 Riesgos de seguridad de la información

Los riesgos de seguridad de información (RSI) de acuerdo a Ld Grupo (LG 2019), es:

> "una organización de procesos de resguardo de datos y de la posibilidad de su presencia, relacionada a una acción de información" (párr. 1).

De otra parte, los RSI son "procedimientos que permiten identificar, evaluar, mitigar y comprender cualquier escenario de amenaza para la información de cualquier institución". (Iso Tools Excellence [ITE], 2019, párr. 1)

2.2.1.1 Objetivos de riesgos de seguridad de la información.

Analizar el RSI debe realizarse en cualquier circunstancia, debiendo considerar el cumplimiento de los objetivos siguientes: la identificación, evaluación, estimación, determinación de los RSI, y llegar a considerar

las decisiones oportunas sobre la seguridad de la información. (Royal, 1988, p. 83)

2.2.1.2 Riesgos básicos de seguridad de la información.

Considerando a Domènech (2017), manifiesta que se pueden encontrar algunos de los RSI (párr. 1), siendo:

- El acceso de administrador en el computador: cuando los usuarios disponen de permisos para acceder a las diferentes aplicaciones.
- Los correos maliciosos o no deseados: pueden llevar pharming, phishing, así como spam.
- Copias de seguridad; para poder recuperar los datos frente a alguna contingencia de vulneración de la seguridad.
- El buen uso de las claves: responsabilidad para gestionar las contraseñas otorgadas.
- El manejo de aplicaciones de resguardo en línea: Dropbox o Google drive (Domènech, 2017, párr. 1).

2.2.1.3 Principios del riesgo de seguridad de la información.

El resguardo de los datos de una institución debe estar basada en los siguientes tres principios (Domènech, 2017, párr. 1), a saber:

- La confidencialidad: caracterizada por impedir que los datos sean difundidos a usuarios que no tienen autorización.
- La integridad: llegara a resguardar la información.
- La disponibilidad: brindar accesibilidad de la información en todo instante a los usuarios autorizados. (Domènech, 2017, párr. 1)

2.2.1.4 Componentes del riesgo de seguridad de la información.

Considerando a Sullivan (2016), sostiene que entre los componentes de los RSI (párr. 1), son:

- El agente de amenaza: todo usuario que llega a vulnera la seguridad de datos.
- La vulnerabilidad: actores que explota y generan amenazas.
- Los resultados: referidos al producto de la vulneración.
- El impacto: Son los productos no deseados (párr. 1).

2.2.1.5 Tipología de controles de seguridad de la información.

El resguardo de los datos en toda organización debe estar sostenido en la implementación de controles y/o elementos con la finalidad de asegurar la información de todo negocio (Instituto Nacional de Ciberseguridad [INCIBE], s.f., p. 13), los cuales son:

- Físicos: elementos y/o materiales físicos para resguardar los componentes e información en la organización.
- Técnicos: soporte lógico para evitar alteraciones, modificaciones y/o destrucción de la información.
- Organizativos: políticas y acciones para brindar seguridad a la información del manejo de los usuarios. (INCIBE, s.f., p. 13)

2.2.2 Calidad de servicio

Larrea (1991), sostiene que la calidad de servicio (CS) es:

> (…) “el arreglo de las obligaciones sustanciales y adicionales a los requerimientos, deseos y expectativas del usuario, considerando la satisfacción de las necesidades y expectativas del cliente” (p. 77).

Es así, que la CS descansa “en el cumplimiento de acciones que percibe el usuario acerca la atención que recibió en un momento determinado en el cumplimiento de sus requerimientos” (Molina, 2014, párr. 1).

2.2.2.1 Componentes de la calidad de servicio.

Molina (2014), señala que los componentes a considerar para la CS, son:

- Confiabilidad: corresponde proporcionar una atención adecuada y segura para la satisfacción del cliente.
- La accesibilidad: brindar las facilidades a los consumidores.
- La respuesta: dar una atención eficiente y eficaz.
- La seguridad: acceder a servicios sin riesgos y libre de errores.
- La empatía: conocer lo que requiere el consumidor.
- La Infraestructura; ambientes adecuados y confortables para la gente (párr. 1).

2.2.2.2 Características de la calidad de servicio.

De las aportaciones por Vázquez (2020), los atributos particulares que se deben tomar en cuenta para proporcionar calidad en los servicios son:

- Intangibles: promoción de acciones, en vez de productos.
- Variables: los servicios son diversos en mérito a las expectativas.
- Durables: el servicio tiene un tiempo de vigencia.
- Simultáneos: brindar el servicio es paralelo al consumo.
- Inseparables: los usuarios y responsables del servicio participan de manera paralela.
- Tiempo: la duración del servicio debe ser óptimos y reducidos (Vázquez, 2020, párr. 1).

2.2.2.3 Propiedades de calidad de servicio.

Sistemas GC-ISO (SGCISO 2019), menciona las cualidades a tener en cuenta en la CS, son:

- Intangibilidad: no es medible el servicio.
- La heterogeneidad: el servicio es diverso y depende de la percepción del consumidor.
- La inseparabilidad: tanto el servicio y tratamiento son integrales. (párr. 1).

2.2.2.4 Dimensiones de calidad de servicio.

A partir de los escenarios científicos latentes de la CS, en un determinado espacio de tiempo. El modelo SERVQUAL es el de mayor impacto para evaluar la CS que brinda una organización.

Para Vázquez (2020), el modelo SERVQUAL (Service of quality), se caracteriza por:

> "los consumidores valoran el servicio recibido midiendo lo que piensan recibir (expectativas) con lo que recibieron (percepciones)" (párr. 1).

De donde se conoce cinco dimensiones:

- La empatía: es el servicio basado en la necesidad y personalización del cliente.
- La confianza (fiabilidad): garantía y precisión del servicio.
- Los elementos tangibles: contexto y ambiente donde se brinda el servicio.
- El potencial de respuesta: predisposición y oportunidad para brindar la prestación.

- Seguridad**:** proveer confianza y credibilidad del servicio a brindar. (Vázquez, 2020, párr. 1)

2.3 Marco conceptual

Riesgo de seguridad de la información

“procedimientos que permiten identificar, evaluar, mitigar y comprender cualquier escenario de amenaza para la información de cualquier institución”. (Iso Tools Excellence [ITE], 2019, párr. 1)

Calidad del servicio

“Cumplimiento de acciones que percibe el usuario acerca de la atención que recibió en un momento determinado en el cumplimiento de sus requerimientos”. (Molina, 2014, párr. 1)

Riesgo

“Probabilidad de que ocurra algún hecho indeseable” (Rodiguez, 2014, párr. 1).

Riesgos informáticos

“Posibilidad de que se presente alguna contingencia que dañe la tecnología informática tangible o intangible”. (Romero, 2018, p. 28)

Riesgo residual

“Inseguridad existente de manera aislada posterior a las medidas de seguridad tomadas” (Rodiguez, 2014, párr. 1).

Riesgo de aceptación

“Decisión anunciada para considerar la presencia de una contingencia particular”.

Análisis de riesgos

“Es la exploración de las inseguridades presentes para entender la naturaleza y el grado de los riesgos” (Unidad Nacional para la Gestión del Riesgo de Desastres [UNGRD], 2019).

Evaluación de riesgos

“Son procedimientos que identifican, analizan y comprenden la presencia de posibles conflictos” (Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres [CENEPRED], 2015).

Gestión de riesgos

“Es el manejo de las acciones de manera integral con la finalidad de dirigir, y monitorear una institución relacionados a los peligros” (SAP Concur, 2022, párr. 1).

Tratamiento de riesgos

“Constituye un procedimiento organizado para reducir y/o eliminar los riesgos en una empresa”.

Virus informático

“Es un programa cuyo propósito es eliminar, distorsionar y/o influir el normal funcionamiento de los sistemas informáticos” (Vieites, 2013, citado por Romero et al., 2018, p. 15).

Información

“Conjunto de datos procesados, que conforman una comunicación para el que lo emite y aquel que lo recibe” (IUPGC, 2016, p. 5).

Revisión de patrones de acceso

“Constituido por analizar los accesos y encontrar si se encuentra sostenido por patrones de acceso” (Romero et al., 2018, p. 21).

Internet

Es una red interconectada de ordenadores para el tratamiento de datos a nivel de toda la comunidad mundial (Cerf, 2022, párr. 1).

Vulnerabilidad

“Inseguridad en el uso de los sistemas tecnológicos para el irrupción de un ataque interno o externo y causar un daño” (IUPGC, 2016, p. 7).

Amenaza

“Constituye una eventualidad latente para producir daños” (IUPGC, 2016, p. 7).

Encriptación

“Es el cifrado de datos para brindar seguridad para todo individuo que no se encuentre autorizado” (Romero et al., 2018, p. 21).

Privilegios

“Permisos concedidos para el tratamiento de datos automatizados a un usuario” (IBM, 2021, párr. 1).

Clave privada

“Es un tipo de clave que se resguardada por el dueño superior” (IBM, 2021a, párr. 1).

Clave pública

“Caracterizada por contar con el acceso o es manejada cada uno de los usuarios” (IBM, 2021a, párr. 1).

Amenazas informáticas

“Actividades inapropiadas para dañar el HW, SW y datos automatizados” (Romero, 2018, p. 28).

Vulnerabilidades informáticas

“Son fallos presentados en los sistemas de seguridad al momento del tratamiento de la información” (Romero, 2018, p. 28).

Ataque pasivo

“Embestida no invasiva que no afecta a la infraestructura tecnológica e información de la organización” (Romero, 2018, p. 37).

Ataque activos

“Son actividades de sabotajes y secuestros directas, con la intensión de vulnerar la infraestructura tecnológica e información” (Romero, 2018, p. 37).

Políticas de seguridad

“Son etapas y normas para la disminución de riesgos en una institución por intermedio de tecnologías específicas” (Romero 2018, p. 55).

Antivirus

“Son sistemas basados en la detección de malware que permiten analizar los archivos y software antes de ser ejecutados” (Instituto Nacional de Ciberseguridad [INC], 2019, párr. 1).

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1 Hipótesis

3.1.1 Hipótesis General

El nivel de concordancia entre los riesgos de seguridad de la información y la calidad de servicio es significativo en la UTEA, Abancay 2021.

3.1.2 Hipótesis específicas

he1. La asociación entre los riesgos físicos de seguridad de la información con la calidad de servicio es significativa en la UTEA, Abancay 2021.

he2. La asociación entre los riesgos técnicos de seguridad de la información con la calidad de servicio es significativa en la UTEA, Abancay 2021.

he3. La asociación entre los riesgos organizativos de seguridad de la información con la calidad de servicio es significativa en la UTEA, Abancay 2021.

3.2 Método

En mérito a la naturaleza y realidad del estudio de los fenómenos en la entidad objeto de investigación, se puso en ejecución los métodos deductivos y analíticos para la manipulación de los datos.

De acuerdo a Brito (2014), el método deductivo consiste en:

> “alcanzar desenlaces específicas a partir de condiciones universales” (párr. 1).

Es así, que el método deductivo, consistió en la exploración de los fenómenos basados en sus dimensiones e indicadores de la realidad problemática objeto de investigación para arribar a conjeturas consistentes y sólidas.

El método analítico “distingue los atributos de los fenómenos y observar de forma especial cada factor que la integran” (Brito, 2014, párr. 1).

Es así que, por intermedio del método analítico, se identificó cada fenómeno estudiado, determinando la situación latente de la contingencia en la entidad educativa de nivel superior, la misma permitió identificar la concordancia existente entre ambas variables y entre sus respectivas dimensiones que la componen.

3.3 Tipo investigación

Corresponde a un estudio tipo básica, donde los datos obtenidos brindaron resultados solidos que permitieron enriquecer los conocimientos e incrementar las teorías existentes en referencia a los fenómenos en estudio.

Según Narvaez (2019), la investigación básica se caracteriza:

> “por comprender y ampliar los conocimientos sobre una variable o campo específico” (párr. 1).

De otra parte, el estudio presenta un enfoque cuantitativo, donde la información fueron estimados de forma objetiva y numérica, bajo la estadística descriptiva (Arteaga, 2020, párr. 1).

3.4 Nivel o alcance de investigación

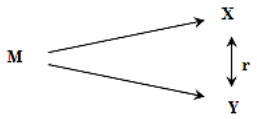
Se partió de una investigación de nivel correlacional descriptivo, donde se describió de manera precisa y robusta la realidad problemática en la entidad en base a los fenómenos estudiados para luego identificar el nivel de concordancia que existía entre ambos fenómenos en la UTEA, Abancay 2021.

Por cuanto todo estudio de nivel correlacional “permite conocer y advertir las asociaciones que pudiera existir entre variables”. (Hernández, Fernández y Baptista, 2014, p. 93).

Señalando Hernández et al. (2014), que la investigación descriptiva:

> “tienden a inspeccionar y señalar los componentes significativos de las peculiaridades de las variables y/o objetos que se encuentran para su respectivo análisis”. (p. 92).

La tipología fue:



Manifestando:

M = La muestra.

X = Variable 1: Riesgo de seguridad de la información.

Y = Variable 2: Calidad de servicio.

r = Relación de las variables.

3.5 Diseño de investigación

Corresponde a un diseño de estudio no experimental-transversal, permitiendo lograr información de los fenómenos basados en sus elementos e indicadores en un solo momento, tal cual se presentaron en su ambiente natural, sin que se realice manipulación alguna de los datos a partir de las cuales se identificó el grado de concordancia significativa del RSI y la CS que se presentan en la UTEA, Abancay 2021.

Toda vez que Hernández et al. (2014), sostienen que el estudio de diseño no experimental:

> “se desarrollan si llegar a manipular deliberadamente los fenómenos en donde se observaran sólo en su entorno natural para examinarlos”. (p. 152).

Por su parte los estudios de corte transversal “son aquellos en donde los datos se logran en un momento único para analizarlos sin ningún tipo de manipulación” (Hernández et al., 2014).

3.6 Operacionalización de Variables

Variable de investigación	Definición conceptual	Dimensiones	Definición operacional	Indicadores
Variable X: Riesgo de seguridad de la información	"Es el proceso mediante el cual se identifica, comprende, evalúa, y mitiga cualquier tipo de riesgo o amenaza en la información de una determinada organización". (IsoTools excellence [ITE], 2019, párr. 1)	Físicos.	Consiste en la protección de la información contra la divulgación, transferencia, modificación o destrucción no autorizada sea de forma voluntaria o accidental en la organización.	Medidas físicas. Sala de servidores. Incendios e inundaciones Accesos no autorizados. Sistema de control de oficina. Cerraduras en los despachos y armarios. Copias de seguridad. Cámaras de seguridad. Puertas de seguridad.
		Técnicos.		Seguridad de la información. Antivirus. Cortafuegos. Cifrado Sistema de copias de seguridad. Sistema de seguridad de la información.
		Organizativos.		Formación de seguridad. Identificación de responsables. Implantación de procedimientos. Alta de usuarios Baja de usuarios Capacitación en seguridad. Políticas de seguridad

Fuente: Elaboración propia.

Variable de investigación	Definición conceptual	Dimensiones	Definición operacional	Indicadores
Variable Y: Calidad de servicio.	“Consiste en cumplir con las expectativas que tiene el cliente sobre que tan bien un servicio satisface sus necesidades”. (Molina, 2014, párr. 1)	Empatía	Es el nivel en que los procesos, medios y equipos deseables de la organización se utilizan para alcanzar los servicios mayores en la satisfacción de los usuarios y/o clientes.	Modelo SERVQUAL
		Confianza (fiabilidad)		Modelo SERVQUAL
		Elementos tangibles		Modelo SERVQUAL
		Capacidad de repuesta		Modelo SERVQUAL
		Seguridad		Modelo SERVQUAL

Fuente: Elaboración propia.

3.7 Población, muestra y muestreo

3.7.1 Población

De acuerdo a lo señalado por Hernández et al. (2014), una población es:

> "una agrupación de bienes, individuos o casos que contienen especificaciones propias" (p. 174).

Por cuanto la población estuvo conformado por el talento humano de la oficina de tecnologías de la información (OTI), y de la subdirección de centro de cómputo e informática (CCI), en un total de 15 trabajadores administrativos, además de los discentes de las diez (10) Escuelas Profesionales (EP) de la UTEA, Abancay, en un total 3256 matriculados en el semestre 2020-I, datos considerados en la fecha de inicio de la investigación.

Tabla 1

Población o universo

Universidad Tecnológica de los Andes, Abancay 2021	
Detalle	Población o universo
Oficina de tecnología de la información	10
Centro de cómputo e informática	05
Estudiantes de la UTEA-Abancay	3256
Total	3271

Fuente: Subdirección de centro de cómputo e informática-UTEA 2020, (2020-I)

3.7.2 Muestra

Las unidades muéstrales que conforman la muestra del estudio fueron el talento humano que se encontraban cumpliendo sus funciones en OTI, subdirección de centro de cómputo e informática, así como los aprendientes de las diez EP de la UTEA, Abancay. Considerando un tamaño total de la muestra de 359 unidades de análisis (15 trabajadores administrativos y 344 estudiantes).

Es así, que para considerar el tamaño de la muestra se aplicó por una parte el método probabilístico para la población de discentes, donde todos los estudiantes tuvieron la misma probabilidad de ser consideradas como unidades de análisis para la obtención de la información. Por cuanto para establecer el tamaño de la muestra se llegó a manejar la fórmula estadística de Cochran.

Llegando a afirmar que Cochran “permite encontrar el tamaño de muestra de la población elegida para una encuesta o experimento” (Bastis Consultores [BC], 2022, párr. 1).

Por otra parte, se manejó el método no probabilístico para los colaboradores de OTI y la subdirección de centro de cómputo e informática por ser una población pequeña, finita y que los sujetos presentan características comunes y propias en concordancia a las funciones que desempeñan en las respectivas oficinas administrativas de la UTEA.

Por cuanto la dimensión de la muestra (estudiantes 2020-I) se obtuvo por Cochran, utilizando la siguiente ecuación:

$$n = \frac{NZ^2S^2}{d^2(N-1) + Z^2S^2}$$

Señalando:

n: La capacidad de la muestra.

N: La capacidad de la población.

Z: El coeficiente de confianza o valor de Z crítico.

S: La varianza de la población estudiada.

d: El nivel de precisión absoluta.

Ejecutando la ecuación:

n = ?

N = 3256 estudiantes.

Z = El CC: de acuerdo a la equivalencia al 95 % = 1.96

S = La VP: 0.5

d = El NPA: según la equivalencia al 95 % = 0.05

$$n = \frac{3256 * 1.96^2 * 0.5^2}{0.05^2 * (3256-1) + 1.96^2 * 0.5^2}$$

$$n = \frac{3127.0624}{9.0979} = 343.71$$

$n =$ 344 estudiantes

Tabla 2

Muestra de la investigación

UTEA - Abancay		
Detalle	Población	Muestra
OTI (2020-I)	10	10
Centro de cómputo e informática (2020-I)	05	05

Estudiantes de la UTEA-Abancay (2020-I)	3256	344
Total	3271	359

Fuente: Elaboración propia.

3.7.3 Muestreo

Para la investigación consistió en primera instancia el muestro tipo intencionado aplicados a los sujetos de OTI y subdirección de centro de cómputo e informática, llegando a participar todos los talentos humanos por sus características, propiedades y ser pequeña (Parra, 2022, párr. 1). En segundo lugar se aplicó en muestreo tipo aleatorio simple, en la determinación de los estudiantes, donde fueron elegidos a cada uno de ellos al azar (Ortega, 2022, párr. 1), quienes presentaron la misma probabilidad de ser seleccionados como unidades muéstrales. Aplicando al total de las 359 unidades muéstrales (15 colaboradores administrativos y 344 estudiantes) los cuestionarios respectivos y obteniendo de los mismos la información del estudio.

De donde el muestreo “es el proceso de seleccionar un subconjunto de un conjunto mayor, población de interés para acopiar información para responder a un planteamiento de un problema de estudio” (Hernández et al., 2014, p. 267).

3.8 Técnicas e instrumentos

3.8.1 Técnica

La encuesta fue la técnica aplicada, que estaba constituido de ítems consistentes para el acopio de los datos entorno a las propiedades, elementos, dimensiones e indicadores de los fenómenos estudiados, la mismas

permitieron describir la naturaleza real y latente del riesgo del resguardo de los datos y de la calidad de los servicios en la UTEA, Abancay 2021.

Por cuanto la encuesta “permite la obtención de los datos mediante la interrogación que se desarrolla al encuestado con la finalidad de que proporción información necesaria para el estudio” (Arias, 2020, p. 18).

3.8.2 Instrumentos

Los instrumentos utilizados para la investigación estuvieron sujetos a dos cuestionarios auto-administrados, de donde para la variable RSI se estructuró de manera propia el cuestionario que contenía 22 ítems necesarios a partir de sus dimensiones e indicadores señaladas en el marco teórico, con sus respectivas categorías, valoraciones y códigos, en donde la escala de medición tipo Likert fue: 1=totalmente inadecuado y 5=totalmente adecuado.

Por cuanto, para Hernández et al. (2014), un cuestionario es:

> “Una agrupación de ítems relacionado a uno o varios fenómenos a ser medidos” (p. 217).

De otra parte, para el fenómeno CS, se aplicó el modelo SERVQUAL, para medir la calidad del servicio y conocer las expectativas de los clientes, y cómo ellos valoran el servicio (Zeithaml, Bitner y Gremler, 2009 citado por Matsumoto-Nishizawa, 2014), de donde el cuestionario contenía 22 ítems para conocer el interés de los estudiantes sobre la CS, que incluye una sección para cuantificar las evaluaciones de los talentos humanos y estudiantes, bajo la escala de medición tipo Likert de 7 puntos, siendo 1=completamente en desacuerdo y 7=totalmente de acuerdo.

En esa línea, sobre la validez de los instrumentos, fueron ejecutados para el fenómeno RSI basado en la validación del juicio de expertos (anexos), mientras que para el modelo SERVQUAL fueron validados por los autores Zeithaml, Bitner y Gremler (2009) citado por (Matsumoto-Nishizawa, 2014).

Así mismo cada uno de los instrumentos, una vez logrado los datos y resultados, fueron sometidos a su confiabilidad respectiva, por intermedio de método de Alfa de Cronbach, siendo “un coeficiente usado para saber cuál es la fiabilidad de una escala o test” (Ruiz, 2019, párr. 1). Aplicado la misma se alcanzó un α=0.711 para la variable RSI y α=0.874 para el fenómeno CS, ($0.7 < \alpha = 0.711$ y $0.874 < 1$); estableciendo que los instrumentos manejados contienen datos consistentes y fiables, de donde el coeficiente de alfa presenta una confiabilidad satisfactoria de ambas variables, en vista que las mismas se encuentran muy próximo a la unidad (1), presentando solidez y seguridad en la información alcanzada a partir de las interrogantes de cada cuestionario.

3.9 Consideraciones éticas

El acopio de información oportuna, se emanó de las exigencias de toda investigación, donde se consideró los elementos, propiedades, actitudes y principios éticos personales de toda investigación, partiendo con la emisión del documento pertinente ante las instancias superiores de la UTEA-Abancay, para autorización y desarrollo del estudio, para luego aplicar los instrumentos en las unidades administrativas respectivas y discentes de las escuelas profesionales de la UTEA.

La investigación se ejecutó bajo los siguientes criterios:

Consentimiento informado; se solicitó de manera verbal la autorización para su participación de la unidades muéstrales de la investigación (estudiantes).

Participación; El talento humano y estudiantes participó libremente en las respuestas de los cuestionarios, sin existir presión alguna.

Motivación; El talento humanos de OTI, subdirección de centro de cómputo e informática, así como los estudiantes de la UTEA, recibieron la motivación correspondiente a cerca de la significancia del estudio.

Protección; la protección absoluta de los datos personales de los discentes y talento humano participantes en la investigación.

La confidencialidad absoluta; donde los datos logrados fueron manejados sólo para el presente estudio.

3.10 Procedimientos estadísticos

3.10.1 Procesamiento y presentación de datos

La información obtenida fueron procesados y tabulados para lograr las bases de datos correspondientes, luego migrar a sus respectivas tablas, la mismas están estructuradas numéricamente bajo frecuencias, porcentajes y representadas en sus figuras pertinentes, considerando para ello la estadística descriptiva, después analizar, interpretar y generar las discusiones necesarias, y arribar a la identificación y valoración de las hipótesis de investigación, al final se llegó a conjeturas robustas y consistentes sobre el nivel de concordancia existente entre los fenómenos objeto de investigación en la UTEA-Abancay, llegando a utilizar el software (SW) SPSS V. 25.

3.10.2 Análisis e interpretación de datos

Las tablas y figuras de los fenómenos reflejan los resultados del estudio, siendo analizados e interpretados objetivamente sobre la realidad latente de las variables en la entidad universitaria, para luego efectuar las discusiones respectivas y cotejadas con trabajos de investigación previos al estudio, llegando al final a validar las hipótesis establecidas, para la cual se aplicó la estadística inferencial por el coeficiente *r* de Pearson, pudiendo plantear las hipótesis estadísticas respectivas que determinaron el nivel de concordancia que existe entre ambos fenómenos estudiados.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Resultados

Alcanzada la información producto del manejo de los instrumentos, fueron tabulados y generadas en las bases de datos pertinentes, luego se representaron en las tablas de frecuencias y porcentuales, para después representadas en las figuras respectivas a partir de la cuales se analizaron, interpretaron y se efectuaron las respectivas discusiones y arribar a conclusiones robustas consistentes.

Variable X: Riesgos de seguridad de la información (RSI)

Tabla 3

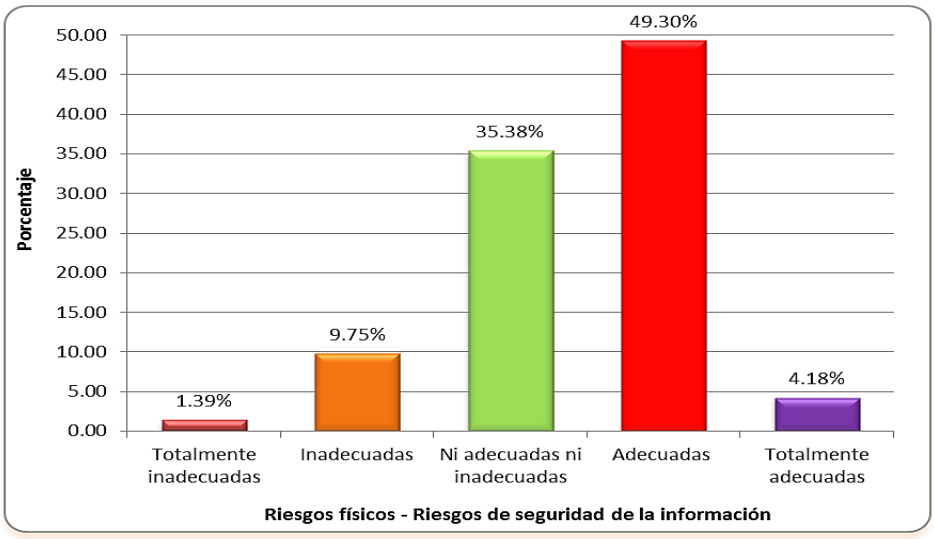
Riesgos físicos-riesgos de seguridad de la información

Afirmación	f	%	Porcentaje Acumulado
Totalmente inadecuadas	5	1.4	1.4
Inadecuadas	35	9.78	11.18
Ni adecuadas ni inadecuadas	127	35.47	46.65
Adecuadas	177	49.44	96.09
Totalmente adecuadas	14	3.91	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 1

Riesgos físicos de seguridad de la información



Fuente: Elaboración de la tabla 3

Al visualizar la tabla 3 y figura 1, se aprecia que el 49.30% de los sujetos que manifestaron adecuadas, el 35.38% ni adecuadas ni inadecuadas, luego el 9.75% sostuvieron inadecuados, después el 4.18% indicaron totalmente adecuados y el 1.39% afirmaron totalmente inadecuados son las inseguridades físicas en cuanto a la SI en la entidad de educación superior.

Tabla 4

Riesgos técnicos-riesgos de seguridad de la información

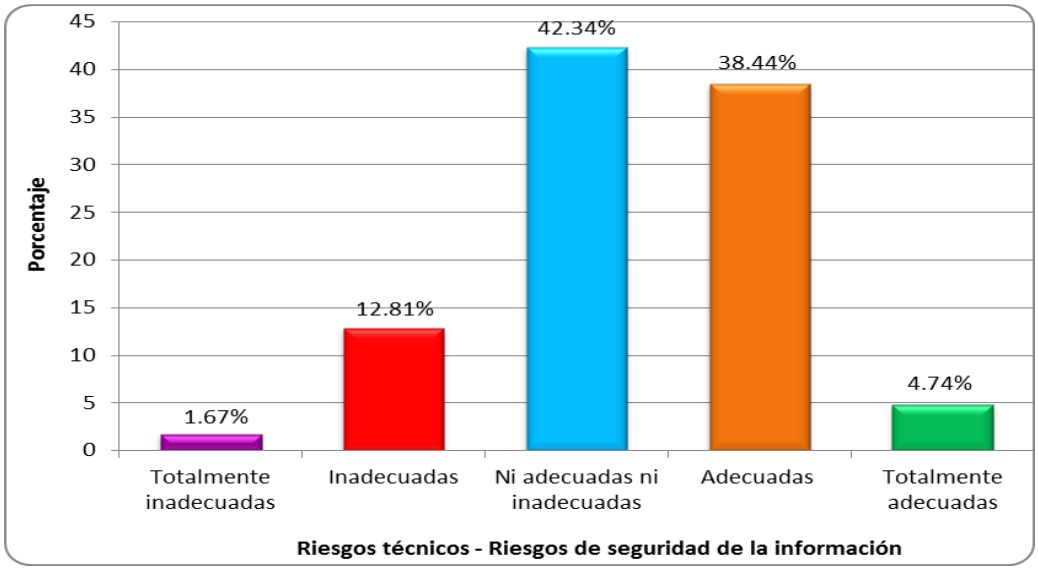
Afirmación	f	%	Porcentaje Acumulado
Totalmente inadecuadas	6	1.67	1.67
Inadecuadas	46	12.81	14.48
Ni adecuadas ni inadecuadas	152	42.34	56.82
Adecuadas	138	38.44	95.26

Totalmente adecuadas	17	4.74	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 2

Riesgos técnicos de seguridad de la información



Fuente: Elaboración de la tabla 4

La tabla y figura que antecede presentan datos de los sujetos encuestados, de donde el 42.34% manifestaron ni adecuadas ni inadecuadas, además el 38.44% señalaron adecuadas, el 12.81% declararon inadecuadas, luego el 4.74% alegaron totalmente adecuadas y al final el 1.67% revelaron totalmente inadecuados son los riesgos técnicos de la SI en la universidad objeto de estudio.

Tabla 5

Riesgos Organizativos-riesgos de seguridad de la información

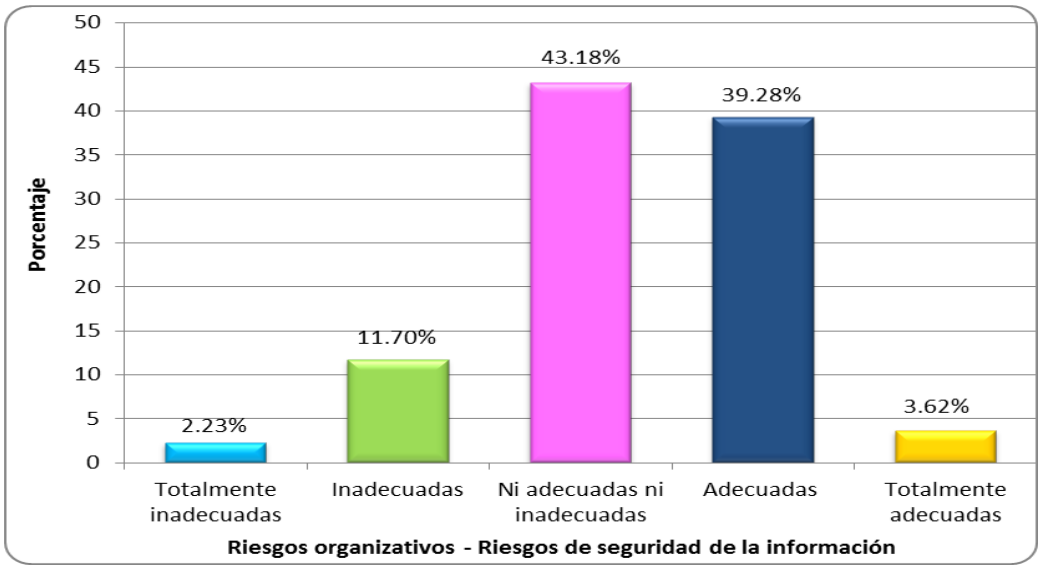
Afirmación	f	%	Porcentaje Acumulado
Totalmente inadecuadas	8	2.23	2.23
Inadecuadas	42	11.70	13.93
Ni adecuadas ni inadecuadas	155	43.18	57.11

Adecuadas	141	39.28	96.39
Totalmente adecuadas	13	3.62	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 3

Riesgos organizativos de seguridad de la información



Fuente: Elaboración de la tabla 5

La presente tabla 5 y su respectiva figura precedente, contienen información de los encuestados, en donde el 43.18% afirmaron ni adecuadas ni inadecuadas, sucesivamente el 39.28% declararon adecuadas, luego el 11.70% asintieron inadecuadas, además del 3.62% que dijeron totalmente adecuadas y sólo el 2.23% enfatizó totalmente inadecuadas son los riesgos organizativos en la SI en la institución universitaria.

Tabla 6

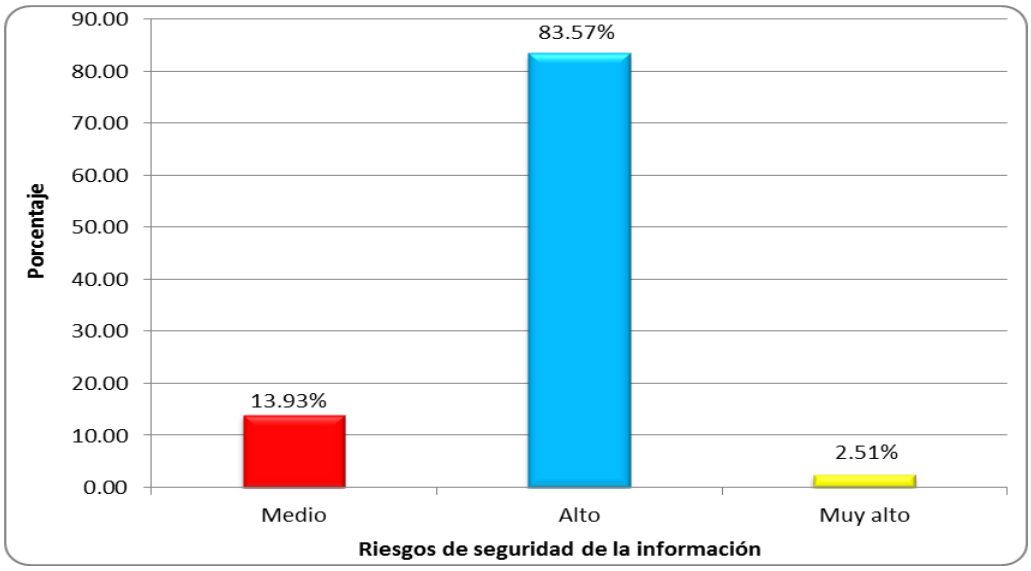
Nivel de riesgo de seguridad de la información

Afirmación	f	%	Porcentaje Acumulado
Medio	50	13.93	13.93
Alto	300	83.57	97.50
Muy alto	9	2.51	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 4

Riesgo de seguridad de la información



Fuente: Elaboración de la tabla 6

A partir de la precedente tabla y figura, se previene el 83.57% de los individuos declararon alto, seguido del 13.93% que sostuvieron medio y el 2.51% afirmaron muy alto el RSI que presenta la UTEA, Abancay-Apurímac.

Variable Y: Calidad de servicio (CS)

Tabla 7

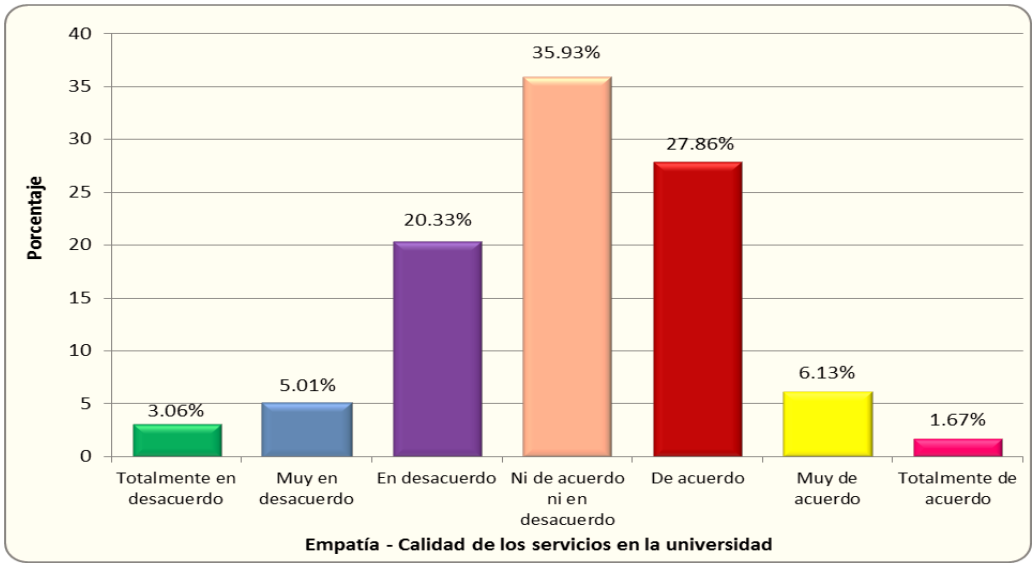
Empatía-calidad de los servicios en la universidad

Afirmación	f	%	Porcentaje Acumulado
Totalmente en desacuerdo	11	3.06	3.06
Muy en desacuerdo	18	5.01	8.07
En desacuerdo	73	20.33	28.40
Ni de acuerdo ni en desacuerdo	129	35.93	64.33
De acuerdo	100	27.86	92.19
Muy de acuerdo	22	6.13	98.32
Totalmente de acuerdo	6	1.67	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 5

Empatía-calidad de los servicios en la universidad



Fuente: Elaboración de la tabla 7

La tabla 7 que refleja los datos porcentuales en la figura 5, donde el 35.93% de las unidades de análisis manifestaron ni de acuerdo ni en desacuerdo, seguido del 27.86% que indicaron de acuerdo, luego el 20.33% dijeron en desacuerdo, además el 6.13% afirmó muy de acuerdo, el 5.01% sostuvieron muy en desacuerdo y tan sólo el 3.06% que dijeron totalmente en desacuerdo y 1.67% señalaron totalmente de acuerdo, con la empatía demostrada por el talento humano en los servicios que proporcionan.

Tabla 8

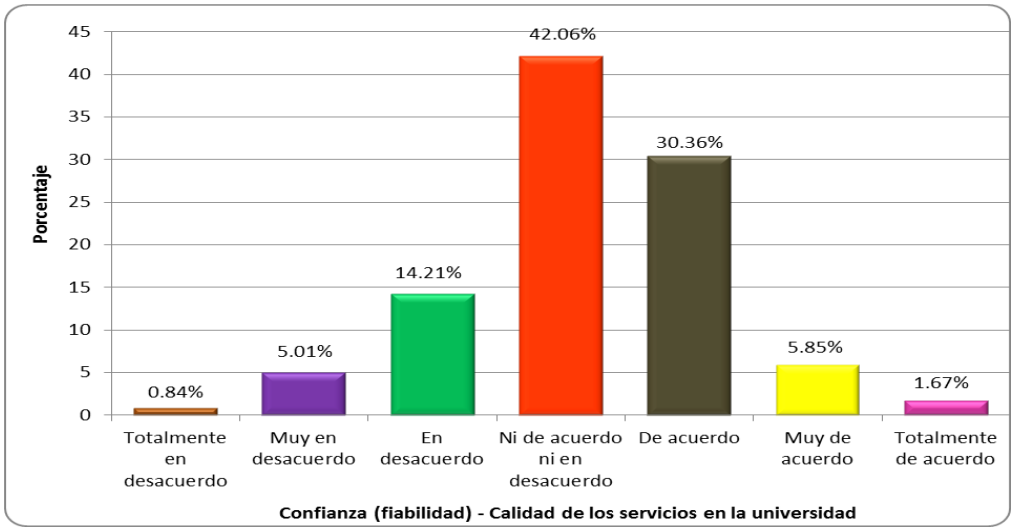
Confianza (fiabilidad)-calidad de los servicios en la universidad

Afirmación	f	%	Porcentaje Acumulado
Totalmente en desacuerdo	3	0.84	0.84
Muy en desacuerdo	18	5.01	5.85
En desacuerdo	51	14.21	20.06
Ni de acuerdo ni en desacuerdo	151	42.06	62.12
De acuerdo	109	30.36	92.48
Muy de acuerdo	21	5.85	98.33
Totalmente de acuerdo	6	1.67	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 6

Confianza (fiabilidad) de la calidad de los servicios en la universidad



Fuente: Elaboración de la tabla 8

Al observar la tabla y figura que antecede, se considera que el 42.06% sostuvieron ni de acuerdo ni en desacuerdo, el 30.36% manifestaron de acuerdo, luego el 14.21% dijeron en desacuerdo, así mismo el 5.85% y el 5.01% afirmaron muy de acuerdo y muy en desacuerdo respectivamente, además el 1.67% asentaron totalmente de acuerdo y sólo 0.84% señalaron totalmente en desacuerdo con la

confianza (fiabilidad) trasmitida en los servicios que proporciona la organización universitaria.

Tabla 9

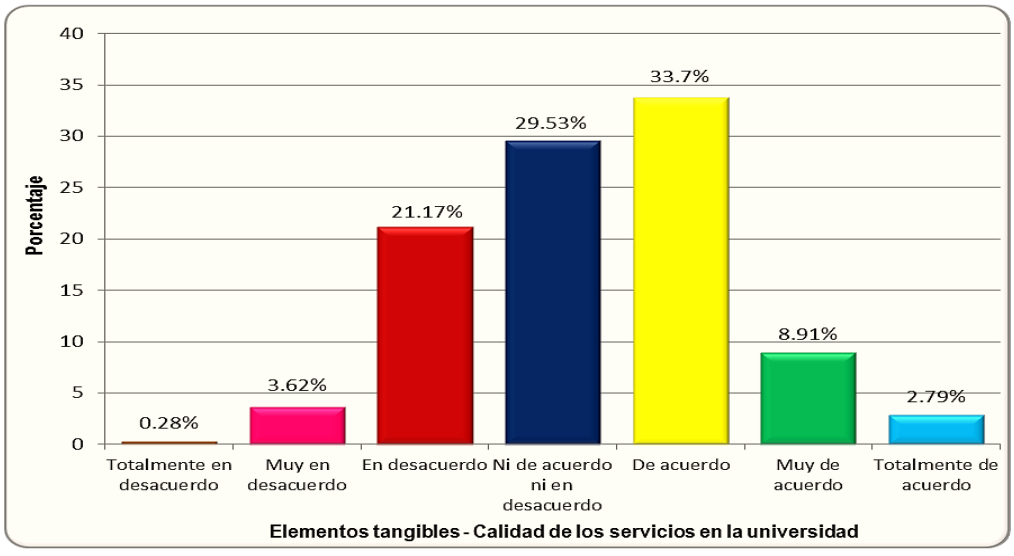
Elementos tangibles-calidad de los servicios en la universidad

Afirmación	f	%	Porcentaje Acumulado
Totalmente en desacuerdo	1	0.28	0.28
Muy en desacuerdo	13	3.62	3.90
En desacuerdo	76	21.17	25.07
Ni de acuerdo ni en desacuerdo	106	29.53	54.60
De acuerdo	121	33.7	88.30
Muy de acuerdo	32	8.91	97.21
Totalmente de acuerdo	10	2.79	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 7

Elementos tangibles de la calidad de los servicios en la universidad



Fuente: Elaboración de la tabla 9

Partiendo de la tabla 9 y la figura 7, donde se distingue que el 33.7% afirmaron de acuerdo, el 29.53% indicaron ni de acuerdo ni en desacuerdo, además el 21.17%

revelaron en desacuerdo, seguido del 8.91% advirtieron muy de acuerdo, luego el 3.62% y 2.79% exteriorizaron muy en desacuerdo y totalmente de acuerdo respectivamente y al final el 0.28% señalaron estar totalmente en desacuerdo en relación a los elementos tangibles que existen en los servicios que brinda en la Casa Superior de Estudios.

Tabla 10

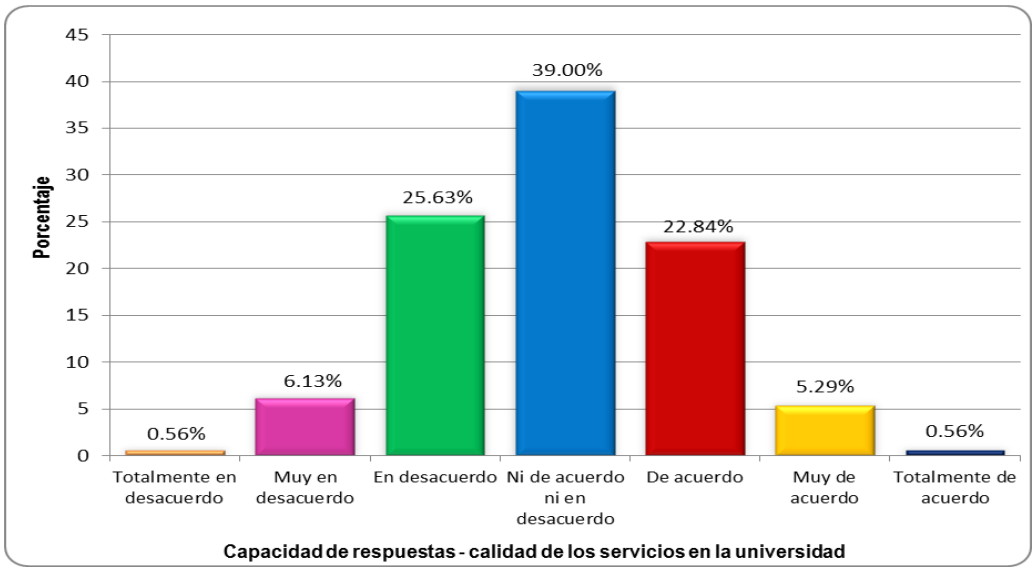
Capacidad de respuestas-calidad de los servicios en la universidad

Afirmación	f	%	Porcentaje Acumulado
Totalmente en desacuerdo	2	0.56	0.56
Muy en desacuerdo	22	6.13	6.69
En desacuerdo	92	25.63	32.32
Ni de acuerdo ni en desacuerdo	140	39.00	71.32
De acuerdo	82	22.84	94.16
Muy de acuerdo	19	5.29	99.45
Totalmente de acuerdo	2	0.56	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 8

Capacidad de respuesta de la calidad de los servicios en la universidad



Fuente: Elaboración de la tabla 10

En la misma línea la tabla y la figura respectiva que precede, contiene datos de las unidades de análisis, en la que el 39.00% anunciaron ni de acuerdo ni en desacuerdo, seguido del 25.63% que afirmaron en desacuerdo, además del 22.84% que asintieron de acuerdo, luego el 6.13% y 5.29% indicaron muy en desacuerdo y muy de acuerdo respectivamente, y de manera igualitaria el 0.56% señalaron totalmente de acuerdo y totalmente en desacuerdo con la capacidad de respuesta que se brinda en la comunidad universitaria.

Tabla 11

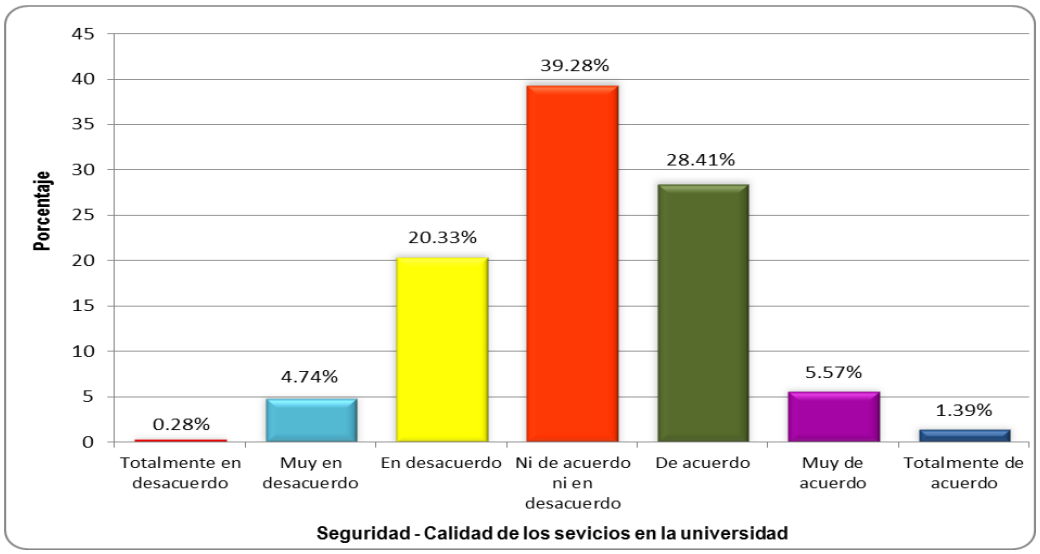
Seguridad-calidad de los servicios en la universidad

Afirmación	f	%	Porcentaje Acumulado
Totalmente en desacuerdo	1	0.28	0.28
Muy en desacuerdo	17	4.74	5.02
En desacuerdo	73	20.33	25.35
Ni de acuerdo ni en desacuerdo	141	39.28	64.63
De acuerdo	102	28.41	93.04
Muy de acuerdo	20	5.57	98.61
Totalmente de acuerdo	5	1.39	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 9

Seguridad de la calidad de los servicios en la universidad



Fuente: Elaboración de la tabla 11

Al visualizar la tabla y figura anterior, se distingue que el 39.28% imprimió ni de acuerdo ni en desacuerdo, el 28.41% sostuvo de acuerdo, también el 20.33% afirmaron en desacuerdo, además del 5.57% manifestaron muy de acuerdo, luego el 4.74% manifestaron muy en desacuerdo, y al final el 1.39% y 0.28% de manera respectiva dijeron totalmente de acuerdo y totalmente en desacuerdo con la seguridad proporcionada en los servicios que proporciona la universidad.

Tabla 12

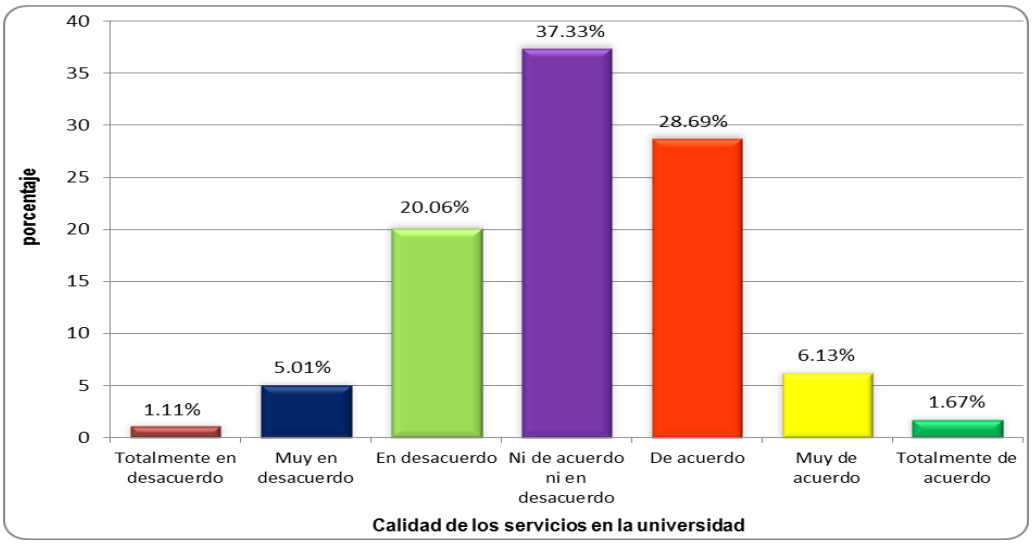
Calidad de los servicios en la universidad

Afirmación	f	%	Porcentaje Acumulado
Totalmente en desacuerdo	4	1.11	1.11
Muy en desacuerdo	18	5.01	6.12
En desacuerdo	72	20.06	26.18
Ni de acuerdo ni en desacuerdo	134	37.33	63.51
De acuerdo	103	28.69	92.20
Muy de acuerdo	22	6.13	98.33
Totalmente de acuerdo	6	1.67	100
Total	359	100	

Fuente: Elaboración propia, instrumento ejecutado

Figura 10

Calidad de los servicios en la universidad



Fuente: Elaboración de la tabla 12

Al visualizar la tabla 12 y figura 10, se desprende que el 37.33% de los sujetos indicaron ni de acuerdo ni en desacuerdo, seguido del 28.69% que revelaron de acuerdo, luego el 20.06% dijeron en desacuerdo, además del 6.13% señalaron muy de acuerdo, el 5.01% afirmaron muy en desacuerdo, para que al final el 1.67% imprimieron totalmente de acuerdo y sólo el 1.11% sostuvieron totalmente en desacuerdo con la CS en la institución universitaria.

4.2 Discusiones de resultados

Los resultados logrados en el estudio permitieron desarrollar las respectivas discusiones:

Respecto al Objetivo general: *"Identificar el nivel de concordancia entre los riesgos de seguridad de la información y la calidad de servicio en la UTEA, Abancay 2021"*.

Se establece de manera categórica la validación de la hipótesis general en base a

la correlación *r* Pearson con rango 0.160** y donde su *p*-valor alcanzado α=0.002 es menor al error de significancia del 5.0% (Sig. bilateral α=0.002 < 0.05) demostrando que el grado de concordancia entre los RSI y la CS sí es significativo, positivo y moderados en la UTEA, Abancay 2021; situación evidenciada en el 83.57% de las unidades de análisis, señalando que los niveles de los RSI en la entidad son altos en lo referente a los entornos físicos, técnicos y organizativos de las instalaciones tecnológicas, lógicas (SW) y políticas de seguridad, al mismo tiempo el 37.33% asintieron que no se encuentran ni de acuerdo ni en desacuerdo con la CS que reciben, enmarcadas en la empatía, confianza, los componentes visibles, capacidad de respuesta y seguridad en las necesidades académicas-administrativas requeridas por los usuarios discentes y padres de familia. Realidad anidada con la investigación de Maquera (2022), señalando que, de acuerdo a la prueba de Pearson cuyo valor 0,540, siendo p=0,000); determinando el sistema de administración del resguardo de datos presenta una influencia directa y significativa con la calidad de servicio en la entidad municipal (p. 70).

En referencia al objetivo específico primero: *"Determinar la asociación entre los riesgos físicos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021*". Se sostiene de forma contundente la contrastación de la primera hipótesis específica a partir de *r* Pearson de 0.126*, cuyo *p*-valor obtenido α=0.017 es menor al grado de error de 0.05 (Sig. bilateral α=0.017 < 0.05), que determina que la asociación entre los RSI con la CS sí es significativa positiva y moderada en la UTEA, Abancay 2021; circunstancias dispuestas en el 49.44% de adecuado los riegos físicos de la SI en la comunidad universitaria, realidad

reflejada por los niveles de protección del perímetro, acondicionamiento de las instalaciones, antiincendios e inundaciones, así de las disposiciones de resguardo y monitoreo de las cerraduras de los despachos y armarios, las cámaras de videovigilancia de la universidad para monitorear y evitar accesos no autorizados y evitar daños a las dependencias, tecnología y datos de la entidad académica superior, entorno anidado por el 37.33% que exteriorizaron estar ni de acuerdo ni en desacuerdo con las instalaciones físicas atractivas, pertinentes, los equipos tecnológicos y sistemas de información, y los materiales que opera para la presentación del servicio a los usuarios uteinos. Realidad tal señalada por Fajardo (2017), que afirma que, existen fisuras asociadas al diseño y manejo del software, además de las debilidades en la infraestructura tecnológica que adquiere, procesa, envía y almacena los datos, haciendo notorio de la gran necesidad de implementar un plan para el monitoreo de riesgos interesados a borrar y/o reducir las contingencias que corren la información institucional. Toda vez que la seguridad encontrada es de criticidad “Alta” (p. 69-70).

Sobre el segundo objetivo específico: *“Identificar la asociación entre los riesgos técnicos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021”*. Se llega a evidenciar y validar la segunda hipótesis específica basada en la correlación *r* de Pearson que fue de 0.153** además y el *p*-valor derivado es α=0.004 estando por debajo del nivel de significancia de 5% (Sig. bilateral α=0.004 < 0.05), señalando que la asociación entre los riesgos técnicos de SI con la CS sí es significativa positiva y moderada en la UTEA, Abancay 2021; condiciones manifestadas en el 42.34% de ni adecuados ni inadecuados las

inseguridades técnicas del resguardo de datos en la organización, por los sistemas de resguardo de redes firewall o cortafuegos, el software antivirus y el secreto de los datos de la institución para el resguardo de la subred de servicios frente a amenazas internas y externas, así como por las copias de seguridad que desarrolla para salvaguardar la información procesada, almacenada y compartida en los archivos de sus bases de datos y perfiles de correos electrónicos institucionales, que realiza, con la concatenación directa del 37.33% que mostraron estar ni de acuerdo ni en desacuerdo con las respuestas brindadas a las expectativas esperadas, la promesa y demostrar estar capacitados los empleados para responder eficientemente a sus problemas, preguntas e inquietudes del estudiante. Contextos concordantes en la investigación de Calderón (2015), donde manifiesta que, los procesos de Octave, permitirá desarrollar la evaluación de inseguridades de forma precisa, debido a sus etapas precisas hacia todas las unidades de la empresa, siendo de significación que los datos no corran riesgo alguno (p. 108).

Al final objetivo específico tercero: *"Determinar la asociación entre los riesgos organizativos de seguridad de la información con la calidad de servicio en la UTEA, Abancay 2021".* Por cuanto se valida la hipótesis especifico tercero en base a la correlación de *r* Pearson que brindo 0.104* y donde su *p*-valor logrado α=0.050 es igual al grado del error de 0.05 (Sig. bilateral α=0.050 < 0.05), determinado que la asociación entre los riesgos organizativos de SI con la calidad de servicio sí es significativa moderada positiva en la UTEA, Abancay 2021; ambiente revelado en el 43.18% de ni adecuadas ni inadecuadas los riesgos organizativos de los RSI, por los mecanismos para revisar los permisos concedidos a los interesados de los

sistemas tecnológicos, las capacitaciones en las políticas de seguridad diseñadas e implantadas para la concientización, salvaguardas en ciberseguridad y proteger la información de la universidad, en afinidad del 37.33% que alegaron ni de acuerdo ni en desacuerdo con los horarios de atención que ofrecen y brindan los colaboradores para responder a sus expectativas esperadas y el comportamiento de los empleados que no trasmiten confianza, seguridad y capacidad de organización del servicio que brindan a los usuarios universitarios. Condiciones sostenidas por Rodríguez y Torres (2019), quienes afirman que en todas las organizaciones deben considerar de manera obligatoria los procesos operacionales y analizar los riesgos informáticos, toda vez que si no se tienen los conocimientos respectivos sería muy complicado afrontar posibles contingencias en el resguardo de datos, para la protección de datos y que de no ser así implicaría impactos negativos para la organización, ameritando una planificación para poner a buen recaudo los datos institucionales (p. 42).

4.3 Prueba de hipótesis

Hipótesis general:

Tabla 13

Concordancia de riesgos de seguridad de la información y la calidad de los servicios en la universidad

		Riesgos de seguridad de la información	Calidad de los servicios en la universidad
Riesgos de seguridad de la información	Correlación de Pearson	1	,160**
	Sig. (bilateral)		,002
	N	359	359
Calidad de los servicios en la universidad	Correlación de Pearson	,160**	1
	Sig. (bilateral)	,002	

N	359	359

Fuente: Elaboración propia, SPSS V. 25, datos obtenidos de los instrumentos

Análisis e interpretación

Partiendo de la tabla 13, se plantea la Hipótesis estadística; Hipótesis nula (Ho) e Hipótesis alterna (Ha), de donde:

Ho: El nivel de concordancia entre los riesgos de seguridad de la información y la calidad de servicio no es significativo en la UTEA, Abancay 2021.

Ha: El nivel de concordancia entre los riesgos de seguridad de la información y la calidad de servicio si es significativo en la UTEA, Abancay 2021.

Con nivel de significancia de: α=0,05.

Coeficiente de correlación r de Pearson: 0.160**.

Donde el valor *p* calculado: p= 0.002

Conclusión de la hipótesis general: En vista que *p* o Sig. bilateral 0.002<0.05 (nivel de significancia), la hipótesis nula (Ho) se rechaza, admitiendo la hipótesis alterna (Ha), concluyendo que el nivel de concordancia entre los RSI y la CS, sí es significativo en la UTEA, Abancay 2021.

Hipótesis específicas

Tabla 14

Asociación del riesgo físico y la calidad de los servicios en la universidad

Correlaciones			
		Riesgos físicos	Calidad de los servicios en la universidad
Riesgos físicos	Correlación de Pearson	1	,126*
	Sig. (bilateral)		,017
	N	359	359
Calidad de los servicios en la universidad	Correlación de Pearson	,126*	1
	Sig. (bilateral)	,017	
	N	359	359

Fuente: Elaboración propia, SPSS V. 25, datos obtenidos de los instrumentos

Análisis e interpretación

Considerando la tabla 14, se plantea la Hipótesis estadística; Hipótesis nula (Ho) e Hipótesis alterna (Ha), por cuanto:

Ho: La asociación entre los riesgos físicos de seguridad de la información con la calidad de servicio no es significativa en la UTEA, Abancay 2021.

Ha: La asociación entre los riesgos físicos de seguridad de la información con la calidad de servicio sí es significativa en la UTEA, Abancay 2021.

Con nivel de significancia de: α=0,05.

Coeficiente de correlación r de Pearson: 0.126*.

Donde el valor *p* calculado: p= 0.017

Conclusión de la hipótesis específica primera: En vista que *p*-valor o Sig. bilateral 0.017<0.05 (nivel de significancia), por lo que la hipótesis nula (Ho) se rechaza admitiendo la hipótesis alterna (Ha), donde se concluye que la asociación de los riesgos físicos de seguridad de la información y la calidad de servicio sí es significativa en la UTEA, Abancay 2021.

Tabla 15

Asociación del riesgo técnico y la calidad de los servicios en la universidad

Correlaciones			
		Riesgos técnicos	Calidad de los servicios en la universidad
Riesgos técnicos	Correlación de Pearson	1	,153**
	Sig. (bilateral)		,004
	N	359	359
Calidad de los servicios en la universidad	Correlación de Pearson	,153**	1
	Sig. (bilateral)	,004	
	N	359	359

Fuente: Elaboración propia, SPSS V. 25, datos obtenidos de los instrumentos

Análisis e interpretación

A partir de la tabla 15, se plantea la Hipótesis estadística; Hipótesis nula (Ho) e Hipótesis alterna (Ha), sosteniendo que:

Ho: La asociación entre los riesgos técnicos de seguridad de la información con la calidad de servicio no es significativa en la UTEA, Abancay 2021.

Ha: La asociación entre los riesgos técnicos de seguridad de la información con la calidad de servicio sí es significativa en la UTEA, Abancay 2021

Con nivel de significancia de: α=0,05.

Coeficiente de correlación r de Pearson: 0.153**.

Donde el valor *p* calculado: p= 0.004

Conclusión de la hipótesis específica segunda: En vista que *p*-valor o Sig. bilateral 0.004<0.05 (nivel de significancia), de donde la hipótesis nula (Ho) se rechaza, admitiendo la hipótesis alterna (Ha), pudiendo concluir que la asociación de los riesgos técnicos de seguridad de la información y la calidad de servicio sí es significativa en la UTEA, Abancay 2021.

Tabla 16

Asociación del riesgo organizativo y la calidad de los servicios en la universidad

Correlaciones			
		Riesgos organizativos	Calidad de los servicios en la universidad
Riesgos organizativos	Correlación de Pearson	1	,104*
	Sig. (bilateral)		,050
	N	359	359
Calidad de los servicios en la universidad	Correlación de Pearson	,104*	1
	Sig. (bilateral)	,050	
	N	359	359

Fuente: Elaboración propia, SPSS V. 25, datos obtenidos de los instrumentos

Análisis e interpretación

En consideración a la tabla 16, se plantea la Hipótesis estadística; Hipótesis nula (Ho) e Hipótesis alterna (Ha), manifestando que:

Ho: La asociación entre los riesgos organizativos de seguridad de la información con la calidad de servicio no es significativa en la UTEA, Abancay 2021.

Ha: La asociación entre los riesgos organizativos de seguridad de la información con la calidad de servicio sí es significativa en la UTEA, Abancay 2021.

Con nivel de significancia de: α=0,05.

Coeficiente de correlación r de Pearson: 0.104*.

Donde el valor *p* calculado: p= 0.050

Conclusión de la hipótesis especifica tercera: En vista que *p*-valor o Sig. bilateral 0.050=0.05 (nivel de significancia), por cuanto la hipótesis nula (Ho) es rechazada y admitida la hipótesis alterna (Ha), pudiendo concluir que la asociación de los riesgos organizativos de seguridad de la información y la calidad de servicio sí es significativa en la UTEA, Abancay 2021.

CONCLUSIONES

Primera.- Que el grado de concordancia de los riesgos de seguridad de la información y la calidad de servicio sí es significativo positivo moderado en la UTEA, Abancay 2021, basado en la correlación *r* de Pearson de 0.160** y el *p*-valor logrado α=0.002 siendo inferior al error del 5.0% (Sig. bilateral α=0.002 < 0.05), escenario presente por los entornos físicos, técnicos y organizativas de los RSI en la entidad, las mismas que se encuentran concordantes con la empatía, la confianza, los componentes palpables, el potencial de respuesta y seguridad de la CS académicos-administrativos que perciben los usuarios discentes a lo largo de sus formación profesional.

Segunda.- Que la asociación entre los riesgos físicos de SI con la calidad de servicio sí es significativa positiva moderada en la UTEA, Abancay 2021, a partir de la prueba *r* de Pearson 0.126* y cuyo *p*-valor es α=0.017 es inferior al error 0.05 (Sig. bilateral α=0.017 < 0.05), circunstancias manifestadas por los adecuados riesgos físicos de la SI, en sus niveles de protección del perímetro, el acondicionamiento de las instalaciones, antiincendios e inundaciones, así como las cámaras de videovigilancia para monitorear y evitar ingresos no concedidos y deterioros a las dependencias, la tecnología y datos de universidad, anidadas de forma directa con las instalaciones físicas, atractivas, pertinentes, así como los equipos tecnológicos y sistemas de información, los materiales que operan para la presentación del servicio a los usuarios uteinos en desarrollo académico.

Tercera.- Que la asociación entre los inseguridades técnicas de SI con la CS sí es significativa positiva y moderada en la UTEA, Abancay 2021, establecida por la correlación *de* Pearson que dio 0.153** además del *p*-valor fue α=0.004 que es menor al error 5% (Sig. bilateral α=0.004 < 0.05), escenario esgrimido por los regulares riesgos técnicos de la SI en la institución educativa superior, tales como los sistemas de resguardo de redes firewall o cortafuegos, el software antivirus y el cifrado de los datos para es resguardo de la subred de servicios frente a desafíos internos y externos, por las copias de seguridad que desarrollan salvaguardando la información procesada, almacenada y compartida en los archivos de sus bases de datos y perfiles de correos

electrónicos corporativos, que se encuentran relacionadas con las regulares respuestas brindadas a las expectativas esperadas, la promesa y demostración de los colaboradores, al estar preparados para sostener eficientemente a los problemas, interrogantes e inquietudes del estudiante al recibir un determinado servicio académico-administrativo en la universidad.

Cuarta.- Que la asociación entre riesgos organizativos de SI con la calidad de servicio sí es significativa moderada positiva en la UTEA, Abancay 2021, determinación realizada por *r* Pearson 0.104* y cuyo *p*-valor es α=0.050 donde es igual al error 0.05 (Sig. bilateral α=0.050 < 0.05), situación mostrada por los regulares riesgos organizativos de SI, en sus mecanismos para revisar los permisos concedidos a los interesados a los sistemas informáticos, las capacitaciones en políticas de seguridad diseñadas e implantadas para la concientización, salvaguardas en ciberseguridad y proteger la información de la universidad, en afinidad directa con los regulares servicios universitarios, en cuanto a los horarios de atención que ofrecen y brindan los colaboradores para responder a las expectativas esperadas y el comportamiento de los trabajadores para trasmitir empatía, seguridad y autoridad de organización de la prestación en beneficio y complacencia de los usuarios universitarios durante su permanencia académica.

RECOMENDACIONES

Primera.- Para el ápice universitario, dirección de administración y a los encargados de OTI de la UTEA, en vista que los fenómenos estudiados tiene relación significativa, deberán realizar un feedback efectivo e integral de todos sus procesos operacionales intrínsecos, donde exista un compromiso y apoyo práctico de la alta dirección, que permita desarrollar cambios y/o eliminación a nivel de los RSI, adecuando sus actividades a los principios de disponibilidad, integridad, confidencialidad y resiliencia para el resguardo de sus respectivas bases de datos, y poder garantizar el fortalecimiento de los procesos administrativos del servicio de calidad que debe ejecutar en beneficio de los discentes y docentes uteinos.

Segunda.- Para el personal administrativo y de los colaboradores de OTI de la UTEA, es necesario asentar estrategias de acción oportunas e integrales de los riesgos físicos de SI en concatenación directa a garantizar la calidad de servicio de la institución, implementando e implantando oportunamente medidas físicas para el mejoramiento continuo de las interferencias y daños de las instalaciones, la operatividad de las TIC, los procesos operativos de videovigilancia, el control y monitoreo de accesos físicos no autorizados a los servidores y terminales informáticas, que conlleve a la correcta adecuación y cambios en la CS de la Primera Casa Superior de Estudios de Apurímac.

Tercera.- Para los colaboradores de la unidad de administración y de OTI de la UTEA, es preciso establecer procesos de innovación dinámicos de inseguridades técnicas de SI que estén integrados al sostenimiento de la calidad de servicio de la entidad, permitiéndoles identificar riesgos, definir e implantar las medidas técnicas adecuadas para la mitigación de las mismas, de la asignación de funciones, responsabilidades, roles claros y planificados de equipos técnicos de seguimiento y procedimientos de resguardo para salvaguardar las bases de datos, los perfiles de correos electrónicos institucional y la construcción de aplicaciones tecnológicas e informáticas, donde las actividades de los servicios organizacionales puedan ejecutarse en beneficio y complacencia de los operadores y clientes de la entidad universitaria.

Cuarta.- Para la autoridad académica, de investigación, de la unidad de administración, docentes, talento humano de OTI, estudiantes de la UTEA, organizaciones privadas y públicas, los investigadores y personas interesadas en la problemática estudiada, tienen el deber de ahondar los fenómenos cultivados en futuras investigaciones con la finalidad de identificar los riesgos, puntualizar e implementar las medidas organizativas adecuadas, estableciendo canales de comunicación continua y de concientización entre el talento humano de las unidades académicas-administrativas y los responsables de seguridad de OTI, para la adecuación de las políticas de ciberseguridad organizacional, la capacidad de identificar el nivel de seguridad adaptable a la información que procesa, almacena, maneja y comparte entre los usuarios, en busca de los cambios innovadores en la CS que otorga la entidad superior de estudios.

ASPECTOS ADMINISTRATIVOS

Recursos: Potencial humano

- Br. PEDRO MIGUEL CHIRINOS PALOMINO; de la Escuela Profesional de Ingeniería de Sistemas e Informática, FI, UTEA, Abancay.
- Los asesores metodológico y temático del estudio.
- Colaboradores de la oficina de tecnología de la información (OTI) y Subdirección de centro de cómputo e informática (CCI) de la UTEA, Abancay.
- Discentes de las escuelas profesionales de la UTEA, Abancay.

Recursos materiales

- Una laptop.
- Una impresora.
- Flas memory (USB).
- Servicio de internet.
- Libros y textos físicos y digitales.
- Trabajos de investigación.
- Fotocopias.
- Hojas bond 80 gr.
- Impresiones.
- Empastados.
- Servicio de movilidad interna.
- Otros.

Cronograma de actividades

Nº	ACTIVIDADES	CRONOGRAMA AÑO 2021																				RESPONSABLES
		Junio				Julio				Agosto				Setiembre				Octubre				
1	Planteamiento y construcción del problema de investigación.																					Tesista - Asesor.
2	Diseño, analisis y confección del marco teórico.																					Tesista - Asesor.
3	Redacción y confección del proyecto de tesis.																					Tesista - Asesor.
4	Anaillado, presentación y aprobación del proyecto de tesis.																					Tesista - Dictaminantes
5	Análisis, diseño y construcción de instrumentos de recolección de datos.																					Tesista - Asesor y Expertos.
6	Ejecución y administración de los instrumentos de recolección de datos, (virtual)																					Tesista - unidades de anáisis.
7	Procesamiento, análisis e interpretación de resultados.																					Tesista - Asesor.
8	Redacción y transcripción de la tesis.																					Tesista - Asesor.
9	Anillado y empastado de la tesis.																					Tesista - Imprenta.
10	Emisión, presentación y aprobación de la tesis.																					Tesista - Asesor.
11	Dictaminación de la tesis.																					Jurado dictaminador.
12	Sustentación y Aprobación del Grado.																					Tesista - Jurado Grado Académico.

Presupuesto y financiamiento

Presupuesto

Está estimado en virtud a la realidad latente que en el país se encuentra atravesando a consecuencia del COVID-19, para el cual se consideró los recursos económicos siguientes:

N°	Componentes	Partidas	Unidad de Medida	Costo Unitario	Costo Total (S/.)
1	Análisis, diseño y construcción del tema y problema de investigación.	Libros, revistas y servicio de biblioteca e internet.	Global	150	150.00
2	Análisis y construcción del marco teórico.	Libros, revistas, textos y servicio de internet	Global	250	250.00
3	Composición y revisión del proyecto de Tesis.	Desarrollo, procesamiento e impresión.	Global	700	700.00
4	Análisis, diseño y confección de instrumentos de recolección de datos.	Laptop, servicio de internet e impresiones.	Global	250	250.00
5	Aplicación y administración de los instrumentos de recolección de datos (virtual)	Impresión y fotocopiado de las encuestas	Global	200	200.00
6	Tabulación, procesamiento, análisis e interpretación de resultados.	LapTop, digitación y almacenamiento.	Global	700	700.00
7	Redacción y transcripción y revisión de la Tesis.	Computadora personal, digitación, almacenamiento e impresiones.	Global	500	500.00
8	Anillado y empastado de la Tesis.	Servicio de impresión de la Tesis.	Global	150	150.00
9	Emisión, presentación de la Tesis.	Empastados finales de la Tesis.	Global	200	200.00
10	Sustentación de la Tesis.	Inversión en la Carpeta de Grado (Derechos Académicos).	Global	2,000.00	2,000.00
11	Transporte y movilidad interna y externa.	Servicio de taxi urbano y rural.	Global	150	150.00
12	Asesoramiento externo.	Desarrollo de la Tesis	Global	2,000.00	2,000.00
13	Materiales fungibles	Varios	Global	300	300.00
14	Imprevistos 4 %.	Para cubrir eventualidades.	Global	302	302.00
TOTAL				S/. 7,576.40	S/. 7,576.40

Financiamiento

El financiamiento fue cubierto por el ejecutor del presente estudio.

BIBLIOGRAFÍA

Álvarez-Beltrán E.L. (2017). La gestión documental frente al reto de las tecnologías de la información y comunicación, como vía para lograr adentrarse en información y comunicación, como vía para lograr adentrarse en el proceso de innovación tecnológica de los archivos en Colombia el proceso de innovación tecnológica de los archivos en Colombia. [Internet]; [Consultado el 03/05/2022] y disponible en: https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1139&context=sistemas_informacion_documentacion

Ángel, Hugo A. (2020). ¿Por qué se debe gestionar el riesgo de seguridad en la información?. [Internet]; [Consultado el 28/02/2021] y disponible en: https://www.piranirisk.com/es/blog/por-que-se-debe-gestionar-el-riesgo-de-seguridad-en-la-informacion

Arias-Gonzáles JL. (2020). Técnicas e instrumentos de investigación científica. [Internet]; [Consultado el 15/07/2021] y disponible en: www.cienciaysociedad.org

Arteaga G. (2020). Enfoque cuantitativo: métodos, fortalezas y debilidades. [Internet]; [Consultado el 07/02/2021] y disponible en: https://www.testsiteforme.com/enfoque-cuantitativo/

Bastis Consultores (2022). Cómo calcular el tamaño de la muestra correctamente. [Internet]; [Consultado el 12/04/2022] y disponible en: https://online-tesis.com/como-calcular-el-tamano-de-la-muestra-correctamente/

Brito P. (2014). Método analítico-deductivo. [Internet]; [Consultado el: 12/06/2022] y disponible en: https://metodologiaecs.wordpress.com/2014/03/18/metodo-analitico-deductivo/

Calderón R., Viviana P. (2015). Análisis de riesgos informáticos y desarrollo de un plan de seguridad de la información para el gobierno autónomo descentralizado municipal de Catamayo. [Internet]; [Consultado el 02/02/2021] y disponible en:

http://dspace.unl.edu.ec:9001/jspui/bitstream/123456789/11295/1/Calder%C3%B3n%20Ramos%2C%20Viviana%20Patricia.pdf

Camapaza-Quispe, AA. (2019). Diseño del plan de seguridad informática basado en la ntp iso/iec 27001:2014 para la municipalidad del centro poblado de Salcedo – Puno. [Internet]; [Consultado el 12/07/2021] y disponible en: https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/3468/Abdon_Tesis_bachiller_2019.pdf?sequence=1&isAllowed=y

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (2015). Manual: Para la Evaluación de Riesgos originados por Fenómenos Naturales. [Internet]; [Consultado el 20/03/2021] y disponible en: https://www.cenepred.gob.pe/web/wp-content/uploads/Guia_Manuales/Manual-Evaluacion-de-Riesgos_v2.pdf

Cerf V. (2022). Prácticas comunes de interconexión y tarificación de redes de Internet. [Internet]; [Consultado el 07/01/2022] y disponible en: https://www.internetsociety.org/es/blog/2022/04/practicas-comunes-de-interconexion-y-tarificacion-de-redes-de-internet/

Comisión Económica para América Latina y el Caribe (2021). Tecnologías digitales para un nuevo futuro". Publicación de las Naciones Unidas LC/TS.2021/43. Distribución: L Copyright © Naciones Unidas, [Internet]; [Consultado el 12/08/2022] y disponible en: https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf

Ciberseguridad (2020). Sistema de Gestión de Seguridad de la Información. [Internet]; [Consultado el 18/03/2021] y disponible en: https://ciberseguridad.com/normativa/espana/sgsi/

Deloitte (2016). Los riesgos de la tecnología de la información en los servicios financieros: Lo que los miembros de junta necesitan saber – y hacer. [Internet]; [Consultado el 05/02/2021] y disponible en: https://www2.deloitte.com/

content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf

Domènech-Meritxell O. (2017). Riesgos en la seguridad de la información de la empresa. [Internet]; [Consultado el 05/03/2021] y disponible en: https://www.iniseg.es/ blog/ciberseguridad/ riesgos-en-la-seguridad-de-la-informacion-de-la-empresa/

Fajardo D., Carmen E. (2017). Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental lider en el mercado colombiano. [Internet]; [Consultado el 06/01/2021] y disponible en: https://alejandria.poligran.edu.co/ bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1

Gonzales C., Omar G. (2017). Calidad de servicio y satisfacción de los estudiantes usuarios con la atención administrativa en la facultad ciencias contables y administrativas, UNA-Puno, 2017. [Internet]; [Consultado el 04/03/2021] y disponible en: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6445/Gonzales_Cornejo_Omar_Gustavo.pdf?sequence=1&isAllowed=y

Hernández-Sampieri R., Fernández-Collado C. y Baptista-Lucio, P. (2014). Metodología de la investigación, sexta edición. Editorial McGraw-Hill Interamericana. México.

Huaura M., MH. (2019). Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones. [Internet]; [Consultado el 04/03/2021] y disponibilidad en: http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/11225/Huaura_mm. pdf?sequence=1&isAllowed=y

IBM (2021). Privilegios de usuario. [Internet]; [Consultado el 07/08/2021] y disponible en: https://www.ibm.com/docs/es/rational-clearquest/9.0.1?topic=accounts-user-privileges

IBM (2021a). Claves privadas, claves públicas y certificados digitales. [Internet]; [Consultado el 07/08/2021] y disponible en: https://www.ibm.com/docs/es/sia?topic=SSIGMP_1.0.0/com.ibm.itim_pim.doc/nov/install_config/c_adk_cert_keys_and_certs_ins.html

Instituto Nacional de Ciberseguridad (2019). ¿Qué hace un antivirus para detectar el malware?. [Internet]; [Consultado el 08/03/2021] y disponible en: https://www.incibe.es/empresas/blog/hace-antivirus-detectar-el-malware

Instituto Nacional de Ciberseguridad (s.f.). Protección de la información. Colección: protege tu empresa. [Internet]; [Consultado el 06/03/2021] y disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Institución Universitaria Politécnico Gran Colombiano (2016). Teoría de la Seguridad. Principios de la seguridad de la información. Bogotá-Colombia.

IsoTools Excellence (2019). Gestión de riesgos de seguridad de la información. Un aspecto clave en las organizaciones actuales. [Internet]; [Consultado el 06/03/2021] y disponible en: https: //www.isotools.org/2019/08/20/gestion-de-riesgos-de-seguridad-de-la-informacion-un-aspecto-clave-en-las-organizaciones-actuales/

Kendall KE. y Kendall JE. (2011). Análisis y diseño de sistemas. Pearson Educación. 8va. Edición. México. Pp. 600.

Larrea, P. (1991). Calidad de Servicio. Díaz de Santos. Madrid, España

Ld grupo (2019). Qué es el riesgo de Seguridad de información. [Internet]; [Consultado el 06/03/2021] y disponible en: https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/

Machicao M., Saulo G. (2019). Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) –UNA Puno 2018. [Internet]; [Consultado el 03/03/2021] y disponible: http://repositorio.unap.edu.pe/

bitstream/handle/UNAP/13958/Machicao_Mollocondo_Saulo_Gustavo.pdf?sequence=1&isAllowed=y

Maquera M. y Galindo Y. (2022). Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya. [Internet]; [Consultado el 25/05/2022] y disponible en: https://repositorio.upt.edu.pe/bitstream/handle/20.500.12969/2524/Maquera-Mamani-Galindo.pdf?sequence=1&isAllowed=y

Matsumoto-Nishizawa R. (2014). Desarrollo del Modelo Servqual para la medición de la calidad del servicio en la empresa de publicidad Ayuda Experto. [Internet]; Revista Perspectivas versión impresa ISSN 1994-3733 Perspectivas n.34 Cochabamba oct. 2014. [Consultado el 25/05/2022] y disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1994-37332014000200005

Melara M. (2017). La relación entre calidad de servicio y satisfacción del cliente. [Internet]; [Consultado el 22/02/2021] y disponible en: https://marlonmelara.com/ la-relacion-entre-calidad-de-servicio-y-satisfaccion-del-cliente/

Mendez-N. ML. (2022). Diseño de un sistema de gestión de seguridad de información para proteger los activos de información del servicio de administración tributaria de la zona norte del Perú. [Internet]; [Consultado el 23/05/2022] y disponible en: https://repositorio.upn.edu.pe/bitstream/handle/11537/30611/Mendez%20Navarro%20Miryam%20Liliana.pdf?sequence=1&isAllowed=y

Molina-T., OD. (2014). Calidad de los Servicios. [Internet]; [Consultado el 01/03/2021] y disponible en: https://www.ecured.cu/Calidad_de_los_Servicios

Mujica M. y Álvarez Y. (2009). El Análisis de riesgo en la seguridad de la información. [Internet]; [Consultado el 25/02/2021] y disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiFn9njyfvvA

hUrH7kGHXJADdYQFjABegQIAhAD&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6505355.pdf&usg=AOvVaw09SBKOPeXOAxazQxxyxElO

Narvaez M. (2019). Investigación básica: Qué es, ventajas y ejemplos. [Internet]; [Consultado el 03/04/2022] y disponible en: https://www.questionpro.com/blog/es/investigacion-basica/

Ortega Cr. (2022). ¿Cómo realizar un muestreo aleatorio simple?. [Internet]; [Consultado 14/04/2022] y disponible en: https://www.questionpro.com/blog/es/como-realizar-un-muestreo-aleatorio-simple/

Pacheco D. y Rodríguez R. (2019). Las TIC como estrategia competitiva en la gestión empresarial. [Internet]; [Consultado el 05/03/2022] y disponible en: https://www.redalyc.org/journal/6219/621968062004/html/

Parasuraman A., Ziethaml V. y Berry LL. (1988). SERVQUAL: A Multiple- Item Scale for Measuring Consumer Perceptions of Service Quality' Journal of Retailing, Vo. 62, N°. 1, pp 12-40.

Parra A. (2022). Muestro tipo intencionado. [Internet]; [Consultado el 14/04/2022] y disponible en: https://www.questionpro.com/blog/es/muestreo-intencional/

Pilla-Y., JC. (2019). Diseño de una política de seguridad de la información para el área de tecnología de la información de la cooperativa de ahorro y crédito Chibuleo Ltda., basado en la norma ISO/IEC 27002:2013. [Internet]; [Consultado el 21/06/2021] y disponible en: https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%C3%91O%20DE%20UNA%20POL%C3%8DTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20PARA%20EL%20%C3%81REA%20DE%20TECNOLOG%C3%8DA%20DE%20LA%20INFORMACI%C3%93.pdf

Quispe L. JE., Pacheco-P DL. (2018). Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 27005 para analizar la viabilidad de

adoptar un servicio en la nube. [Internet]; [Consultado el 03/03/2021] y disponible en: https://repositorioacademico.upc.edu.pe/handle/10757/625879

Rodiguez I. (2014). ¿Qué es el riesgo, riesgo inherente y riesgo residual?. [Internet]; [Consultado el 27/01/2021] y disponible en: https://www.auditool.org/blog/control-interno/que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

Rodríguez-A. JH., Torres-C. WA. (2019). Análisis de riesgos de seguridad de la información del área it de la empresa royal services S.A. Consultado el 02/03/2021 y disponible en: https://repository.ucatolica.edu.co/ bitstream/10983/23389/1/ANALISIS%20DE%20RIESGOS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION%20DEL%20AREA%20IT%20DE%20LA%20EMPRESA%20ROYAL%20SERVICES%20S.A.pdf

Romero O. MA. (2015). Tecnologías de la información y la comunicación: conceptos básicos. [Internet]; [Consultado el 13/02/2021] y disponible en: https://es.slideshare.net/ miguelaromero5099/tecnologias-de-la-informacion-y-la-comunicacion-conceptos-basicos

Royal F. (1988). Seguridad en los sistemas informáticos. Madrid, España: Díaz de Santos, S.A

Ruiz-Mitjana L. (2019). Alfa de Cronbach (α): qué es y cómo se usa en estadística. [Internet]; [Consultado el 25/05/2022] y disponible en: https://psicologiaymente.com/miscelanea/alfa-de-cronbach

SAP Concur (2022). Gestión de riesgos: ¿Qué es y cuáles son sus objetivos?. [Internet]; [Consultado el 05/012/2022] y https://www.concur.pe/news-center/gestion-del-riesgo-objetivos

Schiavonne-Hurtado CF. (2022). Propuesta de mitigación de riesgos en el sistema facturación de la empresa pale consultores haciendo uso de la adaptación de las metodologías pentesting standart y nist-sp 800-30-2022. [Internet]; [Consultado el 15/07/2022] y disponible en:

https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4586/Carlos_Tesis_bachiller_2021.pdf?sequence=1&isAllowed=y

Sistemas de GC - ISO (2019). Calidad en el servicio al cliente. [Internet]; [Consultado el 12/03/2021] y disponible en: https://abc-calidad.blogspot.com/2011/05/calidad-de-los-servicios.html

Sullivan P. (2016). Gestión de riesgos de seguridad de la información: Comprensión de los componentes. [Internet]; [Consultado el 16/02/2021] y disponible en: https://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de seguridad-de-la-informacion-Comprension-de-los-componentes

Unidad Nacional para la Gestión del Riesgo de Desastres (2019). Análisis del Riesgo. [Internet]; [Consultado el 20/02/2021] y disponible en: https://portal.gestiondelriesgo.gov.co/Documents/Conocimiento/Conocimiento-In-Analisis-del-Riesgo.pdf

Universidad Tecnológica de los Andes (2019). Información Institucional. [Internet]; [Consultado el 03/02/2021] y disponible en: https://utea.edu.pe/institucional/

Vaca-E. PN. (2019). Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador. [Internet]; [Consultado el 21/06/2021] y disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/30565/1/Tesis_t1650msi.pdf

Vázquez-C. J. (2020). Calidad en el Servicio. Encuesta de cinco dimensiones. (SERVQUAL). [Internet]; [Consultado el 05/03/2021] y disponible en: https://www.inbox.mx/blog/calidad-en-el-servicio-encuesta-de-cinco-dimensiones-servqual