UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSTGRADO

MODELO DE GESTIÓN DE RIESGOS DE TI BASADOS EN ESTÁNDARES ADAPTADOS A LAS TI QUE SOPORTAN LOS PROCESOS PARA CONTRIBUIR A LA GENERACIÓN DE VALOR EN LAS UNIVERSIDADES PRIVADAS DE LA REGIÓN LAMBAYEQUE

AUTORES:

Arangurí García María Ysabel
Iman Espinoza Ricardo David
León Tenorio Gregorio Manuel

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

Chiclayo, Perú 2016

MODELO DE GESTIÓN DE RIESGOS DE TI BASADOS EN ESTÁNDARES ADAPTADOS A LAS TI QUE SOPORTAN LOS PROCESOS PARA CONTRIBUIR A LA GENERACIÓN DE VALOR EN LAS UNIVERSIDADES PRIVADAS DE LA REGIÓN LAMBAYEQUE

POR

Arangurí García María Ysabel
Iman Espinoza Ricardo David
León Tenorio Gregorio Manuel

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADO POR

_____
Mgtr. Marco Agustín Arbulú Ballesteros
Presidente de Jurado

_____
Mgtr. Jury Yesenia Aquino Trujillo
Secretaria de Jurado

_____
Mgtr. Juan Dávila Ramírez
Vocal/Asesor de Jurado

CHICLAYO, 2016

Dedicatoria:

A nuestras familias, por su apoyo y comprensión en este arduo proceso.

Epígrafe

A la sobriedad en las costumbres le debe corresponder la moderación en las actitudes, la tolerancia en el trato, la honradez en el comportamiento y la exigencia para contigo mismo.

San Agustín

Agradecimientos:

A nuestro asesor Mgtr. Juan Dávila Ramírez, por su apoyo en el desarrollo de este proyecto, brindándonos sus recomendaciones y experiencia profesional.

ÍNDICE

RESUMEN

La presente investigación centra su estudio en la necesidad de incluir la gestión de riesgos de tecnologías de la información (TI) en las universidades privadas de la región Lambayeque, el diagnóstico aplicado a una muestra de seis sobre once universidades detectó que estas no implementan gestión de riesgos o no la implementan de una manera efectiva, además determinó que los conceptos de gestión de riesgos de TI no son conocidos a nivel de la gerencia de TI, condicionando una respuesta reactiva ante situaciones adversas en los servicios importantes soportados por TI, con la posibilidad de generar pérdidas económicas y deterioro de imagen ante la comunidad universitaria.

Se planteó como objetivo general: contribuir a la generación de valor en los procesos académicos y administrativos soportados por TI en las universidades privadas de la región, formulando un modelo de gestión de riesgos de TI basados en metodologías y estándares adaptados, que posea características de simplificación de procesos y flexibilidad adaptadas al contexto de las universidades.

El modelo se validó por juicio de expertos midiendo su confiabilidad aplicando el alfa de Cronbach y la concordancia de su contenido en base a Kendall.

El modelo validado se aplicó a un caso de estudio para una universidad privada de la región, identificando 73 riesgos, siendo 11 categorizados como alta prioridad en base a la valoración de su apetito y tolerancia, se plantearon estrategias de tratamiento con 5 proyectos aplicados a monitorear y revisar que la gestión de riesgos logra contribuir a la generación de valor.

ABSTRACT

This research focuses its study on the need to include IT risk management in private universities of the Lambayeque region. The diagnosis applied to a sample of six of the eleven universities in the region found that these ones do not implement risks management or at least they do not implement it effectively, in addition it was determined that the concepts of IT risk management are not known at the level of IT management which determines a reactive response face to adverse situations in the important services supported by IT, with the possibility to generate economic and image loss in front of the university community.

The research had as a main purpose to contribute to value creation in academic and administrative processes supported by IT in private universities in the region, developing an IT risk management model based on methodologies and adapted standards, having simplification processes characteristics and flexibility adapted to the context of universities.

The model was validated by expert judgment measuring reliability using Cronbach's alpha as well as the consistency of its content based on Kendall.

The validated model was applied to a case study for a private university in the region identifying 73 risks 11 of which were categorized as high priority based on the assessment of their appetite and tolerance. Treatment strategies were raised with five projects intended to monitor and check that risk management does contribute to value creation.

INTRODUCCIÓN

En el presente trabajo de investigación se propuso un modelo de gestión de riesgos aplicado en las universidades privadas.

A pesar que existen diversos estándares de gestión de riesgos que definen modelos de trabajo, no tratan directamente un contexto académico universitario.

En el contexto de las universidades privadas, se reconoce la importancia de las tecnologías de información (TI) para mejorar los procesos, sin embargo, como resultado de la realidad problemática analizada en las universidades privadas, éstas no han dimensionado la necesidad de una efectiva gestión de riesgos, dado que no se presenta una guía estructurada aplicada al contexto que establezca procedimientos claros, sea por desconocimiento, ausencia de conocimiento, o no se aplican los conceptos de gobierno y gestión de riesgos para valorar de manera precisa los costos de reposición, reparación o administración de recursos de TI.

En el contexto internacional, las organizaciones que manifiestan alta rentabilidad, consideran a las TI como el soporte de sus transacciones para dar una respuesta efectiva a la continuidad de los procesos. Además, están convencidas que la administración de riesgo empresarial es un proceso realizado por el consejo directivo, la administración y el personal.

También afirman que la administración de riesgos debe ser aplicado en el establecimiento de estrategias de toda la empresa, diseñada para identificar eventos potenciales que puedan afectar a la entidad y administrar los riesgos

para proporcionar una seguridad e integridad razonable referente al logro de objetivos. Según Romeral (2008), en el entorno competitivo actual, la posesión de tecnología no supone por sí misma una ventaja competitiva para las empresas, es la gestión de las tecnologías la que puede hacer la diferencia, pero con especial énfasis en la gestión de los riesgos derivados de su uso. ISO 31000:2009, menciona que para un efectivo gobierno empresarial, se debe tener como base los conceptos de calidad alineado al mismo.

La gestión de riesgos contribuye con la generación de valor, minimizando los costos de afrontar situaciones adversas que amenazan los procesos de negocio, evitando tomar decisiones reactivas no planificadas para superar estas situaciones.

Los riesgos, están presentes en todas las actividades organizacionales, pero cuando algún evento que amenace el logro de los objetivos de la organización se manifiesta, no se debe improvisar posibles soluciones. La gestión de riesgos tiene por finalidad detectar oportunamente los riesgos organizacionales que puedan afectar la generación de valor, generando estrategias para controlar fuentes de riesgos antes que ocurra, al identificar los riesgos de manera oportuna este puede convertirse en una ventaja estratégica en el sector. La gestión de riesgos provee beneficios a la organización: Hace la organización más segura, siendo consciente de sus riesgos, logra la mejora continua de sus procesos internos, aprovecha oportunidades de negocio y da estabilidad a la organización en un entorno cambiante.

En el análisis de la situación problemática de las universidades privadas de la región Lambayeque, se identificó que:

- En la evaluación del gobierno de TI, se desconocen los riesgos de TI, relacionados a la entrega de resultados, pudiendo generar costos no previstos en el ciclo de vida de los activos, lo que ha provocado la aparente falta de transparencia en la propuesta de inversión en la organización y discrepancias entre lo presupuestado al inicio del ciclo de vida del activo y el costo total de propiedad al finalizar el mismo.

- La gestión de riesgos no se implementa o se implementa de manera empírica, tomando decisiones de última hora para afrontan situaciones adversas, generando pérdidas de productividad por interrupción de servicios por periodos que pueden ir desde un día (cuando los materiales de repuesto existen en el mercado local/nacional), hasta varias semanas (si los materiales existen en mercados internacionales).

- No se tiene claro cuáles son los procesos de negocio soportado por TI que son afectados cuando un riesgo se materializa sobre los activos de TI.

En base a la realidad problemática descrita en el apartado anterior, se planteó la siguiente pregunta ¿De qué manera se podría contribuir a la generación de valor de los procesos de negocio soportados por TI en las Universidades Privadas de la Región Lambayeque?

Para proponer una alternativa de solución, desde la perspectiva tecnológica se buscó gestionar de forma efectiva los riesgos, reconociendo y dimensionando el impacto que puedan tener sobre los procesos, actividades de negocio, así como en la infraestructura de TI, para potenciar la capacidad de respuesta inmediata en la continuidad del servicio brindado.

Desde el punto de vista económico se define que el modelo permitió gestionar los riesgos de TI asegurando la continuidad de los procesos, sin afectar las operaciones económicas y operativas en las Universidades Privadas de la Región Lambayeque, haciendo los riesgos más visibles, permitiendo adoptar acciones de prevención, generando la aprobación y compromiso de los directivos. Desde el punto de vista científico, se planteó el diseño de contrastación pre test en la etapa diagnóstica - de post test validando el Modelo de Gestión de Riesgos de TI desarrollado, adaptado a los estándares requeridos, se formuló la elaboración y posterior evaluación basado en indicadores, como el nivel de integración, nivel económico, índice de impacto, y nivel de capacidad de respuesta frente a un riesgo materializado en las Universidades Privadas de la Región Lambayeque, probado en el caso de estudio de una Universidad Privada de la Región.

Con respecto a la justificación social, el modelo permitió brindar información a los miembros de la alta dirección de cada institución sobre la importancia de desarrollar una efectiva gestión de riesgos, para contribuir en la generación de valor. La gestión de riesgo contribuye en la continuidad, eficiencia y eficacia de los procesos, generando satisfacción por los servicios recibidos, promoviendo la mejora constante, que surge de las necesidades propias del giro del negocio y no por las amenazas o vulnerabilidades que surjan por una equívoca gestión de las TI.

Teniendo como referencia lo anteriormente expuesto se plantea la hipótesis: Con la implementación de un modelo de gestión de riesgos de Tecnologías de Información basado en estándares adaptados a las TI, que soportan los procesos de negocio se contribuye a la generación de valor en las Universidades Privadas de la Región Lambayeque.

De la hipótesis se desprende la variable Independiente definida como Modelo de Gestión de Riesgos de Tecnologías de Información basado en estándares adaptados a las TI que soportan los procesos. Como variable Dependiente se propuso contribuir a la generación de valor en las Universidades Privadas de la región.

INDICADOR	DESCRIPCIÓN	INSTRUMENTO	OPERACIONALIZACIÓN
Número de riesgos detectados por proceso de negocio	Aumentar el número de riesgos detectados por proceso de negocios para una oportuna toma de decisiones	Ficha de monitoreo y revisión	Número de riesgos detectados por procesos de negocio después de la aplicación del modelo - Número de riesgos detectados por procesos de negocio antes de la aplicación del modelo
Nivel porcentual de actitud proactiva respecto al nivel de impacto en los procesos de negocio afectados	Incrementar el nivel porcentual de actitud proactiva respecto al nivel de impacto en los procesos afectados como resultado de la gestión de riesgos de TI en la institución.	Encuesta	Nivel porcentual de actitud proactiva después de la aplicación del modelo – Nivel porcentual de actitud proactiva antes de la aplicación del modelo
Número de proyectos propuestos de gestión de riesgos.	Incrementar el número de proyectos de gestión de riegos propuestos a partir de la aplicación de modelo.	Ficha de proyecto	Número de proyectos propuestos de gestión de riesgos después de la aplicación del modelo – Número de proyectos propuestos de gestión de riesgos antes de la aplicación del modelo

Tabla 1: Indicadores y operacionalización de variables

Objetivo General:

Contribuir a la generación de valor en las universidades privadas de la región, a través de la implantación del modelo de Gestión de Riesgos basado en estándares adaptados a las TI que soportan los procesos de negocio.

Objetivos Específicos:

- Aumentar el número de riesgos detectados por proceso de negocio, para disminuir la frecuencia de interrupción de los procesos, generando información oportuna para la toma de decisiones,
- Incrementar el nivel porcentual de actitud proactiva respecto al nivel de impacto en los procesos afectados como resultado de la gestión de riesgos de TI en la institución, disminuyendo costos innecesarios.
- Incrementar el número de proyectos propuestos para el monitoreo y revisión periódica permitiendo una efectiva gestión de riesgos que promuevan decisiones de carácter proactivo.

CAPÍTULO I: MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes del problema

Según Romeral y Torres (2008), las tecnologías de la información tienen gran relevancia en el mercado y considera que los riesgos tecnológicos son un punto crítico por ser posibles desencadenantes de riesgos operacionales, por lo que propone que una efectiva gestión de riesgos es un proceso cíclico que incluye análisis y priorización de riesgos de manera periódica para asegurar la continuidad de los procesos.

La presente tesis, toma este antecedente como soporte a la propuesta que se plantea desde un aspecto empresarial, para adaptarlo en el ámbito educativo superior universitario, buscando establecer un modelo adaptado, que asegure en el soporte de tecnologías, la funcionalidad, eficiencia y eficacia permanente de los procesos académico - administrativos que contribuya a la generación de valor en las universidades privadas de la región.

DeMarco y Lister (2003) quienes argumentan que "Los sistemas vigentes que permiten cambiar el mundo conllevan muchos riesgos; sin embargo, el retorno de la inversión es enorme". Por lo que Pastor (2010) concluye en su investigación que cada uno debe saber cómo manejar el riesgo; para cuyo efecto, debe incluir en sus procesos, la manera de identificar las fuentes de riesgo, cuantificar los parámetros de riesgo y finalmente desarrollar planes, los cuales serían requeridos para manejar los mismos.

Este antecedente es una referencia para la presente investigación, en la medida que permita establecer la importancia de proponer un modelo que oriente a los stakeholders en la identificación de riesgos, valorar los parámetros adaptados al contexto de la educación superior universitaria con respecto a los procesos que son soportados por las tecnologías de información, así como los costos que significa el no gestionarlos correctamente.

La tesis Moncayo (2014), con el título "Modelo de evaluación de riesgos en activos de TIC's, para pequeñas y medianas empresas del sector automotriz", esta investigación hace una evaluación de las pequeñas y medianas empresas, reconociendo que no se conocen de forma clara los riesgos a la que está sometida su organización, parte de ellas aplican planes de contingencia a nivel empresarial, pero no cuantifican sus activos y el riesgo por cada uno de ellos. Por esta razón este antecedente propuso la creación de un modelo de evaluación de riesgos, basado en las metodologías Magerit, Octave y normas NIIF (Normas Internacionales de Información Financiera), el mismo que aportó a las empresas una manera de obtener información sobre los riesgos, amenazas, y protecciones que se deben considerar para evitar y tomar medidas de prevención oportunas y adecuadas.

Con respecto a este antecedente, permite evaluar un modelo aplicado a pequeñas y medianas empresas, siendo las universidades de la región encajadas en la clasificación de mediana empresa, facilitando parámetros de medición que podrían ser aplicados en el modelo propuesto.

Es importante medir el impacto económico derivado de la caída de servicios de TI. Algunos de los factores que permiten medir este impacto son: Costos de Inactividad de los empleados o pérdidas por productividad, pérdidas por detención de las operaciones, incumplimiento de acuerdos de nivel de servicios (SLA) y el impacto en la marca por pérdida de confianza.

Las organizaciones cada vez son más conscientes de los impactos que les pueden generar los riesgos referentes a las TI. Es frecuente que empresas de diversos sectores económicos reporten pérdidas debido a fallas o ataques sobre sus servicios de TI que afectan seriamente su reputación.

En este artículo se muestra estándares y normas que se debe considerar al realizar un análisis de riesgos, posteriormente explicó cómo utilizar una metodología y la articulación en el proceso de gobernabilidad de TI para desarrollar en forma exitosa este tipo de iniciativas.

En el artículo de investigación denominado "Metodología y gobierno de la gestión de riesgos de tecnologías de la información" escrito por Gómez (2011), se realizó un análisis de cómo las organizaciones son cada vez más conscientes de los impactos que les pueden generar los riesgos referentes a las TI, dado que las empresas de diversos sectores económicos han reportado pérdidas debido a fallas y/o ataques sobre sus servicios de TI, los cuales han afectado su reputación y su solidez financiera como consecuencia de los mismos. Según este análisis existen dos pilares fundamentales para realizar el análisis de riesgos: los estándares y normas, de un lado, y las metodologías adecuadas a cada negocio, de otro; los cuales por sí mismos no aseguran el éxito, sino la articulación de estos en el contexto de la aplicación que se desea analizar.

En este artículo se deja en claro que la gestión de riesgos, no es la panacea a las necesidades de la organización, ya que siempre existirá un riesgo remanente y latente en sus procesos de misión crítica, sin embargo, no es suficiente dicha articulación si no se cuenta con un gobierno de TI que establezca en forma clara las directrices estratégicas para llevar en forma exitosa estos procesos de análisis de riesgos, que permitan establecer el liderazgo, la organización y la definición de los lineamientos a seguir, con miras a sostener sus procesos de misión crítica bajo una cultura organizacional.

1.2. Marco teórico conceptual

1.1.1. 2.1. Gobierno

Según Alfaro (2008) "*El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la*

toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas."

Según ISACA (2012), menciona que "*Durante la pasada década, el término "Gobierno" ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.*". Así también, menciona que las "*Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección tanto en funciones de negocio como de TI deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión*".

Analizando los conceptos previos se concluye que gobierno corporativo debe incluir a las tecnologías de la información como una herramienta estratégica para una efectiva toma de decisiones.

1.2.2. Gobierno corporativo

El gobierno corporativo, según ISACA (2009): "*es un conjunto de responsabilidades y prácticas usadas por la gerencia de una organización para proveer dirección estratégica; de ese modo, asegurando que las metas sean alcanzables, los riesgos sean tratados adecuadamente y los recursos organizacionales sean utilizados debidamente*".

1.2.3. Definiciones de gobierno de TI

Entre las definiciones más importantes se destaca:

Según ISACA (2009) *"El gobierno de TI es una estructura de relaciones y procesos utilizados para dirigir y controlar que la empresa alcance sus metas, dando valor agregado mientras balancea el riesgo en comparación al rendimiento en lo que respecta a TI y sus procesos".*

Según la Asociación Española de Empresas de Tecnologías de Información, AEETI (2005), la norma ISO/IEC 38500, define el

gobierno de TI como: *"El sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información", distinguiéndose de la Gestión de TI, definida como "El sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización, sujeto a la guía y monitorización establecidas mediante el gobierno corporativo".*
Según el ISACA, COBIT (2012), lo define como: *"Un enfoque de gobierno que garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la empresa y la consecución de las metas corporativa".*

Borghello (2001), en su trabajo de investigación. "Seguridad informática sus Implicancias e Implementación" para la definición de gobierno de TI comenta que es un *"Conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio".*

1.2.4. Propósito del gobierno de TI

El propósito del gobierno de TI es alinear los esfuerzos de TI para contribuir el logro de los objetivos de la empresa y la obtención de los beneficios prometidos. Adicionalmente, TI debe apoyar a la empresa al aprovechar las oportunidades y maximizar los beneficios. Los recursos de TI deben usarse responsablemente, y los riesgos relacionados con TI deben ser gestionados de manera apropiada.

1.2.5. Riesgo

Según la ISO 31000:2009, "*el efecto de la incertidumbre en la consecución de los objetivos*".

1.2.6. Gestión de riesgos

Según COBIT 5 (2012), menciona que "*Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa*".

1.2.7. Estándares de riesgos

ISO 31000

La Organización Internacional de Estandarización ha desarrollado el ISO 31000:2009 "Gestión de Riesgos. Principios y directrices". Se trata de una norma general, de aplicación a cualquier organización independientemente de tamaño o sector y que no es certificable, pero proporciona una guía para los programas de auditoría interna o externa. Las organizaciones que la utilizan se pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido a nivel internacional, proporcionando sólidos principios para la gestión eficaz y el gobierno corporativo.

Al tratarse de una norma general la ISO/IEC 31000 (Organización Internacional de Estandarización/Comisión Electrotécnica Internacional) no establece directrices concretas para el tratamiento de riesgos, sino que da orientaciones para la implantación de un sistema de gestión del riesgo que sea compatible con los estándares de gestión de riesgos particulares de cualquier sector.

Los riesgos que se presentan en las organizaciones pueden tener consecuencias en el factor económico y reputación empresarial, así como el medio ambiente, seguridad y resultados en la sociedad. Por lo tanto, la gestión del riesgo efectivamente ayuda a las organizaciones a un buen desempeño en un entorno lleno de incertidumbres.

El uso de esta norma puede ayudar a las organizaciones a aumentar la probabilidad de lograr los objetivos, mejorar la identificación de oportunidad y amenazas, y dar una asignación y uso efectivo de los recursos para el tratamiento de riesgos.

ISO 31000:2009 está estructurado en tres elementos claves para una gestión de riesgos efectiva, transparente, sistémica y creíble:

- Principios de la gestión de riesgos.
- Marco de trabajo para la gestión de riesgos.
- Proceso de gestión de riesgos.

En primer término, una efectiva gestión de riesgos debería satisfacer una serie de principios:

- Crear y proteger valor para ayudar a alcanzar los objetivos de la organización y mejorar su desempeño.
- Estar integrada en los procesos de una organización. Hacer la responsabilidad del riesgo una responsabilidad de cada gerente.
- Ser parte de la toma de decisiones. La gestión de riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
- Tratar explícitamente la incertidumbre. Trata aquellos aspectos de la toma de decisiones que no son ciertos, la naturaleza de esa incertidumbre y cómo pueden solucionarse.
- Ser sistemática, estructurada y oportuna. Contribuye a la eficiencia y a la obtención de resultados fiables.
- Basarse en la mejor información disponible. Los insumos del proceso de gestión del riesgo están basados en fuentes de información fiables.
- Alinearse al contexto y al perfil de riesgo de la organización.

●Tener en cuenta factores humanos y culturales. La capacidad, percepciones o intenciones humanas pueden facilitar o dificultar el logro de los objetivos de la organización.

●Ser transparente e inclusiva. Asegurar que la gestión sea abierta, visible y accesible e involucrando a las partes interesadas y responsables de la organización.

●Ser dinámica, iterativa y sensible al cambio. La gestión de riesgos debe ser capaz de detectar y responder a los cambios de la organización y de su entorno.

●Facilitar la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente el enfoque de la gestión de riesgos.

Teniendo en cuenta estos principios, se pretende que las organizaciones:

●Incrementen la probabilidad de alcanzar los objetivos trazados

●Fomentar una gestión proactiva

●Sean conscientes de la necesidad de identificar y tratar los riesgos en toda la organización.

●Mejoren la identificación de las oportunidades y amenazas.

●Cumplan con las exigencias legales y reglamentarias y las normas internacionales.

●Mejoren la confianza de los inversionistas.

●Establezcan una base confiable para la toma de decisiones y la planificación de resultados.

●Mejoren los controles.

●Efectivamente asignen y utilicen recursos para el tratamiento de riesgos.

●Mejorar la eficacia y eficiencia operativa.

●Mejoren la salud y la seguridad, así como la protección del medio ambiente.

●Mejoren la prevención de pérdidas y de manejo de incidentes.

●Reduzcan al mínimo las pérdidas.

●Mejoren el aprendizaje organizacional.

●Mejoren la capacidad de resistencia de la organización.

La ISO 31000:2009 recomienda desarrollar, implementar, y mejorar de forma continua un marco de referencia, cuyo propósito es integrar el proceso de gestión de riesgos en la dirección, estrategia y planificación, procesos, políticas, valores y cultura de toda la organización.

El marco de trabajo sigue la estructura del ciclo de vida PDCA, con una etapa previa de Mandato y Compromiso. La norma establece una serie de mandatos que debe cumplir la dirección de la organización para asegurar la efectividad de la gestión de riesgos, así como una planificación estratégica y rigurosa.

El proceso de gestión de riesgos consta de tres etapas: establecimiento del contexto, valoración de riesgos y tratamientos de los mismos. La parte más importante es establecer el contexto en el que trabaja la organización, para conocer el entorno en el que la organización busca alcanzar sus objetivos y así poder gestionar, identificar, analizar, valorar y tratar los riesgos que puedan suceder.

La ISO 31010, "Gestión del riesgo. Técnicas de evaluación de Riesgos" que ofrece directrices para la aplicación de técnicas sistemáticas de evaluación de riesgos, donde propone esta clasificación:

- Métodos basados en evidencias.
- Enfoques sistemáticos del equipo.
- Técnicas de razonamiento inductivo.

Para la identificación de los riesgos se debe tener en cuenta la cadena del riesgo, tal como lo indica Miguel Ángel Carmona miembro de Instituto Andaluz de Tecnología: *"Un Riesgo está*

siempre asociado a un suceso; el suceso puede tener una o varias causas (o fuentes de riesgo), y de manera similar sus consecuencias pueden implicar diferentes impactos. La identificación de un riesgo debe permitir comprender en cada caso esta cadena, ya que esto facilita la posterior apreciación del riesgo, mediante el análisis de la probabilidad de ocurrencia y de las consecuencias."

1.2.8. Normas, estándares, metodologías de Gestión de riesgos de TI.

La norma ISO/IEC 27000: es el conjunto de estándares desarrollados o en fase de desarrollo por la Organización Internacional de Estandarización y la Comisión Electrotécnica Internacional donde se proporciona un marco para la Gestión de la Seguridad de la Información para cualquier tipo de organización, publicada en su tercera edición de 15 de Enero de 2014, recoge todas definiciones para la serie de normas de 27000, aportando las bases de la importancia de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI); Introducción, establecimiento, monitorización, mantenimiento y mejora. Las normas incluyen:

ISO/IEC 27001: Publicada en octubre de 2005 y revisada en septiembre de 2013, es la principal norma de la serie 27000, contiene los requisitos del sistema de gestión de seguridad de la información, basa sus orígenes en la norma británica anulada BS-7799-2:2002. Esta norma enumera los objetivos de control y controles que desarrolla en la ISO 27002:2005.

La aplicación de todos los controles no son obligatorios para las organizaciones que estén en desarrollando su SGSI pero si deben argumentar sólidamente la no aplicabilidad de los controles no implementados.

Muchos países han adoptado esta norma a su entorno como por ejemplo en España UNE-ISO/IEC 27001:2007, Colombia NTC-ISO-IEC 27001, Chile NCh-ISO27001, Perú NTP-ISO 27000, etc.

ISO/IEC 27002: Tiene su origen en la ISO 17799:2005 pero publicada en Julio 2007 y revisado en Septiembre de 2013, contiene la guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Esta norma contiene 35 objetivos de control y 114 controles, que son agrupados en 14 dominios.

ISO/IEC 27003: Publicada en febrero de 2010, contiene los aspectos críticos necesarios para el diseño e implementación un SGSI de acuerdo al ISO/IEC 27001:2005. Esta describe los procesos de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Esta norma está basada en los anexos B de la norma Británica BS 7799-2.

ISO/IEC 27004: Publicada en Diciembre de 2009. Esta norma es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001, que concreta cómo configurar el programa de medición, qué parámetros medir, cuñado y cómo medirlos, y ayuda a la empresas a crear objetivos de rendimiento y criterios de éxito. La medición de la seguridad aporta protección a los sistemas de la organización y da respuesta a las amenazas de la misma. Las etapas propuestas para esta norma son: selección de procesos y objetivos de medición, definición de las líneas base, recopilación de Datos, Desarrollo de un método de medición,

interpretación de los valores medidos y por último la comunicación de los valores de medición.

ISO/IEC 27005: Publicada en Junio de 2008 y actualizada a una segunda edición en Junio de 2011. Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la Información, apoyando los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos, sustituyendo a las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

Esta norma es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. Aunque no recomienda una metodología a seguir, esto dependerá de una serie de factores, como el alcance real del sistema de gestión de seguridad de la información, o el sector comercial de la propia industria.

Las organizaciones utilizaran el método que mejor se adapte a su realidad para la evaluación de riesgos. Esta norma contiene:

- Prefacio.
- Introducción.
- Referencias normativas.
- Términos y definiciones.
- Estructura.
- Fondo.
- Descripción del proceso de ISRM.
- Establecimiento Contexto.
- Información sobre la evaluación de riesgos de seguridad (ISRA).

- Tratamiento de Riesgos Seguridad de la Información.
- Admisión de Riesgos Seguridad de la información.
- Comunicación de riesgos de seguridad de información.
- Información de seguridad Seguimiento de Riesgos y Revisión.

La norma sirve para no tener dudas sobre elementos que deben incluir toda buena metodología de Análisis de Riesgo. El estándar incluye seis anexos, entre carácter informativo y no normativo, con orientaciones que van desde la identificación de activos e impactos, ejemplos de vulnerabilidades y sus amenazas asociadas, hasta distintas aproximaciones para el análisis distinguiendo entre análisis de riesgo de alto nivel y análisis detallado.

Metodologías

Las metodologías de Gestión de Riesgos de TI, establecen una estructura de trabajo para desarrollar un orden secuencial y formal que permita establecer resultados coherentes para en cada contexto particular definir las necesidades diagnosticadas, establecer las estrategias preventivas y asegurando la efectiva generación de valor de las Tecnologías de Información.

Figura 1: Ciclo de administración de riesgos

Fuente: Deloitte Training

OCTAVE: (Operationally Critical Threat, Asset and Vulnerability), Metodología de Análisis de Riesgos que se centra en la seguridad de la Información, que establece la evaluación como una iniciativa de vital importancia generando una visión a lo ancho de la organización proveyendo una base para mejorar a partir de allí cada uno de los procesos. Se propone como una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo, con una visión enfocada en en tecnología, que tiene como objetivo los riesgos tecnológicos y el foco en los

temas tácticos, el objetivo de OCTAVE es el riesgo organizacional y el foco son los temas relativos a la estrategia y a la práctica.

Cuando se aplica OCTAVE: un pequeño equipo de gente desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT) trabajan juntos dirigidos a las necesidades de seguridad, balanceando tres aspectos: riesgos operativos, prácticas de seguridad y tecnología. Por lo tanto además de la referencia en cuanto a la secuencia lógica de desarrollo, se orienta a los procesos, los cuales serían evaluados en el esquema de contrastación para validar el modelo que en esta investigación propuesta.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el entonces Ministerio de Administraciones Públicas de España, hoy en día Ministerio de Hacienda y Administraciones Públicas. La primera versión se publicó en 1997. En el 2012 introduce cambios con respecto al alineamiento con la normativa ISO, buscando una integración de las tareas de análisis de riesgos, normalizando actividades como el MAR - Método de Análisis de Riesgos, PAR – Proyecto de Análisis de Riesgos, PS – Plan de seguridad, dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno, razón por la que se tomó como referencia para la presente investigación. Como otro punto relevante se tomó en cuenta sus objetivos de concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo. Ofrecer un método sistemático, adaptado al contexto de una institución privada universitaria, para analizar tales riesgos. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

RISK IT: Propuesta por ISACA, publica como un marco de trabajo, para gestión de riesgos "The RISK IT Framework", el cual ha sido diseñado y creado principalmente como un recurso educativo para los oficiales de información, la alta dirección y administración de TI.

El marco de RISK IT se basa en los principios de gestión de los riesgos organizacionales (ERM), las normas y marcos como COSO ERM 2 y AS/NZS 43603 y provee información acerca de cómo aplicar estos principios a las TI. RISK IT aplica los conceptos generalmente aceptados de los principales estándares y marcos, así como los principales conceptos de la gestión de otros riesgos de TI, relacionados con las normas.

RISK IT es un marco de referencia para gestión de riesgos basado en el valor y beneficios que la organización obtiene a través de las iniciativas de TI. Se centra principalmente en la consecución de los objetivos de la organización y en la gestión de los riesgos que causan la no obtención de valor y sus beneficios, de igual manera analiza el riesgo de no aprovechar las iniciativas y ventajas de TI. Mientras los otros modelos se centran en eliminar los riesgos, RISK IT contempla la posibilidad de tomar riesgos que pueden traer beneficios a la organización, teniendo en cuenta que haya un adecuado balance entre el Riesgo y el Valor para tomar ventaja de TI.

Esta metodología ha sido referenciada porque está tomando en cuenta que el Gobierno de TI se define como la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos.

NIST SP 800-30: Guía de Gestión de riesgos para sistemas de tecnologías de Información. En esta guía se define al riesgo como el impacto negativo neto de la manifestación de una vulnerabilidad, considerando tanto la probabilidad y el impacto de ocurrencia. La gestión de riesgos es el proceso de identificación de riesgos, evaluación de riesgos por lo que se debe tomar medidas para reducir el mismo a un nivel aceptable. Esta guía proporciona una base para desarrollar un programa eficaz de gestión de riesgos, que contiene tanto las definiciones y la orientación práctica necesaria para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI. El objetivo final es ayudar a las organizaciones a gestionar mejor los riesgos relacionados con los procesos que son soportados por TI. Además se ofrece información sobre la selección de controles. Estos controles se pueden utilizar para mitigar el riesgo para mejorar la protección de misión crítica de la información y los sistemas informáticos que procesan, almacenan y transportan dicha información. Las organizaciones pueden optar por ampliar o abreviar los procesos y medidas integrales que se sugieren en esta guía, adaptarlos a su entorno y procesos relacionados con la misión de gestionar los riesgos de TI.

Se plantean 3 objetivos:

1. Asegurar los sistemas que almacenan, procesan o transmiten información organizacional.
2. Permitir la toma de decisiones efectiva en la gestión de riesgos bien informados, para justificar los gastos que forman parte de un presupuesto de TI; y
3. Ayudar a la administración en autorizar (o acreditar) que las sistemas de TI sobre la base de la documentación respalden los resultados de la realización de la gestión de riesgos.

CAPÍTULO II: MATERIALES Y MÉTODOS

1. Tipo de estudio y diseño de contrastación

Tipo de Estudio: Cuantitativa aplicada

1.1. Diseño de Contrastación: Pre test – Post Test

Para el cumplimiento de los objetivos de la presente tesis, se identificó como diseño de contrastación el de tipo pre test – post test; el mismo que permitirá probar el planteamiento de la hipótesis. Para esto se medirá la variable dependiente a ser utilizada (pre test), luego se efectúa una nueva medición de la variable dependiente en la información de las tecnologías de información que dan soporte a los procesos académicos administrativos de las universidades de la región (post test), y finalmente la aplicación de la variable independiente el Modelo de Gestión de Riesgos basado en estándares adaptados a las TI utilizadas.

En la siguiente figura se detalla lo que se propone lograr en el resultado del método de diseño pre test – post test.

Diseño de Contrastación Pre-Test y Post-Test

$$GE = O_1 \quad X \quad O_2$$

Dónde:

GE = Grupo Experimental.

O1 = Contribuir a la generación de valor en las Universidades Privadas de la región, antes aplicar el modelo de gestión de Riesgos.

X = Modelo de Gestión de Riesgos basado en estándares adaptados a las TI que soportan los procesos

O2 = Contribuir a la generación de valor en las Universidades Privadas de la región, antes aplicar el modelo de gestión de Riesgos, después de aplicar el modelo de gestión de Riesgos.

La comparación mencionada, determinará, si las tecnologías de información que soportan los procesos académicos administrativos de las universidades privadas de la región, contribuyen a la generación de valor, determinado en base a:

- Aumentar el número de riesgos detectados por proceso de negocio, para disminuir la frecuencia de interrupción de los procesos, generando información oportuna para la toma de decisiones.
- Incrementar el nivel porcentual de actitud proactiva respecto al nivel de impacto en los procesos afectados, como resultado de la gestión de riesgos de TI en la institución, disminuyendo costos innecesarios.
- Incrementar el número de proyectos propuestos para el monitoreo y revisión periódica permitiendo una efectiva gestión de riesgos que promuevan decisiones de carácter proactivo.

1.2. Población, muestra de estudio y muestreo

- La población considerada para esta investigación tomó en consideración las universidades privadas de la región Lambayeque, 11 al momento de la investigación, sobre la cual se aplicó el cálculo de la muestra, para la aplicación de los instrumentos diseñados para la presente investigación.

- La población considerada para esta investigación en respecto al caso de estudio de una universidad privada de la región Lambayeque, en la que se implantó el Modelo de gestión de riesgos.
- Se tomarán como elementos de la población a los directores a cargo de las tecnologías de información que dan soporte a los procesos de negocio académicos y administrativos de las universidades privadas de la región.
- Cada uno de los procesos académicos que se gestionan en la universidad, así como los procesos administrativos, que son soportados por las tecnologías de información instaladas.
- Los miembros de cada una de las unidades funcionales de la Universidad.

1.3. Métodos, técnicas e instrumentos

Variable	Técnicas	Instrumentos
Contribuir a la generación de valor en las Universidades Privadas de la región.	Encuesta	Cuestionario Entrevistas
	Observación	Documentos Estratégicos

Tabla 2: Métodos, técnicas e instrumentos

2. Plan de procesamiento para análisis de datos

Para la obtención de la información se usó entrevistas y aplicación de encuestas, así también el uso de la observación, técnica importante para la revisión de documentación estratégica.

Entrevistas:

Con los Directores de tecnologías de información, encargados de determinar la situación de la tecnología de información que soportan los procesos académicos administrativos de las universidades privadas de la región.

Encuestas:

Dirigido a los dueños de los procesos para obtener información de funcionalidad de las tecnologías de información que soportan los procesos de cada unidad funcional.

Observación:

Permite tener una perspectiva de la documentación estratégica que reflejan las normativas con respecto a las tecnologías de información que soportan los procesos de la organización.

Resultados:

Para la obtención de los resultados se utilizó un programa estadístico básico SPSS, también en Microsoft Excel, se realizó el traslado de los datos de cada una de las encuestas realizadas con la finalidad de obtener gráficas que permitan visualizar la situación actual en la medición de los porcentajes por indicador establecido en cada uno de los objetivos específicos y su comportamiento mejorado, frente a la aplicación del Modelo de Gestión de Riesgos basados en estándares adaptados a las TI, que soportan los procesos de la Universidad caso de estudio

El Modelo de gestión de riesgos de TI basados en estándares adaptados a las universidades privadas, previamente validado por juicio de expertos que en cuanto a la confiabilidad del mismo, se obtuvo el 88% de fiabilidad y por la concordancia entre los expertos respecto de los contenidos, a través del método de Kendall obteniendo un parámetro p de 0.011. Ambos valores se encuentran dentro de los márgenes válidos de aceptación del modelo.

En el proceso de obtención de la información, se tomó en cuenta el rigor científico mediante la contrastación de la hipótesis que plantea contribuir a la generación de valor de las universidades privadas de la región por la validez del modelo y la aplicación del mismo a un caso de estudio, en una universidad privada de la región. Se hizo la medición de cada uno de los indicadores obteniendo resultados que respaldan el logro del objetivo general de la tesis.

Se aplicaron los criterios de ética en la obtención de la información a través del consentimiento informado, por parte de los encuestados, dado que se dio a conocer mediante documentos presentados en sus instituciones, que la información brindada por ellos persigue una finalidad netamente académica y se cuidará la denominación de su organización.

CAPÍTULO III: RESULTADOS Y DISCUSIÓN

En este capítulo se analizaron estándares y metodologías referentes a la gestión de riesgos de tecnologías de la información, se identificó las siguientes fases coincidentes, las cuales fueron adaptadas a las necesidades de la realidad en el entorno académico de Universidades Privadas.

Figura 2: Estructura base del modelo de gestión de riesgos propuesto tomando como referencia ISO 31000:2009:

Fases I - Establecimiento de contextos

La norma ISO 31000:2009 aporta información sobre el establecimiento del contexto en la gestión del riesgo, con un carácter universal.

Según Ramírez, A., Ortiz, Z. (2011) *"El objetivo de esta etapa es conocer a la organización para determinar que los puede afectar a nivel interno y externo, que requieren proteger y de acuerdo a los recursos actuales como podría darse esa protección para establecer el nivel de aceptación de riesgo al cual están dispuestos, determinar los alcances y limitaciones existentes"*.

Por lo tanto se analizó los dos contextos de influencia para las universidades privadas de la región Lambayeque, como se detalla a continuación:

1. **Contextos Internos**

a) Cultural: Se define como el conjunto de conocimientos que permite identificar las características de las universidades privadas de la región Lambayeque, para definir los escenarios de comportamiento en cuanto a los actores que pertenecen al mismo, como son: estudiantes, docentes, administrativos, padres de familia y autoridades.

Fuentes de información: Plan estratégico, visión, misión, objetivos estratégicos, principios rectores, organigrama de institución, modelo operativo empresarial, etc.

b) Partes internas involucradas: Se define como las interrelaciones que se establecen entre cada uno de los actores del sistema, mencionados en el punto anterior, dando lugar a los procesos soportados por las tecnologías de información que definen la naturaleza de las universidades privadas de la región Lambayeque, siendo estos académicos y administrativos.

Fuentes de Información: Plan estratégico, visión, misión, objetivos estratégicos, principios rectores, organigrama de institución, modelo operativo empresarial, etc.

c) Estructura: Se define como el conjunto de componentes organizacionales de acuerdo a la función que se le asigna según los requerimientos de la institución, que para el caso de instituciones educativas de nivel superior son de tipo vertical por su estructuración, pero desde el sentido funcional es de forma transversal por su naturaleza colaborativa.

Fuentes de Información: Organigrama de institución

d) Recursos: Se define como el conjunto de activos que componen la infraestructura tecnológica que dan soporte a los procesos de las instituciones de superior privadas como servidores, tecnologías de

información, equipos de cómputo de escritorio o portátiles, equipos de red, sistema de protección eléctrica, etc.
Fuentes de Información: Inventario de infraestructura tecnológica.

e) Metas y objetivos: Se define como el conjunto de ideas rectoras de las instituciones educativas superior privadas que apuntan a la calidad educativa y a la acreditación universitaria.
Fuentes de Información: Plan Estratégico.

2. Contextos Externos

a) Ambiente del negocio: es un conjunto de elementos existentes fuera de las universidades privadas de la región Lambayeque que tienen el potencial de afectar en su desempeño como las fuentes laborales de las empresas que definen los perfiles de los egresados que requiere el mercado, así como las proveedoras de servicios e insumos.
Fuente de información: Lista de proveedores de servicios, convenios establecidos con instituciones externas.

b) Social y cultural: es un conjunto de elementos referentes al estilo de vida, el contexto geográfico, demográfico, etc. relacionado a los grupos de interés como padres de familia, estudiantes, empresas, gobiernos locales y otros organismos de la región.
Fuente de información: Datos censales, Información INEI, gobiernos locales.

c) Reglamentos: son las exigencias legales y reglamentarias, donde los riesgos de incumplimiento pueden poner en jaque a la organización, como normas de acreditación y el cumplimiento de estándares de calidad.
Fuente de información: SUNEDU, SUNAT, INDECI, SUNARP, INDECOPI, etc.

d) Competitivo: en un conjunto de elementos resultado del análisis de la competencia directa, la cual puede afectar económicamente como las instituciones educativas de nivel superior de la región.

Fuente de Información: Análisis FODA de la institución.

e) Financiero: es un conjunto de elementos relacionados con la economía, la situación fiscal, las variaciones en los precios, evolución de tasas de interés, tasa de cambio, las distintas políticas fiscales y monetarias a nivel nacional e internacional.
   Fuentes de Información: INEI, BCR

f) Político: es un conjunto de normas establecidas por un gobierno que regula las actividades de las universidades privadas de la región, en algunos casos las incentivan, y en otros casos las limitan, e incluso las prohíben como la ley universitaria promulgada recientemente.
   Fuentes de Información: Constitución Política del Perú

Fase II – Identificación de activos

Esta fase tiene como objetivo determinar los activos que da soporte a la operatividad de las universidades privadas de la región Lambayeque, con sus características, atributos y clasificación en el entorno de las universidades privadas de la región, permitiendo establecer las dependencias entre los activos, valorar los activos con precisión, identificar y valorar los riesgos.

Fuentes de información: Inventario actualizado de infraestructura tecnológica, mapa de procesos (lista de procesos) en el siguiente formato:

Ítem	Lista de activos	Codificación de Etiqueta
Núm. de Ítem	Nombre de Activo	Etiqueta de Activo

Tabla 3: Formato de lista de activos

Esta estructura se formulado tomando en cuenta las recomendaciones de Magerit.

1. Clasificación de activos:

1.1. Procesos de Negocio

Etiqueta: [P]

Descripción: Totalidad que cumple un objetivo útil a la organización, que agrega valor al servicio o producto alineados con la visión y objetivos estratégicos de la organización.

Hammer (2006): Un proceso es una serie organizada de actividades relacionadas, que conjuntamente crean un resultado de valor para el servicio o producto. En el caso de las universitarias privadas de la región tienen prevalencia de carácter académico.

Ítem	Activos Catálogo Procesos de Negocio	Etiqueta
1	Proceso de Matrícula	[P_Mat]
2	Proceso de Gestión Académica	[P_GAcad]
3	Proceso de Investigación	[P_Inv]
4	Proceso de Gestión Curricular	[P_GCur]
5	Proceso de Gestión de Biblioteca	[P_GBib]
6	Proceso de Tutoría	[P_Tut]
7	Proceso de Bienestar Educativo	[P_BienEd]
8	Proceso de Gestión de Educación Continua	[P_GEdCon]
9	Proceso de Gestión Virtual	[P_GVirtual]
10	Proceso de Gestión Convalidación	[P_GConv]

Tabla 4: Activos - Catálogo Proceso de Negocios

1.2.Servicios

Etiqueta: [S]

Descripción: Función que satisface una necesidad de los usuarios. Un servicio es un medio para entregar valor a los clientes, facilitando un

resultado deseado sin la necesidad de que estos asuman los costos y riesgos específicos asociados.

En el caso de las universidades privadas de la región se distingue dos grandes agrupaciones de servicios de carácter académico y administrativo.

En el caso del presente modelo se contemplan los servicios prestados por el sistema:

Ítem	Activos Catálogo Servicio	Etiqueta
1	Servicio Gestión Académica	[S_GAcad]
2	Servicio Campus Virtual - Intranet	[S_Intranet]
3	Servicio de Correo Electrónico	[S_Email]
4	Servicio Wifi	[S_Wifi]
5	Servicio Acceso Internet	[S_Internet]
6	Servicio Telefonía	[S_Tel]
7	Servicio de Conferencias	[S_Confe]
8	Servicios Audiovisuales	[S_Audiov]
9	Servicio de Catálogo Biblioteca	[S_CatBib]
10	Servicio de Biblioteca en Línea	[S_BibLinea]

Tabla 5: Activos - catálogo servicios

1.3.Aplicaciones

Etiqueta: [App]

Descripción: Conjunto de programas, instrucciones y reglas informáticas que permiten dar soporte a un servicio necesario para un proceso de negocio académico y administrativo.

Ítem	Activos Catálogo Software	Etiqueta
1	Sistema de Gestión de Base de Datos	[App_SGBD]
2	Sistema de Gestión Académica	[App_GAcad]
3	Sistema de Gestión Administrativo	[App_GAdm]
4	Sistema de Gestión de Personal	[App_GPer]
5	Sistema de Pensiones	[App_Pens]
6	Sistema de Gestión de Investigación	[App_GInv]
7	Sistema de Biblioteca	[App_Bib]
8	Sistema de Tutoría	[App_Tut]
9	Sistema de Finanzas	[App_Fin]
10	Sistema Logística	[App_Log]
11	Sistema de Gestión Continua	[App_GCont]
12	Sistema de Bolsa de Trabajo	[App_Bolsa]

Tabla 6: Activos - catálogo de aplicaciones

1.4.Soporte de TI

Etiqueta: [Sop]

Descripción: Infraestructura tecnológica que permite la ejecución de aplicaciones tratados en la sección anterior.

Ítem	Activos Catálogo Soporte	Etiqueta
1	Servidor Web	[Sop_Web]
2	Servidores Base de Datos	[Sop_BD]
3	Servidores de Seguridad	[Sop_Seg]

Ítem	Activos Catálogo Soporte	Etiqueta
4	Servidores de Comunicación	[Sop_Com]
5	Dispositivos de Comunicación	[Sop_DisCom]

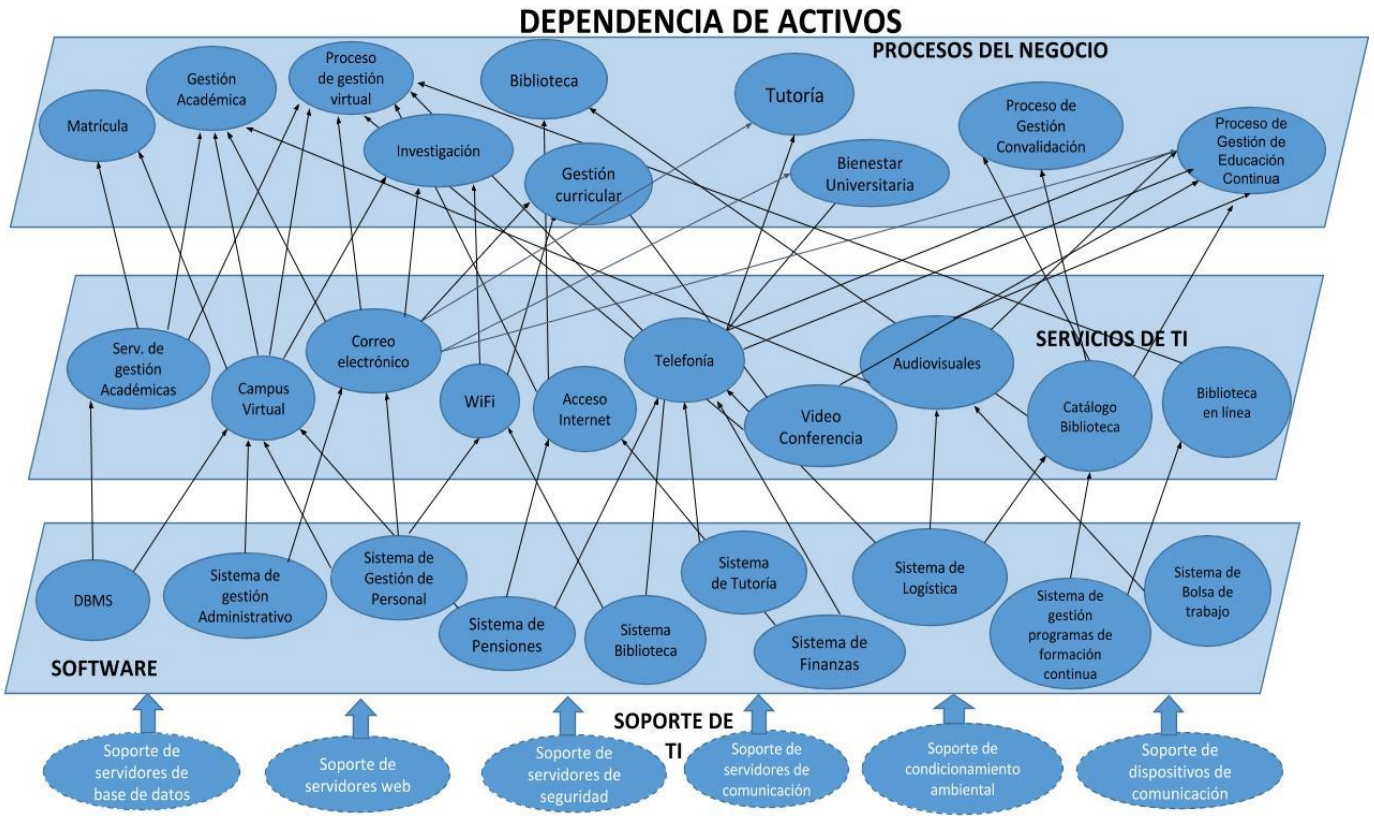
Tabla 7: Activos - catálogo soporte

2. Dependencia de activos:

En este apartado se identifican los activos y se establece una relación de dependencia. Para establecer la relación de dependencia de activos se debe tener en cuenta:

- **Identificación de activos**: Se propone establecer las categorías identificadas en la sección anterior: Procesos de Negocio, Servicios de TI, Aplicaciones y Soporte de TI, correspondiente a las instituciones de tipo universitarias privadas.
- **Establecer las líneas de dependencia**: Esta actividad, permite establecer las líneas de soporte entre categorías con respecto a los activos, apoyando en la determinación de los activos críticos y el impacto que representaría de manifestarse el riesgo.

Figura 3: Dependencia de activos



En la figura N°2 muestra el esquema propuesto de la relación de dependencias entre los activos agrupados en cuatro niveles: soporte TI, aplicaciones, servicios de TI y procesos de negocio.

La propuesta determina la necesidad de ampliar la relación de dependencia a los procesos de negocio, que es el aporte de esta investigación, los estándares sobre los cuales se ha construido proponen solo dos niveles: software y servicios de TI. Los procesos de negocio identifican también como parte importante de su desarrollo a las personas y el uso que estas hacen de los activos, así como la naturaleza de las universidades privadas de la región Lambayeque, que sería un factor que caracteriza el planteamiento de estrategias en la aplicación de gestión de riesgos.

3. Valoración de activo

La valoración de activos debe ser identificada desde una visión TOP-DOWN, para asignar el valor de acuerdo al grado de importancia teniendo en cuenta los criterios de disponibilidad, integridad y confidencialidad con una valoración cuantitativa y cualitativa.

Para el proceso de valoración, se recomienda usar la Escala de Likert, que permite medir grados de conformidad con respecto a los criterios que se desean, para la disponibilidad, integridad y confidencialidad. Además de establecer rangos de valoración que en el caso se estableció del 1 al 5, permitiéndonos tener la amplitud suficiente para la valoración.

Disponibilidad (D): Acceso a la información cuando se necesita.
Integridad (I): Exactitud y totalidad de la información
Confidencialidad (C): Información debe ser accedida sólo por las personas autorizadas.
Matrices para la valoración de riesgos:

DISPONIBILIDAD (D)	
VALOR	CRITERIO
1	No aplica/No es relevante
2	Debe estar disponible al menos el 10% del tiempo
3	Debe estar disponible al menos el 50% del tiempo
4	Debe estar disponible al menos el 75% del tiempo
5	Debe estar disponible al menos el 95% del tiempo

Tabla 8: Valoración de criterio de disponibilidad

INTEGRIDAD (I)	
VALOR	CRITERIO
1	No aplica / No es relevante
2	No es relevante los errores que tenga o la información que falte
3	Tiene que estar correcto y completo al menos en un 50%
4	Tiene que estar correcto y completo al menos en un 70%
5	Tiene que estar correcto y completo al menos en un 95%

Tabla 9. Valoración de criterio de integridad

CONFIDENCIALIDAD (C)	
VALOR	CRITERIO

1	No aplica / No es relevante.
2	Daños muy bajos, el incidente no trasciende del proceso afectado.
3	Daños bajos, el incidente no trasciende del proceso afectado.
4	Los daños serían relevantes, el incidente implica a otros procesos
5	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas

Tabla 10: Valoración de criterio de confidencialidad

Se aplica el nivel de criticidad según matriz en las tablas propuestas. Los niveles de criticidad de los activos de TI se obtendrán del producto de las calificaciones realizadas para cada criterio de seguridad, como se expresa en la ecuación.

Nivel de Valoración = Confidencialidad + Integridad + Disponibilidad

Aplicando en dicha ecuación la siguiente valoración clasificada de la siguiente manera:

Rango	Valor	Descripción	
1 – 3	1	Muy bajo	MB
4– 6	2	Bajo	B
7– 9	3	Medio	M
10 – 12	4	Alto	A
13 – 15	5	Muy alto	MA

Tabla 11: Tabla de valoración de los niveles de criticidad de activos

En esta fase, las áreas de la institución deben participar e involucrarse para obtener un resultado lo más cercano posible a la realidad, estableciendo matrices de valor para cada uno de los activos identificados en la fase anterior para obtener resultados coherentes.

CUADRO DE VALORACIÓN DE ACTIVOS							
ACTIVO			CRITERIOS				
CATEGORIA	CODIGO	DESCRIPCION	C	I	D	TOTAL	
Etiqueta Categoría	Código activo	Descripción del activo	Valoración confidencialidad	Valoración de integridad	Valoración de disponibilidad	Rango de Valoración	Descripción de valoración

Tabla 12: Ejemplo de cuadro de valoración

CUADRO DE VALORACIÓN DE ACTIVOS								
	ACTIVO			CRITERIOS				
N	CATEGORIA	CODIGO	DESCRIPCION	C	I	D	TOTAL	
1	[P]	[P_Mat]	Proceso de Matrícula					
2	[P]	[P_GAcad]	Proceso de Gestión Académica					
3	[P]	[P_Inv]	Proceso de Investigación					
4	[P]	[P_GCur]	Proceso de Gestión Curricular					
5	[P]	[P_GBib]	Proceso de Gestión de Biblioteca					
6	[P]	[P_Tut]	Proceso de Tutoría					
7	[P]	[P_BienEd]	Proceso de Bienestar Educativo					

CUADRO DE VALORACIÓN DE ACTIVOS								
	ACTIVO			CRITERIOS				
N	CATEGORIA	CODIGO	DESCRIPCION	C	I	D	TOTAL	
8	[P]	[P_GVirtual]	Proceso de Gestión de Educación Continua					
9	[P]	[P_GVirtual]	Proceso de Gestión Virtual					
10	[P]	[P_GConv]	Proceso de Gestión Convalidación					
11	[S]	[S_GAcad]	Servicio Gestión Académica					
12	[S]	[S_Intranet]	Servicio Campus Virtual - Intranet					
13	[S]	[S_Email]	Servicio de Correo Electrónico					
14	[S]	[S_Wifi]	Servicio WIFI					
15	[S]	[S_Internet]	Servicio Acceso Internet					
16	[S]	[S_Tel]	Servicio Telefonía					
17	[S]	[S_Confe]	Servicio de Conferencias					
18	[S]	[S_Audiov]	Servicios Audiovisuales					
19	[S]	[S_CatBib]	Servicio de Catálogo Biblioteca					
20	[S]	[S_BibLinea]	Servicio de Biblioteca en Línea					
21	[App]	[App_SGBD]	Sistema de Gestión de Base de Datos					
22	[App]	[App_GAcad]	Sistema de Gestión Académica					
23	[App]	[App_GAdm]	Sistema de Gestión Administrativo					
24	[App]	[App_GPer]	Sistema de Gestión de Personal					

CUADRO DE VALORACIÓN DE ACTIVOS								
	ACTIVO			CRITERIOS				
N	CATEGORIA	CODIGO	DESCRIPCION	C	I	D	TOTAL	
25	[App]	[App_Pens]	Sistema de Pensiones					
26	[App]	[App_GInv]	Sistema de Gestión de Investigación					
27	[App]	[App_Bib]	Sistema de Biblioteca					
28	[App]	[App_Tut]	Sistema de Tutoría					
29	[App]	[App_Fin]	Sistema de Finanzas					
30	[App]	[App_Log]	Sistema Logística					
31	[App]	[App_GCont]	Sistema de Gestión Continua					
32	[App]	[App_Bolsa]	Sistema de Bolsa de Trabajo					
33	[Sop]	[Sop_Web]	Soporte Servidor Web					
34	[Sop]	[Sop_Web]	Soporte de Servidores Base de Datos					
35	[Sop]	[Sop_Seg]	Soporte de Servidores de Seguridad					
36	[Sop]	[Sop_Com]	Soporte de Servidores de Comunicación					
37	[Sop]	[Sop_DisCom]	Soporte de Dispositivos de Comunicación					

Tabla 13: Cuadro valoración de activos

Fase III - Análisis del riesgo

Según la ISO (Guide 73:2009, 2009) es el proceso para comprender la naturaleza del riesgo determinando su nivel, proporcionando la base para la evaluación y decisiones sobre el tratamiento del riesgo.

En esta etapa se recomienda utilizar técnicas como: análisis de procesos, brainstorming, entrevistas, talleres de trabajo, benchmarking, cuestionarios,

etc., que permitan identificar los riesgos de cada uno de los activos con sus amenazas y vulnerabilidades.

Riesgo = P_F * I

Donde:

P_F: Representa dos acepciones; de contar con data histórica que establezca el valor estadístico, se denomina probabilidad, caso contrario se denomina frecuencia de ocurrencia del riesgo. En ambos casos P_F indica el número de veces que se puede materializar el riesgo.

I: Impacto, grado de afectación del riesgo sobre los procesos de negocio (revisar Mapa de dependencias de activos).

Tabla de niveles de valorización

Para el análisis del riesgo se establece el nivel de impacto que permitan describir el valor de este.

Nivel de impacto	Valor	Descripción	
1 – 3	1	Muy bajo	MB
4– 6	2	Bajo	B
7– 9	3	Medio	M
10 – 12	4	Alto	A
13 – 15	5	Muy alto	MA

Tabla 14: Nivel de impacto

Además de la probabilidad o frecuencia de ocurrencia con su respectiva descripción, como se muestra en la Tabla N° 15.

Probabilidad o frecuencia	Valor	Descripción de probabilidad	
Cada varios años	1	Muy poco frecuente	MB
Una vez al año	2	Poco frecuente	B

Cuatro veces al año	3	Normal	M
Mensualmente	4	Frecuente	A
A diario	5	Muy frecuente	MA

Tabla 15: Probabilidad o frecuencia de ocurrencia
Fuente: Basado en Magerit v3 libro I p.28

RANGO	NIVEL DE CRITICIDAD	DESCRIPCIÓN
1 – 5	1	Bajo
6– 10	2	Medio
11– 25	3	Alto

Tabla 16: Categoría de riesgo

Se propone una estructura de semaforización que permita resaltar mediante colores la clasificación de los riesgos para ser identificados, de manera rápida y amigable.

RANGO	NIVEL DE CRITICIDAD	DESCRIPCIÓN	VISTA SEMÁFORO
1 – 5	1	Bajo	
6– 10	2	Medio	
11– 25	3	Alto	

Tabla 17: Categoría de riesgo semaforizado

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descripción	Nivel	Categoría	Código Riesgo	Nivel	Categoría
1	Código Categoría	Nombre de activo	Descripción de la amenaza 01	vulnerabilidad 01							
				vulnerabilidad 02							
			Descripción de la amenaza 02	vulnerabilidad 03							
				vulnerabilidad 04							

Tabla 18: Ejemplo cuadro de análisis de riesgos.

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descripción	Nivel	Categoría	Cód. Riesgo	Nivel	Categoría
1	[P_Mat]	Proceso de Matrícula									
2	[P_GAcad]	Proceso de Gestión Académica									
3	[P_Inv]	Proceso de Investigación									
4	[P_GCur]	Proceso de Gestión Curricular									
5	[P_GBib]	Proceso de Gestión de Biblioteca									
6	[P_Tut]	Proceso de Tutoría									
7	[P_BienEd]	Proceso de Bienestar Educativo									
8	[P_GVirtual]	Proceso de Gestión de Educación Continua									
9	[P_GVirtual]	Proceso de Gestión Virtual									
10	[P_GConv]	Proceso de Gestión Convalidación									
11	[S_GAcad]	Servicio Gestión Académica									

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descripción	Nivel	Categoría	Cód. Riesgo	Nivel	Categoría
12	[S_Intranet]	Servicio Campus Virtual - Intranet									
13	[S_Email]	Servicio de Correo Electrónico									
14	[S_Wifi]	Servicio WIFI									
15	[S_Internet]	Servicio Acceso Internet									
16	[S_Tel]	Servicio Telefonía									
17	[S_Confe]	Servicio de Conferencias									
18	[S_Audiov]	Servicios Audiovisuales									
19	[S_CatBib]	Servicio de Catálogo Biblioteca									
20	[S_BibLinea]	Servicio de Biblioteca en Línea									
21	[App_SGBD]	Sistema de Gestión de Base de Datos									
22	[App_GAcad]	Sistema de Gestión Académica									
23	[App_GAdm]	Sistema de Gestión Administrativo									

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descripción	Nivel	Categoría	Cód. Riesgo	Nivel	Categoría
24	[App_GPer]	Sistema de Gestión de Personal									
25	[App_Pens]	Sistema de Pensiones									
26	[App_GInv]	Sistema de Gestión de Investigación									
27	[App_Bib]	Sistema de Biblioteca									
28	[App_Tut]	Sistema de Tutoría									
29	[App_Fin]	Sistema de Finanzas									
30	[App_Log]	Sistema Logística									
31	[App_GCont]	Sistema de Gestión Continua									
32	[App_Bolsa]	Sistema de Bolsa de Trabajo									
33	[Sop_Web]	Soporte Servidor Web									
34	[Sop_Web]	Soporte de Servidores Base de Datos									
35	[Sop_Seg]	Soporte de Servidores de Seguridad									
36	[Sop_Com]	Soporte de Servidores de Comunicación									

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descripción	Nivel	Categoría	Cód. Riesgo	Nivel	Categoría
37	[Sop_DisCom]	Soporte de Dispositivos de Comunicación									

Tabla 19: Cuadro de identificación y valorización de riesgos

Fase IV –Valoración del Riesgo

La fase de valoración del riesgo tiene sus fuentes en aquellos ámbitos de las universidades privadas de la región Lambayeque tanto internos como externos, que provocan incertidumbres al logro de los objetivos.

Según la ISO (Guide 73:2009, 2009) La valoración del riesgo es el proceso de comparación de los resultados del análisis del riesgo con sus criterios para determinar si el riesgo o su magnitud son aceptables o tolerables.

Priorización del riesgo:

Se ubican los riesgos identificados en la fase anterior (Tabla N° 19) en el mapa de calor (Figura N° 5), tomando como base los valores de impacto y probabilidad o frecuencia, para identificar la prioridad de riesgo, facilitando la toma de decisiones para el tratamiento de los riesgos que se desarrolla en la siguiente etapa, iniciando con los riesgos ubicados en la zona de alta prioridad.

Figura 4: Formato de priorización de riesgos

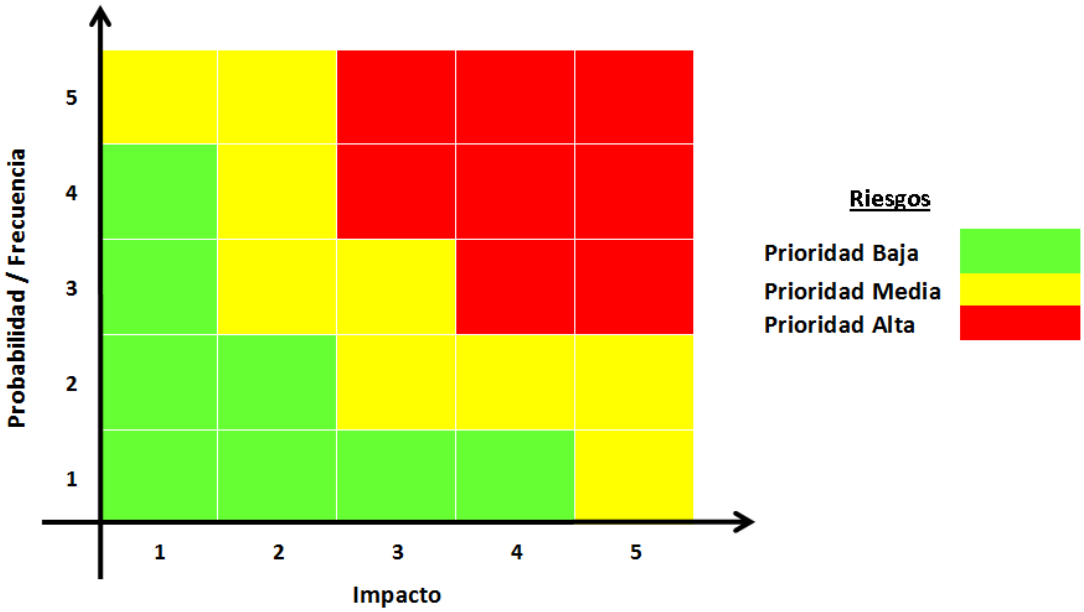
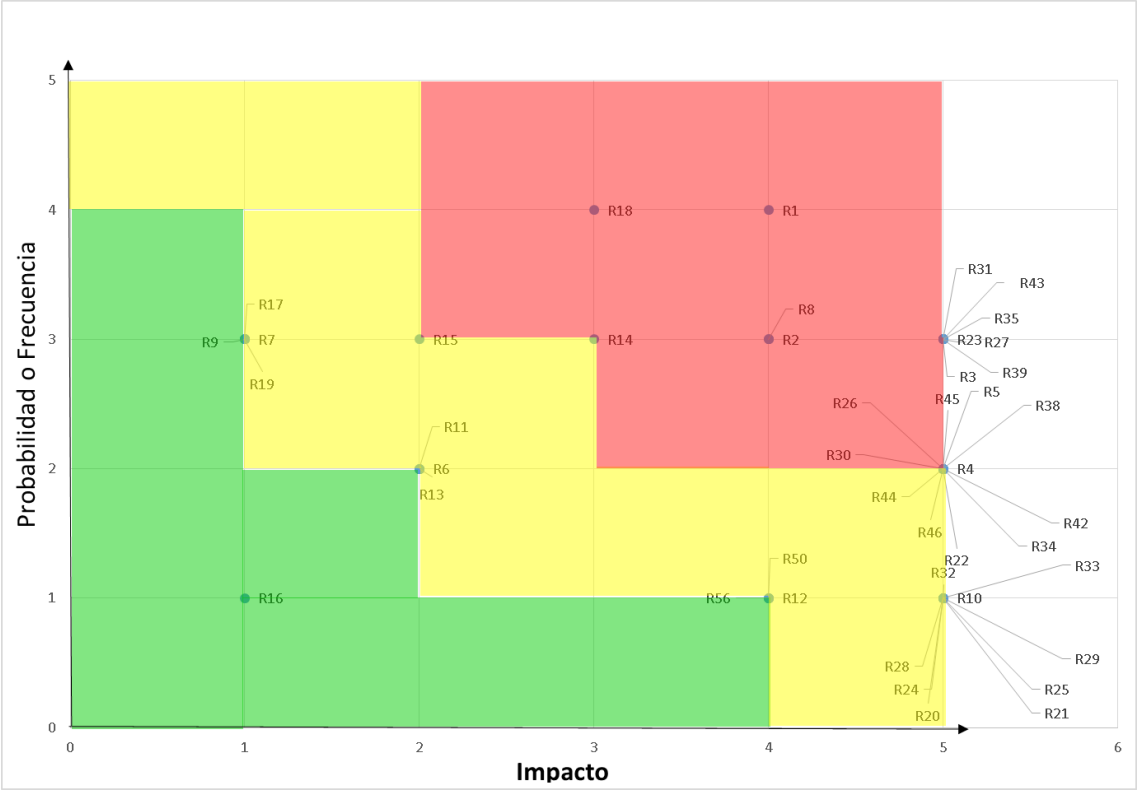


Figura 5: Ejemplo priorización de riesgos



Cuadro de valoración del riesgo.

En el siguiente cuadro, por cada riesgo se determina la capacidad, que define los límites de tolerancia o apetito de riesgo que asumiría la organización en base a su contexto, el activo y su relación con los procesos de negocio para determinar si la magnitud del riesgo es aceptable o tolerable.

Según la ISO (Guide 73:2009, 2009) define los siguientes conceptos:

- Apetito: cantidad y tipo de riesgo que una organización está dispuesta a obtener o conservar.
- Tolerancia de riesgo: disponibilidad de una organización o de las partes interesadas para soportar el riesgo después del tratamiento con el fin de lograr sus objetivos.
- Capacidad de riesgo: Cantidad y tipo de riesgo máximo que la empresa es capaz de soportar en la persecución de sus objetivos.

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valoriza
A	R1	[S_CamVir]	Servicio Campus Virtual	Error de usuario (A1)	Carencia de validación de datos entradas en los sistemas	16	10	15	Intolera
A	R3	[S_CamVir]	Servicio Campus Virtual	Alteración accidental de información (A3)	Carencia de programas de capacitación al personal	15	10	15	Toleral
A	R23	[App_BDCamp]	BD Campus Virtual	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	9	16	Toleral
A	R27	[App_WebCamp]	Web Campus Virtual	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	10	15	Toleral

Tabla 20: Cuadro de valoración del riesgo

Fase V - Tratamiento de los riesgos

Tratamiento o Respuesta al Riesgo, esta fase tiene como objetivo determinar la forma de actuar o las medidas a implementar para afrontar un riesgo por medio de las estrategias: Aceptar, Evitar, Mitigar, Compartir el riesgo. Para determinar la estrategia se toma como referencia la información de identificación y valorización de riesgos (Tabla N° 18), la priorización de riesgos (figura N°4), y tabla de valorización del riesgo para determinar la estrategia del tratamiento.

Teniendo como posibles estrategias definidas según ISACA (COBIT, 2012):

- Evitar: Dejar de realizar las actividades o salir de las condiciones que permiten que el riesgo se presente.
- Transferir–Compartir: Reducir la frecuencia y el impacto al transferir o compartir el riesgo. Suele darse a través de la contratación de seguros, la externalización de servicios o instrumentos de mercado de capital a largo plazo
- Mitigar: Ejecutar acciones para disminuir frecuencia e impacto de un riesgo. Implementación de procesos de gestión de riesgos.
- Aceptar: Se conoce el riesgo y se reconoce la exposición a la pérdida pero no se toman acciones relativas a un riesgo en particular. Se acepta la pérdida en caso ocurra.

.

Para realizar el tratamiento de riesgos, se debe revisar cada uno de los activos y sus amenazas identificadas, además se debe proponer acciones que permitan implementar una estrategia de respuesta al riesgo que deberá reducir la probabilidad de ocurrencia o el impacto sobre los procesos de negocio.

Cada una de las acciones para el tratamiento de riesgos debe trabajarse como acciones o proyectos individuales, es importante considerar la inversión necesaria para cada proyecto, el cual debe estar sustentado en función al impacto sobre los procesos de negocio.

Nombre del Proyecto:	
Acción :	
Riesgo que se trata:	
Estrategia de riesgo:	
Categoría de Riesgo:	
Objetivo:	
Responsable:	
Recursos requeridos:	
Presupuesto:	
Procesos de negocios afectado	
Tiempo de ejecución	
Anexos:	

Tabla 21: Formato de ficha de proyecto para definir acciones de tratamiento de riesgos

Fase VI: Monitoreo y revisión de riesgos

Esta fase permite evaluar periódicamente los cambios en los factores que puedan modificar o invalidar la evaluación de riesgos.

Se recomienda realizar una revisión de proceso de evaluación de Riesgos por lo menos una vez al año o cuando existan cambios en el contexto o en los procesos de negocio.

En este proceso se revisa los cambios en los contextos internos, externos, modificaciones en los catálogos de procesos, servicios, aplicaciones, soporte de TI y mapa de dependencias de activos.

Los cambios pueden incluir: agregar nuevos procesos de negocios y sus riesgos inherentes, cambios en la probabilidad o cambios en el impacto de los riesgos existentes.

Nombre del Proyecto:	
Acción :	
Riesgo que se trata:	
Estrategia de riesgo:	
Categoría de Riesgo:	
Objetivo:	
Responsable:	
Recursos requeridos:	
Presupuesto:	
Procesos de negocios afectado	
Tiempo de ejecución	
Anexos:	
Monitoreo y revisión	
Verificación:	**Variables a controlar:**
Acciones a ejecutar para obtener datos para el procesamiento de los indicadores.	Identificación de características del objetivo del proyecto para determinar el indicador de medición.
Indicadores:	

Expresión de medida de lo logrado en la aplicación del procesamiento de la verificación, para evaluar el grado de cumplimiento del objetivo planteado.
Acciones para mejorar el proyecto
Medidas correctivas para mejorar los resultados obtenidos.

Tabla 22: Ficha de monitoreo y revisión

La tabla N° 22 pretende facilitar al gestor de riesgos el proceso de monitoreo y revisión de los riesgos, el cual toma la ficha de identificación de proyectos que se evalúa con los componentes de verificar y actuar del ciclo Deming.

Usa los proyectos identificados en la fase de tratamiento de riesgos, verificando los resultados de los datos obtenidos de las variables que se pretenden medir, para luego aplicar los indicadores de medición, cuyos resultados permitirán retroalimentar la necesidad de acciones de mejora en la consecución de los objetivos.

Nombre del Proyecto:	
Acción :	Implementar los planes de validación de datos de entrada en cada uno de los módulos de gestión según estándares de calidad de desarrollo de software
Riesgo que se trata:	R1
Estrategia de riesgo	mitigar
Categoría de Riesgo:	Alto
Objetivo:	Reducir el índice de errores de usuario en el ingreso de datos en cada uno de los módulos.
Responsable:	Dirección de TI
Recursos requeridos:	Personal de la jefatura de desarrollo de sistemas
Presupuesto:	Número de personas*tiempo*costohora = 02 * 48 * 1 0 = S/. 960
Procesos de negocios afectado	Gestión de personal / Gestión de pensiones / Gestión de tutoría / Gestión Administrativa

	/ Gestión de contabilidad / Gestión curricular / Gestión Académica.
Tiempo de ejecución	48 horas
Anexos:	--
Monitoreo y revisión	
Verificación:	**Variables a controlar:**
Inspeccionar el cumplimiento de los planes de validación de los datos de entrada	Validaciones erradas
Indicadores:	
Índice de validaciones erradas = Número de validaciones totales – Número de validaciones erradas.	
Acciones para mejorar el proyecto	
Si el resultado de la operacionalización es negativo, se adoptan medidas correctivas para mejorar los resultados obtenidos.	

Tabla 23: Ejemplo de ficha de monitoreo y revisión

Discusión

Según el objetivo general planteado en la presente tesis de contribuir en la generación de valor de las TI, que soportan los procesos académicos y administrativos en las universidades privadas de la región, se desarrolló el modelo de gestión de riesgos basado en estándares adaptados.

Para la validación del modelo se diseñó para el mismo dos instrumentos:

Por juicio de expertos, para lo cual 2 profesionales expertos validaron la estructura y contenido del modelo propuesto en la presente tesis, obteniendo la aceptación del mismo (Ver Anexo N° 06).

Para medir el nivel de confiabilidad del modelo, se procesó los resultados del juicio de expertos, aplicando Alfa de Crombach, obteniendo un nivel de confiabilidad del 88% como lo refiere los resultados del cálculo siguiente:

Estadísticas de confiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0,893	0,889	8

Teniendo en referencia a Herrera (1998, 101) los valores hallados pueden ser comprendidos entre la siguiente

Tabla:

0,53 a menos Confiabilidad nula

0,54 a 0,59 Confiabilidad baja

0,60 a 0,65 Confiable

0,66 a 0,71 Muy Confiable

0,72 a 0,99 Excelente confiabilidad

1.0 Confiabilidad perfecta

La medida obtenida del coeficiente de confiabilidad es excelentemente confiable.

Prueba de concordancia de Kendall, para la validación de contenidos:

Se utilizó la prueba de concordancia de Kendall para la validez de contenido, con la cual se midió el grado de concordancia entre un grupo de expertos (K = 3) y un conjunto de ítems (n). La respuesta es ordinal. Siendo la hipótesis nula es que no hay concordancia: W=0; y la hipótesis alterna afirma la concordancia, es decir (W > 0). Este estadístico sigue una $\chi 2$, con grados de libertad: n-1. El valor resultante es:

Estadísticos de prueba	
N	22
W de Kendall	0.205
Chi-Cuadrado	9
gl (grados de libertad)	2
Sig (valor de p)	0.011

De acuerdo a los resultados obtenidos se acepta la hipótesis alterna es decir que existe concordancia entre las opiniones de los expertos y que este valor es significativo ($p < 0.05$).

Luego de la validación del modelo se procede a contrastar la hipótesis analizando los siguientes indicadores:

Indicador 1: Nivel porcentual de actitud proactiva respecto al nivel de impacto en los procesos de negocio afectados como resultado de la gestión de riesgos de TI en la institución.

De las 4 universidades privadas que respondieron al cuestionario (Ver anexo N° 01) en el procesamiento de la pregunta 14 (Ver Anexo N° 03, gráfico N°13), se evidencia el nivel porcentual de actitud proactiva respecto al nivel de impacto de los procesos de negocio afectados, que al ser evaluado con respecto a los resultados de la ejecución, la información del nivel de impacto de los procesos de negocio afectados, en el caso de estudio, se formula de la siguiente manera:

Indicador	Nivel porcentual
Nivel porcentual de actitud proactiva antes de la ejecución del modelo de gestión de riesgos	25%
Nivel porcentual de actitud proactiva después de la ejecución del modelo de gestión de riesgos	100%

Del análisis de los resultados se desprende que se mejora el nivel porcentual de actitud de proactiva en un valor promedio de 75%, dada la información de los proyectos generados en el proceso de tratamiento de los riesgos, para la reducción del impacto de los procesos de negocio afectados en la institución.

Indicador 2: Número de proyectos propuestos de gestión de riesgos

En la evaluación de la situación problemática que motivo el desarrollo de la presente tesis, se determinó que los miembros de los grupos de interés involucrados para enfrentar alguna vulnerabilidad materializada por la activación de alguna amenaza, adoptaban respuestas de carácter reactivo que generaban altos costos de corrección, no se tenían proyectos organizados que hayan sido propuestos con anticipación.

La ejecución del modelo propuesto en la presente tesis, aplicado al caso de estudio de la universidad privada, bajo un enfoque de simplicidad y

flexibilidad, mostró como resultado (Ver Anexo N° 05, Tabla N°11) la Identificación de 73 riesgos, de los cuales 11 se determinaron de alta prioridad, que serían mitigados a través de la ejecución de 5 proyectos en el proceso de tratamiento de los mismos.

Indicador 3: Número de riesgos detectados por procesos de negocio

Como resultado del reconocimiento de la situación problemática abordado por la presente investigación los miembros de los grupos de interés involucrados, manifiestan tener información de la existencia de metodologías y estándares de gestión de riesgos de TI, sin embargo las características de alta complejidad, que consecuentemente requieren un índice de tiempo del cual no disponen para una gestión de riesgos propiamente dicha.

Para medir el indicador de número de riesgos detectados por procesos de negocio, se implementó para el caso de estudio el modelo propuesto validado por juicio de expertos (Ver Anexo N°06) lográndose bajo el criterio de simplicidad a través de sólo 8 plantillas, la identificación de 73 riesgos calificándose como prioritarios 11 riesgos los cuales afectan a todos los procesos de negocio soportados por TI.

CAPÍTULO IV: CONCLUSIONES

1. Como producto acreditable de la presente tesis se propuso el modelo de gestión de riesgos basado en estándares adaptados a las TI que soportan los procesos para contribuir a la generación de valor en las universidades privadas de la región Lambayeque, que se validó por 3 profesionales expertos, quienes aceptaron el modelo validando las características de flexibilidad y simplificación de procesos que promuevan una cultura de gestión de riesgos de TI en estas organizaciones, como se explica en el análisis de resultados. (Ver el instrumento de validación en el Anexo N° 06).

2. Se valoró la implementación del modelo de gestión de riesgos de TI validado, aplicándolo en un caso de estudio en una universidad privada de la región, verificando contribuir a la generación de valor, identificando 73 riesgos, categorizando 11 como alta prioridad, apoyando la efectiva toma de decisiones.

3. En la ejecución del modelo de gestión de riesgos desarrollado en la presente tesis, se lograron identificar 11 riesgos calificándolos como de alta prioridad, los cuales serán tratados en los 5 proyectos formulados que promueven una toma de decisiones de carácter proactivo. Estos resultados contribuye a evitar el comportamiento reactivo para corregir efectos de un riesgo materializado.

4. Con la ejecución del modelo de gestión de riesgos propuesto se demuestra que con características de procesos simplificados es posible mapear los 74 riesgos identificados, en un esquema de priorización, con una lectura semaforizada que permite al encargado de la gestión de las tecnologías de información, proponer proyectos para el tratamiento de los mismos de manera proactiva, definiendo los recursos requeridos y las actividades de mejora continua.

REFERENCIAS BIBLIOGRÁFICAS

ISACA. COBIT 5 enabling information. Rolling Meadows Ill. 2013.

ISACA. COBIT 5 for risk. Rolling Meadows, Ill. 2013.

ISACA. COBIT 5 a business framework for the governance and management of enterprise IT. Rolling Meadows, Ill. 2012.

Caralli, Richard A. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, 2007.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I. Madrid, Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones, 2012.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II. Madrid, Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones, 2012

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro III. Madrid, Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones, 2012

Draper, Rick. Using AS/NZS 4360: 1999 Risk Management in Security Risk Analysis. Browns Plains, Old: International Security Management & Crime Prevention Institute, 2000.

Kurt, Dillard, Pfost Jared, and Ryan Stephen. The Security Risk Management Guide. Microsoft Corporation - TechNet, 2006.

Ramírez, A. Ortiz Z. Gestión de Riesgos tecnológicos basado en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios, 2011.

Varun Arora. Comparing different information security standards: Cobit vs ISO 27001, 2005.

ANEXOS

ANEXO 1: Cuestionario para Director de TI

1. ¿En el organigrama de la Institución ¿de quién depende el área de TI?

2. ¿Se ha elaborado un plan estratégico de TI?

3. ¿Cuáles son los objetivos del área de TI y cuáles son los parámetros que se han definido para evaluar su cumplimiento?

4. ¿Cuáles son las funciones del área de TI y quienes son los responsables? Implementar, mantener y velar por el bueno del software creado.

5. ¿El personal de TI posee las competencias y habilidades adecuadas para cumplir con su función, cuáles son los parámetros de medición?
   Si, se mide mediante experiencias de trabajos anteriores y cursos de especialidad.

6. ¿El centro de datos y cuartos de comunicaciones cuentan con ambientes apropiados para su correcto funcionamiento? (aire acondicionado, área mínima, sistema de protección eléctrico, extintores, piso técnico, falso techo, etc.)

7. ¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados por TI?

8. ¿Se cuenta con un inventario de activos de TI?

9. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?

10. ¿La alta dirección es informada sobre los riesgos a los que se encuentran expuestos los activos de TI?

11. ¿Se ha cuantificado las pérdidas económicas relacionadas a la falta de servicios de TI?

12. ¿Se han identificado los riesgos asociados a los proveedores de servicios internos / externos? (Internet, energía eléctrica, etc.)

13. ¿Cómo califica usted las acciones (Proactiva/Reactiva) para solucionar las incidencias de TI a lo largo del último año?

Actividad/ Proceso/ Servicio	**Proactivo(1) /Reactivo (2)**	**Descripción de criterio**

14. ¿En el instrumento que se muestra a continuación, valore la probabilidad de ocurrencia y el impacto que causaría para la institución, eventos relacionados con las tecnologías que brindan soporte a sus procesos?

			PROBABILIDAD					IMPACTO				
Actividad/Proceso/Servicio	**Proactivo (1) / Reactivo (2)**	**Descripción de criterio**	**Casi imposible**	**Raro**	**Posible**	**Muy posible**	**Casi ciert o**	**Insignificante**	**Menor**	**Medio**	**Mayor**	**Catastrófico**

ANEXO 2: Resultado del cuestionario para director de TI

	Universidad 01	Universidad 02	Universidad 03	Universidad 04
1. En el organigrama de la Institución ¿de quién depende el área de TI?	Gerencia General	Desconoce	Gerencia General	Gerencia General
2. ¿Se ha elaborado un plan estratégico de TI?	Si	No	SI	NO
3. ¿Cuáles son los objetivos del área de TI y cuáles son los parámetros que se han definido para evaluar su cumplimiento?				
3.1 - Cuenta con Objetivos establecidos	SI	SI	NO	SI
3.2 - ha definido parámetros para evaluar el cumplimiento de sus objetivos	NO	NO	NO	SI
4. ¿Cuáles son las funciones del área de TI y quienes son los responsables?				
	Cobit 5-APO04 - Gestionar la Innovación	Cobit 5-APO03 - Administrar la Arquitectura Empresarial	Cobit 5-APO05 - Gestionar la Cartera	Cobit 5-APO04 - Gestionar la Innovación
	Cobit 5-BAI09 - Gestionar los Activos	Cobit 5-DSS03 - Asegurar la Optimización del Riesgo	Cobit 5-DSS03 - Gestionar los Problemas	Cobit 5-BAI09 - Gestionar los Activos
	Cobit 5-APO12 - Gestionar el Riesgo	Cobit 5-DSS02 - Asegurar la Entrega de Beneficios	Cobit 5-BAI07 - Gestionar la Aceptación del Cambio y de la Transición	Cobit 5-APO12 - Gestionar el Riesgo
	Cobit 5-APO07 - Gestionar los Recursos Humanos			Cobit 5-APO07 - Gestionar los Recursos Humanos
	Cobit 5-EDM01 - Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno			Cobit 5-EDM01 - Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno

	Universidad 01	Universidad 02	Universidad 03	Universidad 04
	Cobit 5-BAI03 - Gestionar la Identificación y la Construcción de Soluciones			Cobit 5-BAI03 - Gestionar la Identificación y la Construcción de Soluciones
	Cobit 5-APO02 - Gestionar la Estrategia			Cobit 5-APO02 - Gestionar la Estrategia
	Cobit 5-APO06 - Gestionar el Presupuesto y los Costos			Cobit 5-APO06 - Gestionar el Presupuesto y los Costos
5. ¿El personal de TI posee las competencias y habilidades adecuadas para cumplir con su función, cuáles son los parámetros de medición?				
5.1 El personal de TI Posee competencias y habilidades adecuadas para cumplir con su función	SI	SI	SI	SI
5.2 Ha definido parámetros para medir las competencias y habilidades del personal de TI	Si	NO	NO	SI
6. ¿El centro de datos y cuartos de comunicaciones cuentan con ambientes apropiados para su correcto funcionamiento? (aire acondicionado, área mínima, sistema de protección eléctrico, extintores, piso técnico, falso techo, etc.)	SI	SI	SI	SI
7. ¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados por TI?	SI	SI	SI	SI
8. ¿Se cuenta con un inventario de activos de TI?	SI	NO	SI	SI
9. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?	SI	NO	SI	SI

	Universidad 01	Universidad 02	Universidad 03	Universidad 04
10. ¿La alta dirección es informada sobre los riesgos a los que se encuentran expuestos los activos de TI?	SI	NO	SI	SI
11. ¿Se ha cuantificado las pérdidas económicas relacionadas a la falta de servicios de TI?	NO	NO	NO	NO
12. ¿Se han identificado los riesgos asociados a los proveedores de servicios internos / externos? (Internet, energía eléctrica, etc.)	NO	NO	NO	NO

ANEXO 3: Grafico del resultado de las encuestas

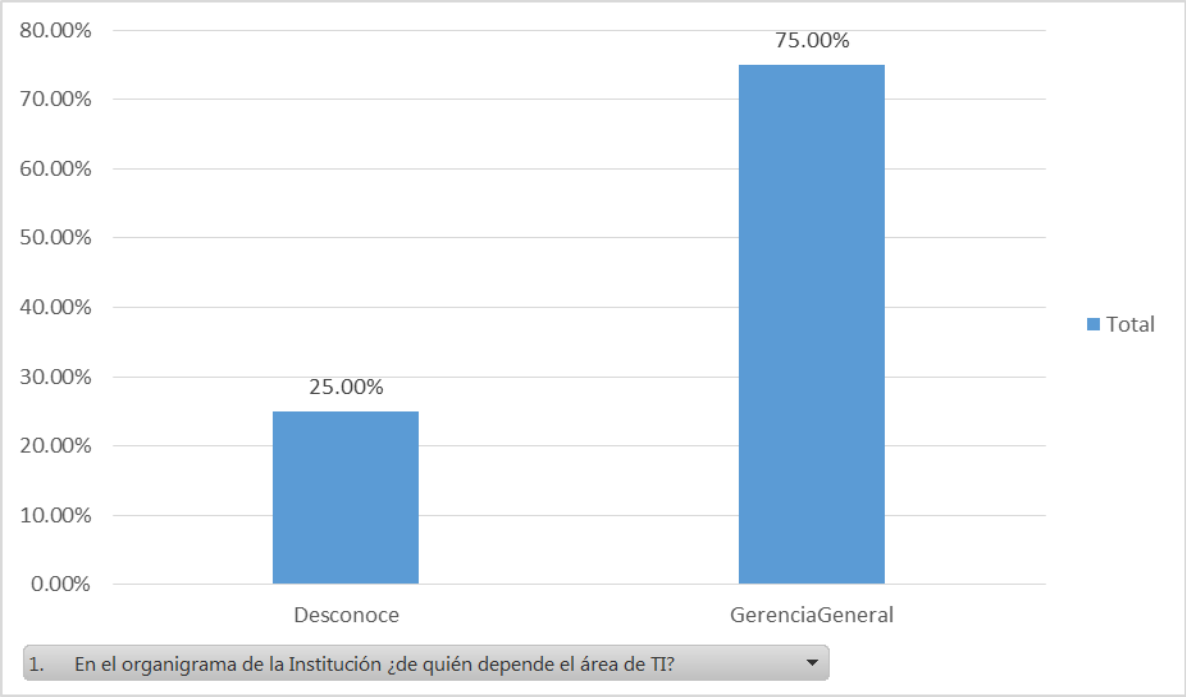


Gráfico 01: En el organigrama de la Institución ¿de quién depende el área de TI?

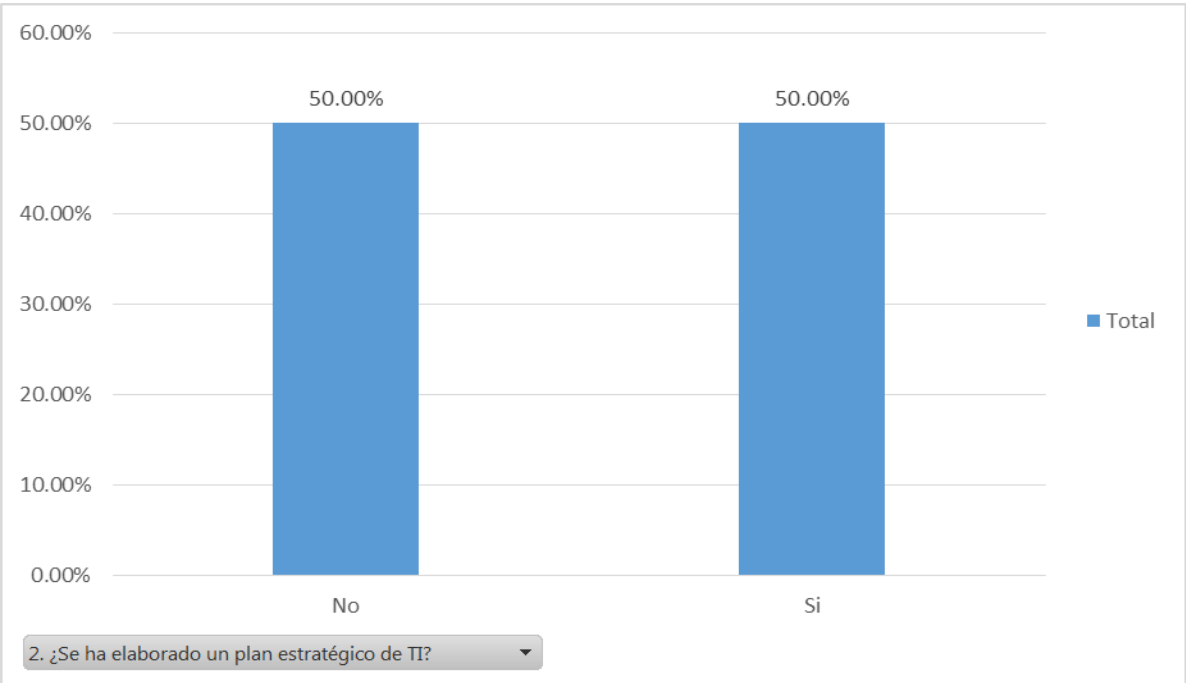


Gráfico 02: ¿Se ha elaborado un plan estratégico de TI?

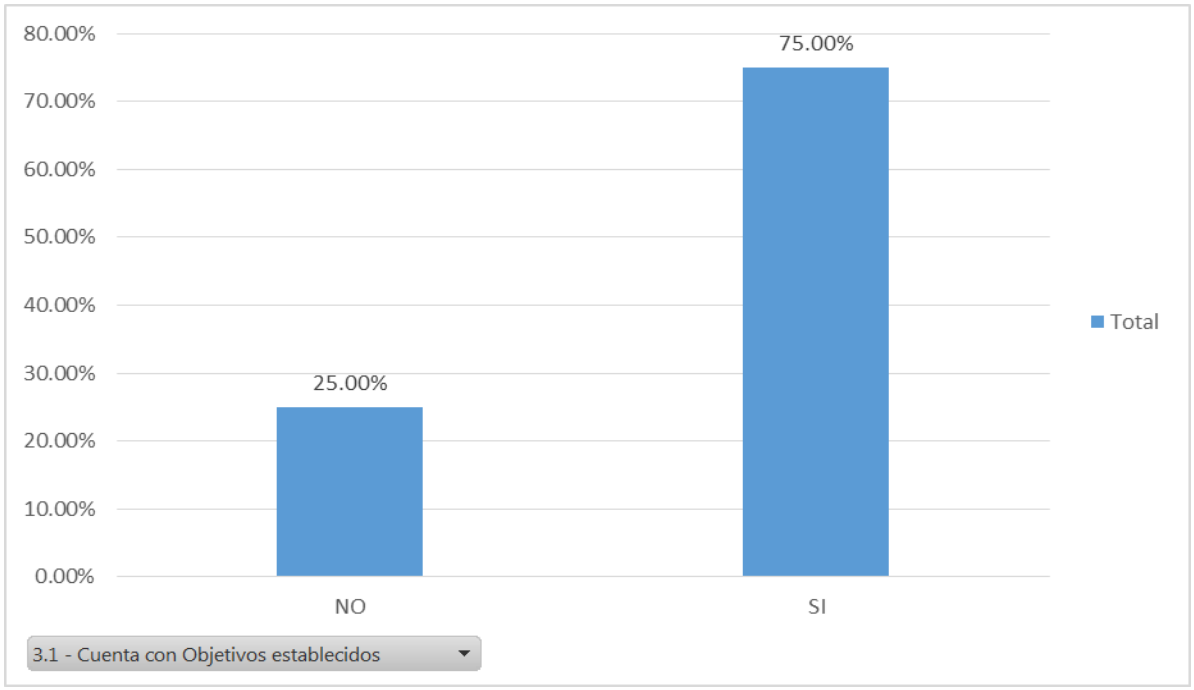


Gráfico 03.1: Cuenta con Objetivos establecidos

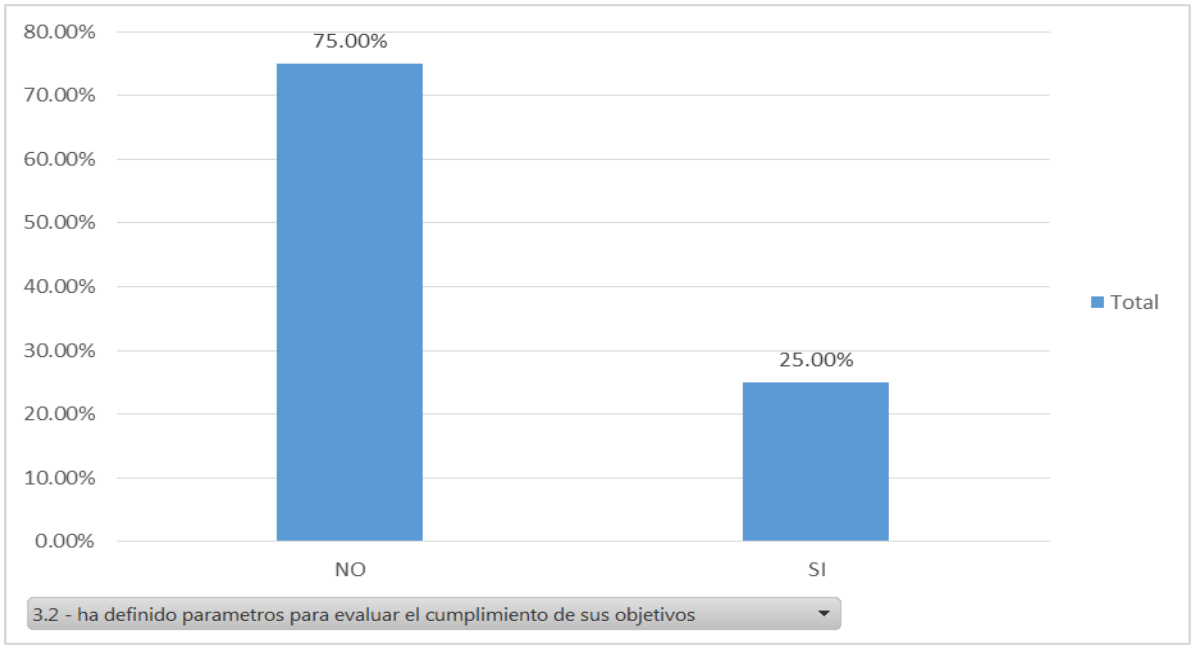


Gráfico 03.2: ha definido parámetros para evaluar el cumplimiento de sus objetivos

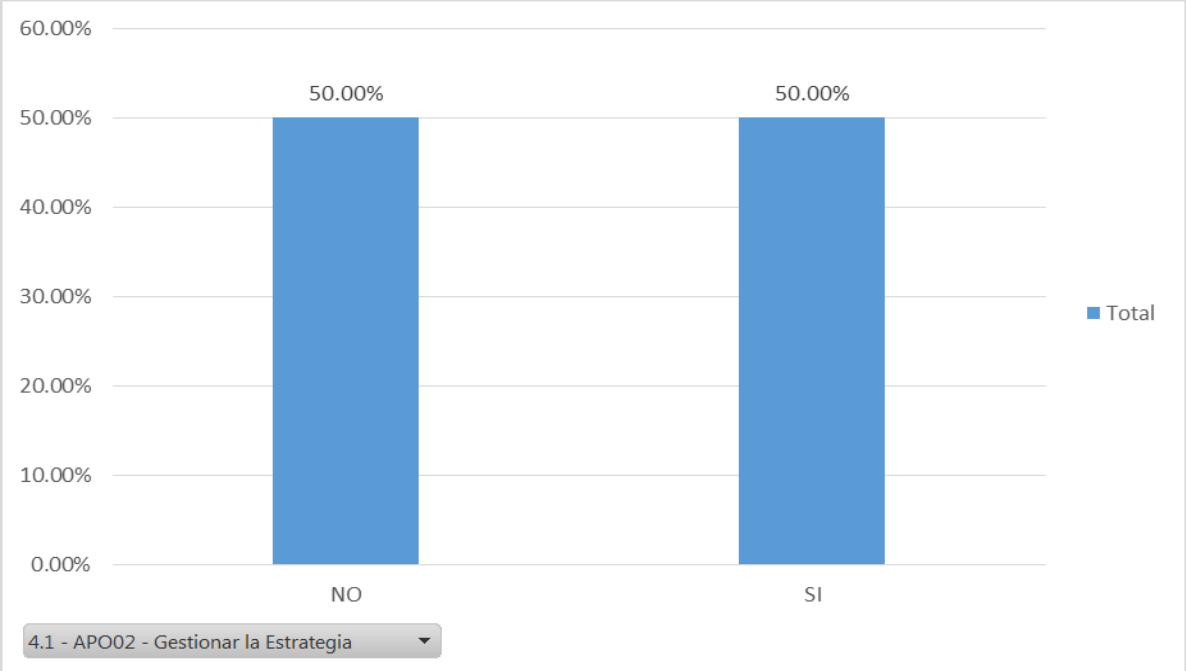


Gráfico 4.1: Cobit5-APO02 - Gestionar la Estrategia

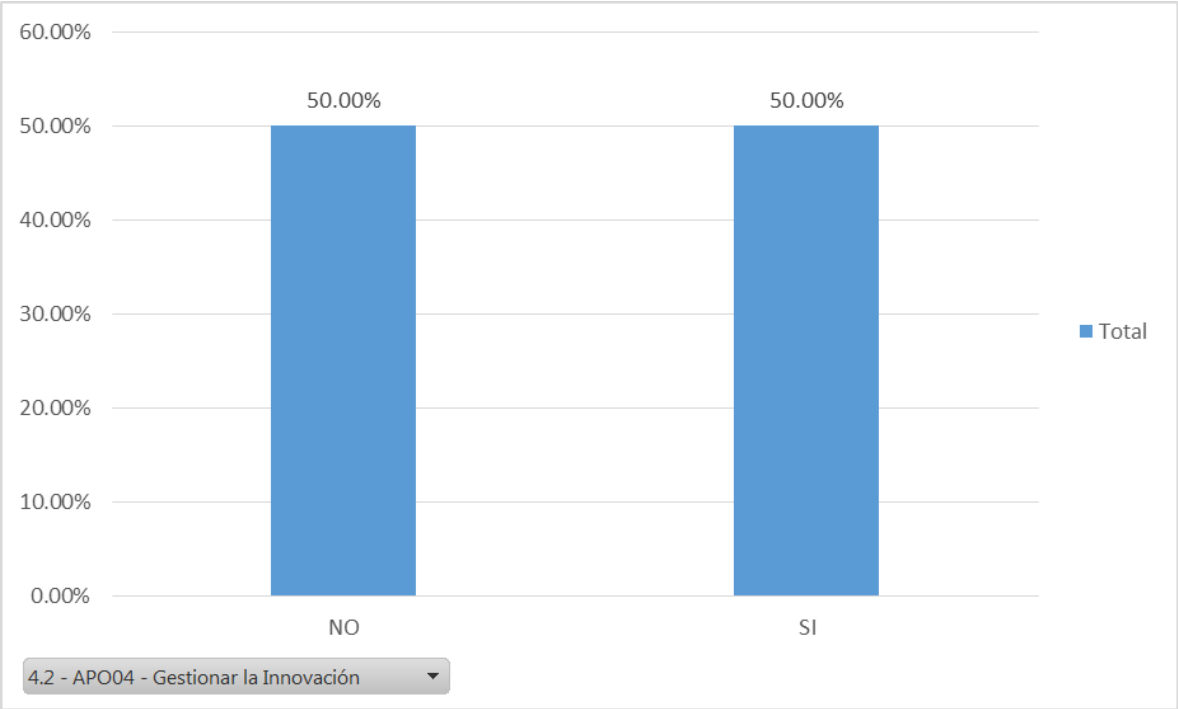


Gráfico 4.2: Cobit5-APO04 - Gestionar la Innovación

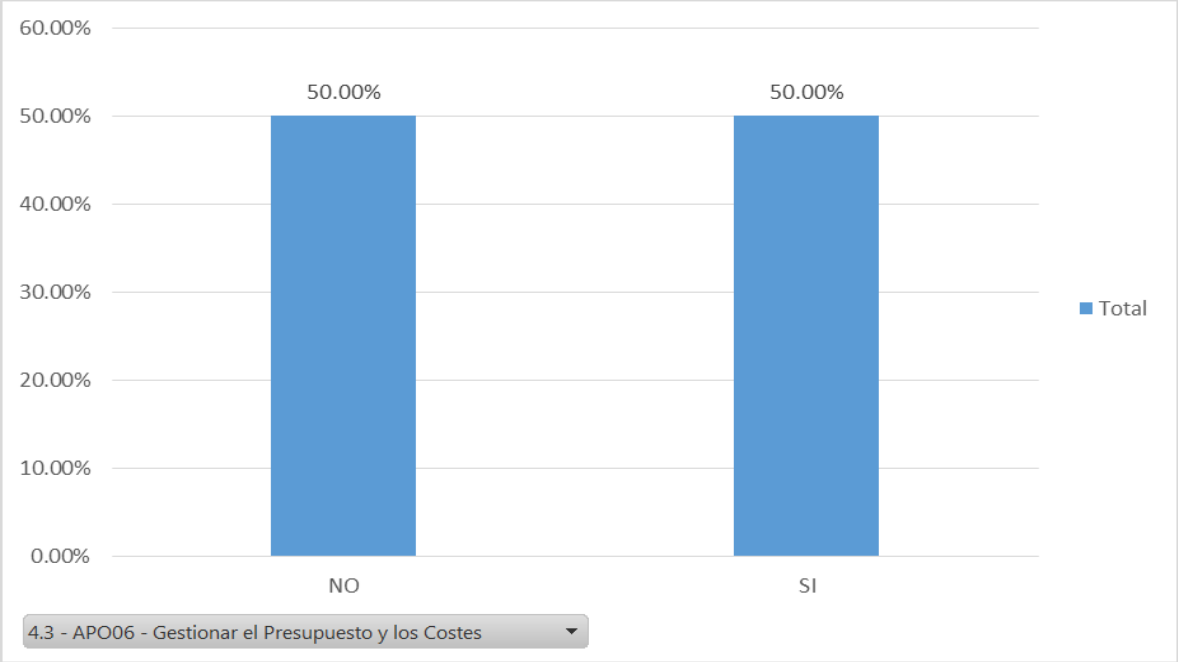


Gráfico 4.3: Cobit5-APO06 - Gestionar el Presupuesto y los Costos

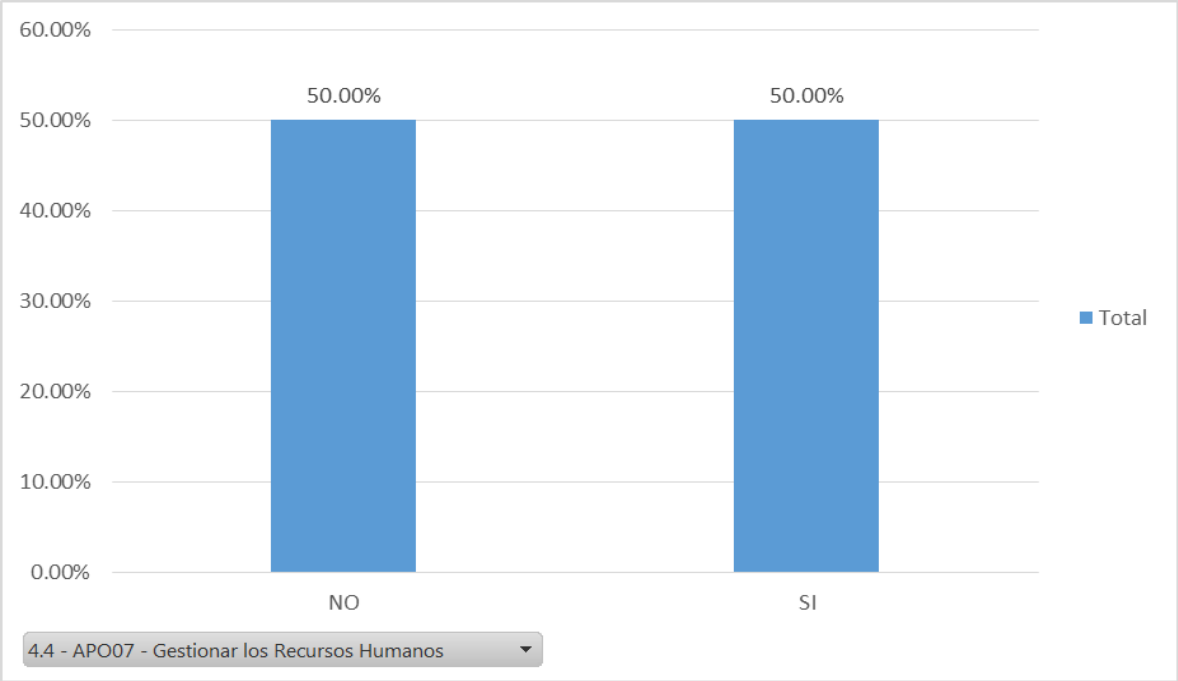


Gráfico 4.4: Cobit5-APO07 - Gestionar los Recursos Humanos

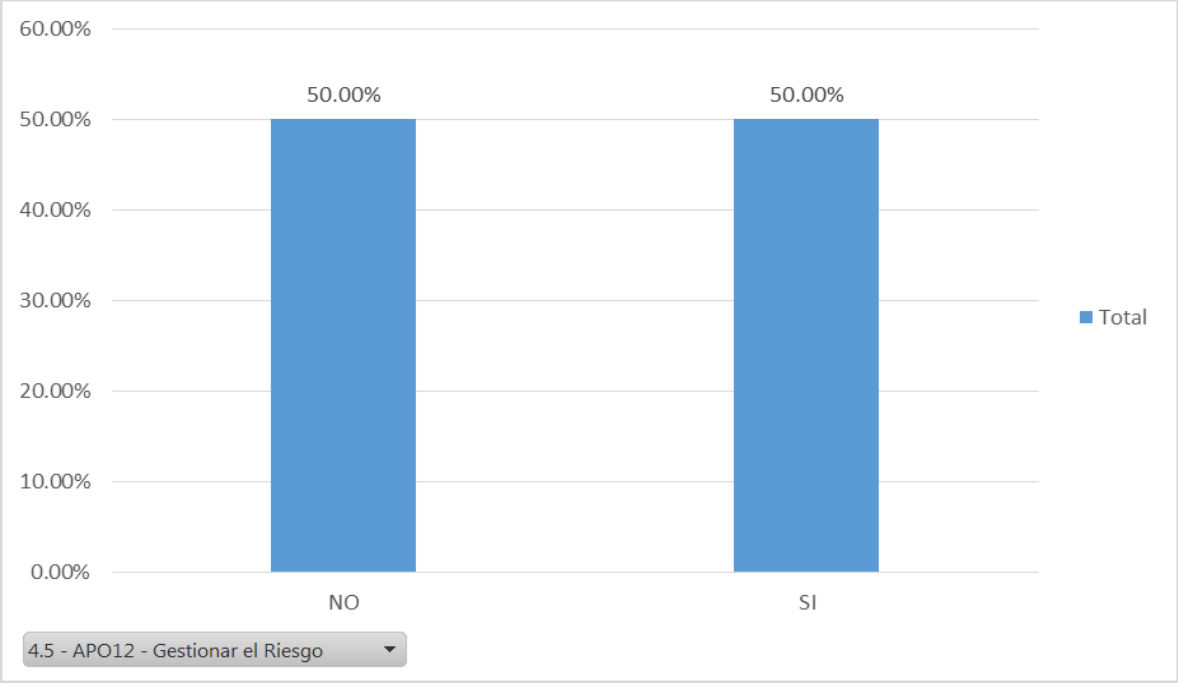


Gráfico 4.5: Cobit5-APO12 - Gestionar el Riesgo

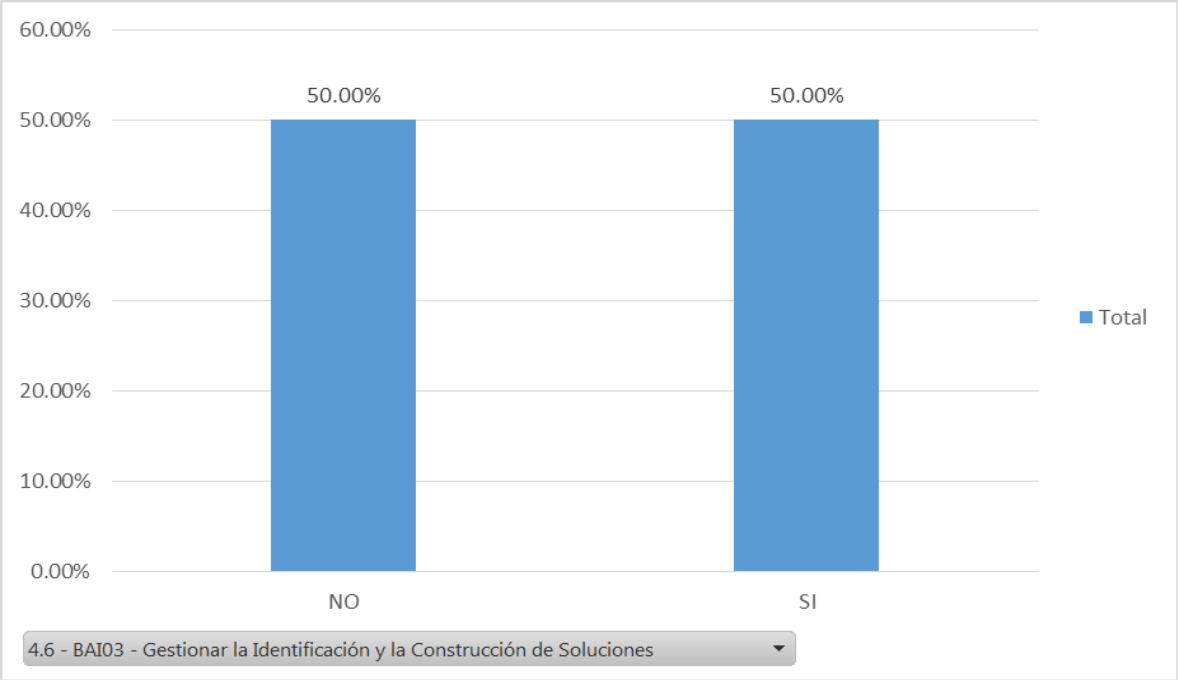


Gráfico 4.6: Cobit5-BAI03 - Gestionar la Identificación y la Construcción de Soluciones

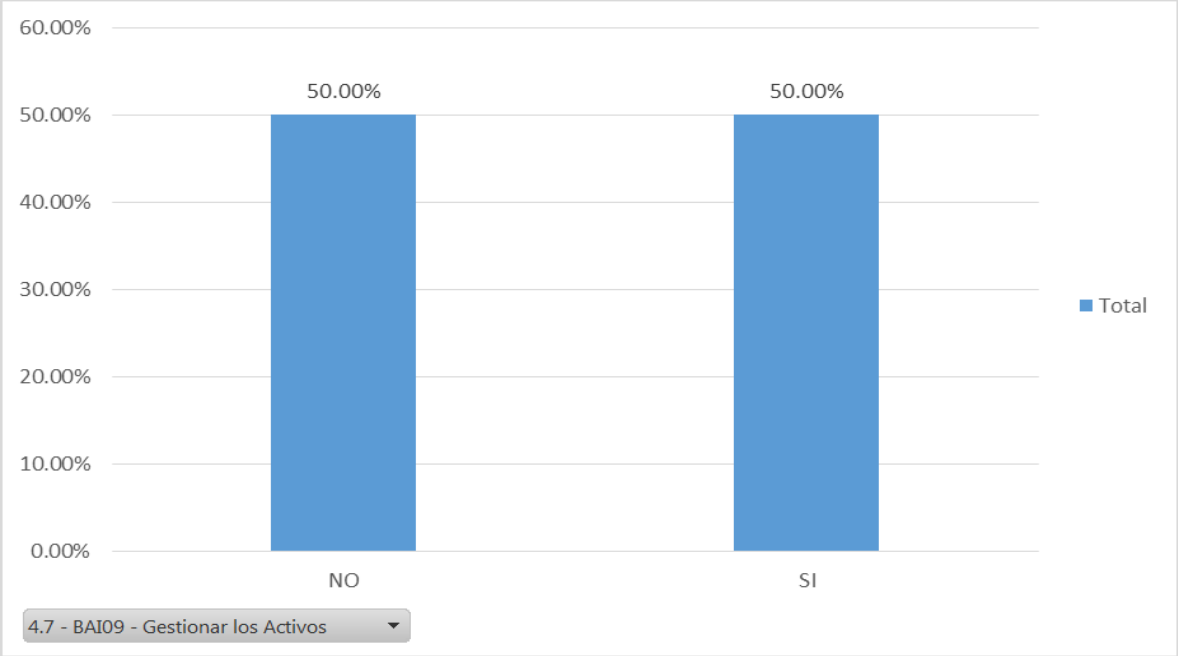


Gráfico 4.7: Cobit5-BAI09 - Gestionar los Activos

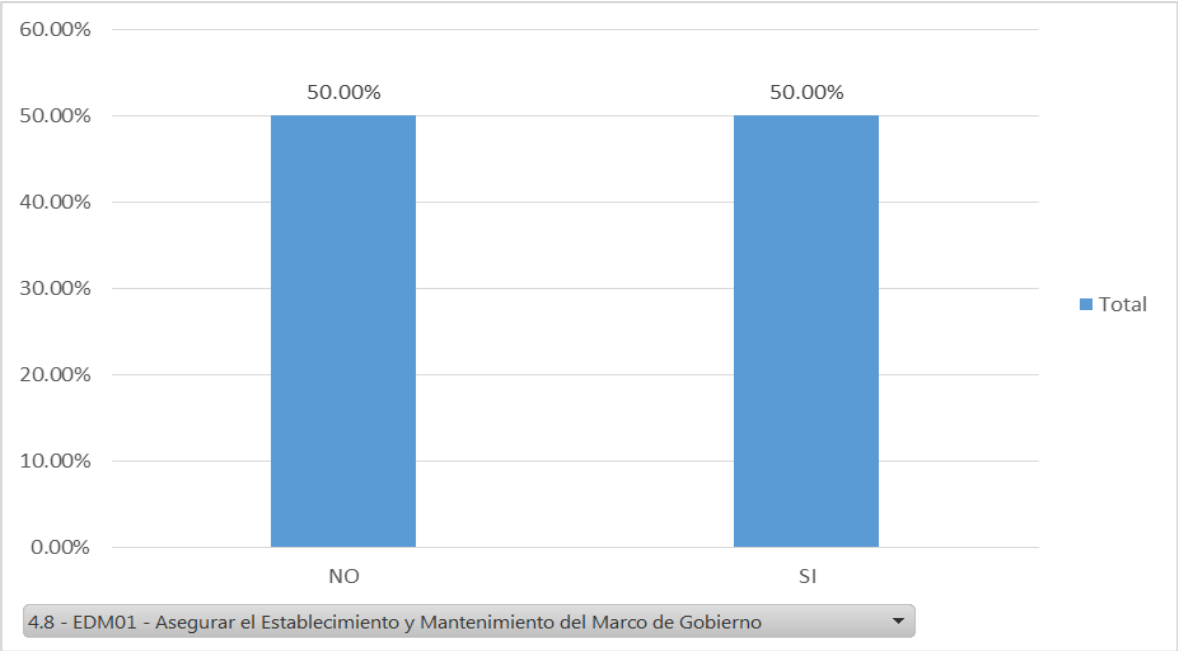


Gráfico 4.8: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno

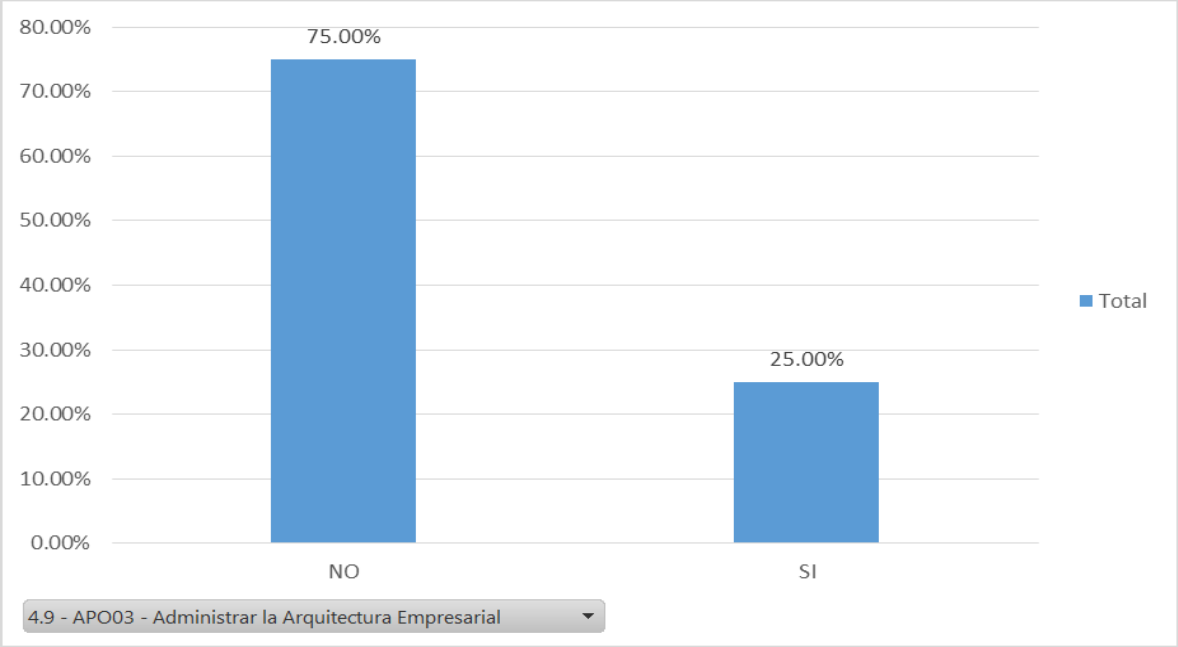


Gráfico 4.9: Cobit5-APO03 - Administrar la Arquitectura Empresarial

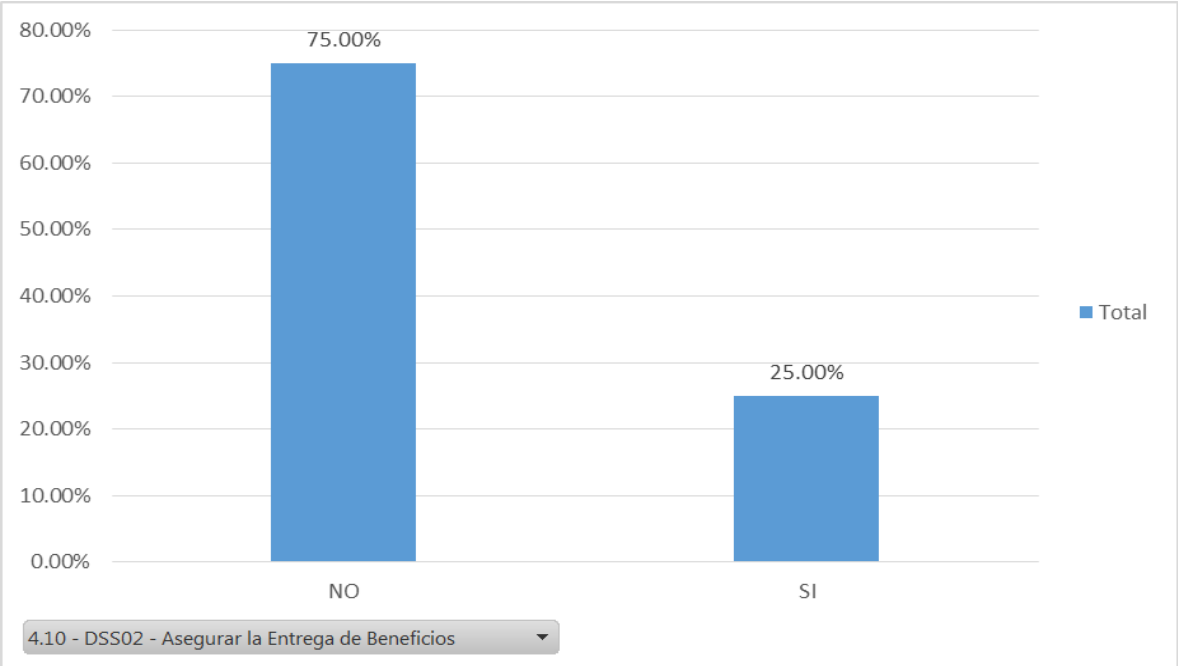


Gráfico 4.10: Cobit5-DSS02 - Asegurar la Entrega de Beneficios

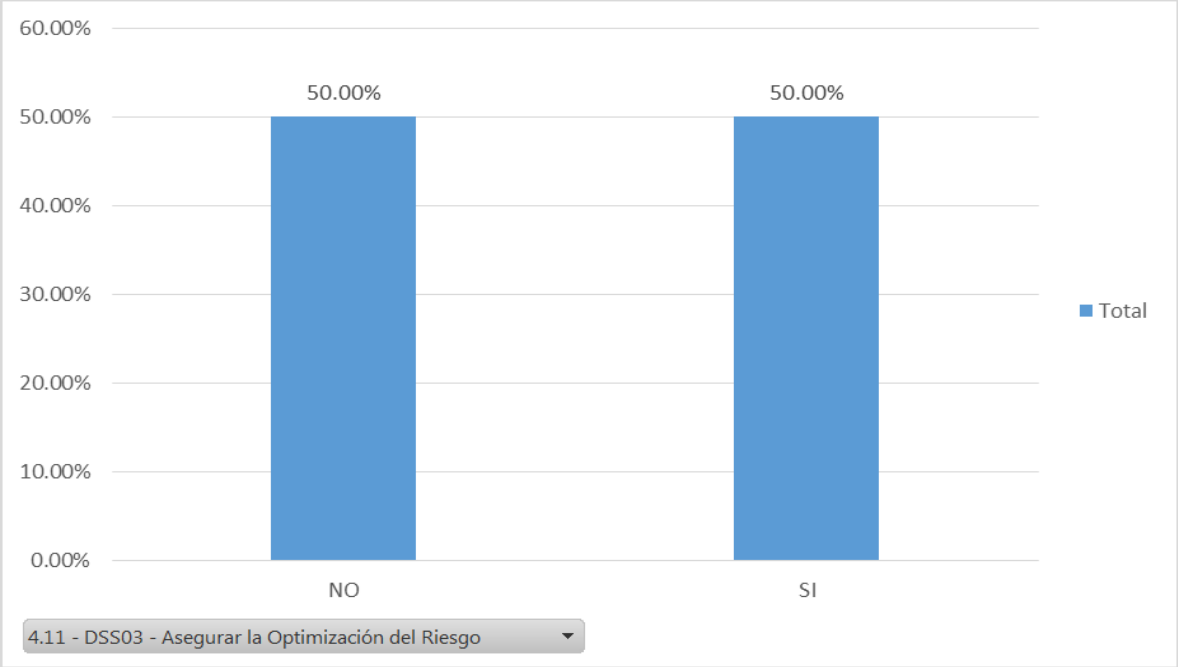


Gráfico 4.11: Cobit5-DSS03 - Asegurar la Optimización del Riesgo

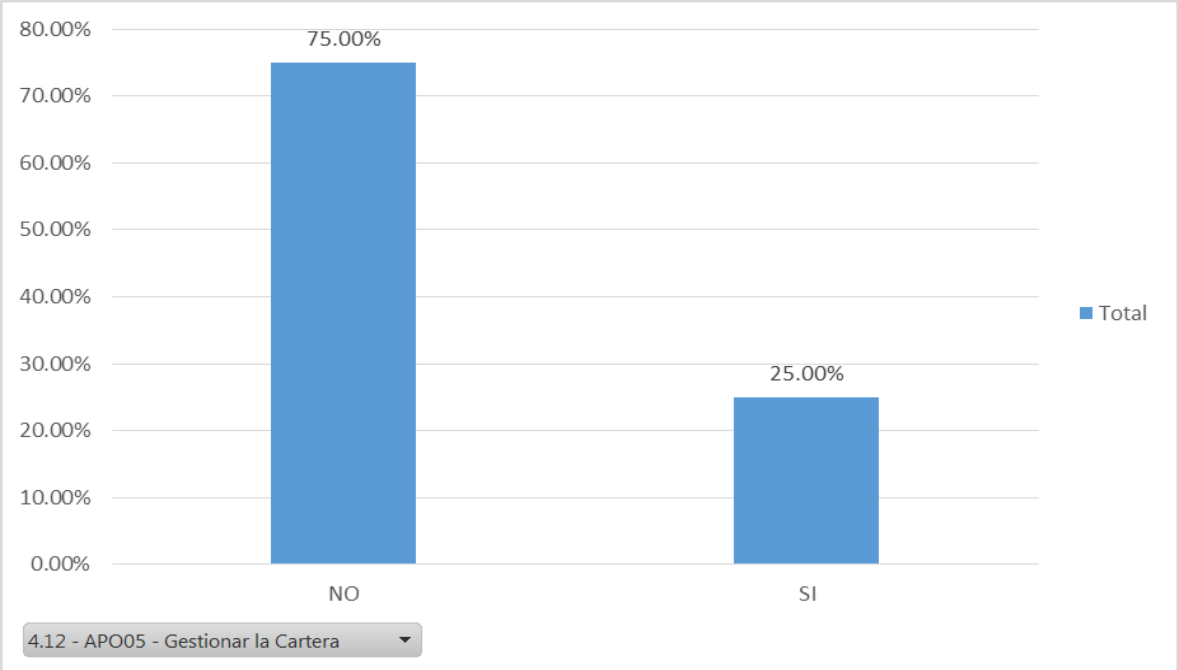


Gráfico 4.12: Cobit5-APO05 - Gestionar la Cartera

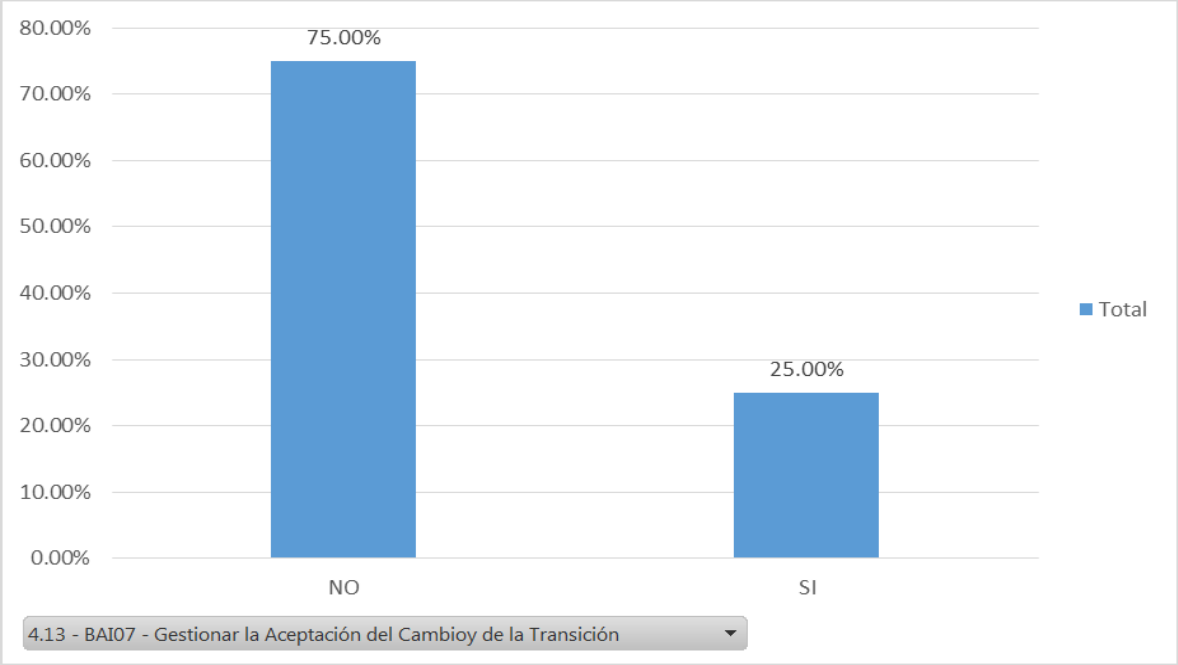


Gráfico 4.13: Cobit5-BAI07 - Gestionar la Aceptación del Cambio y de la Transición

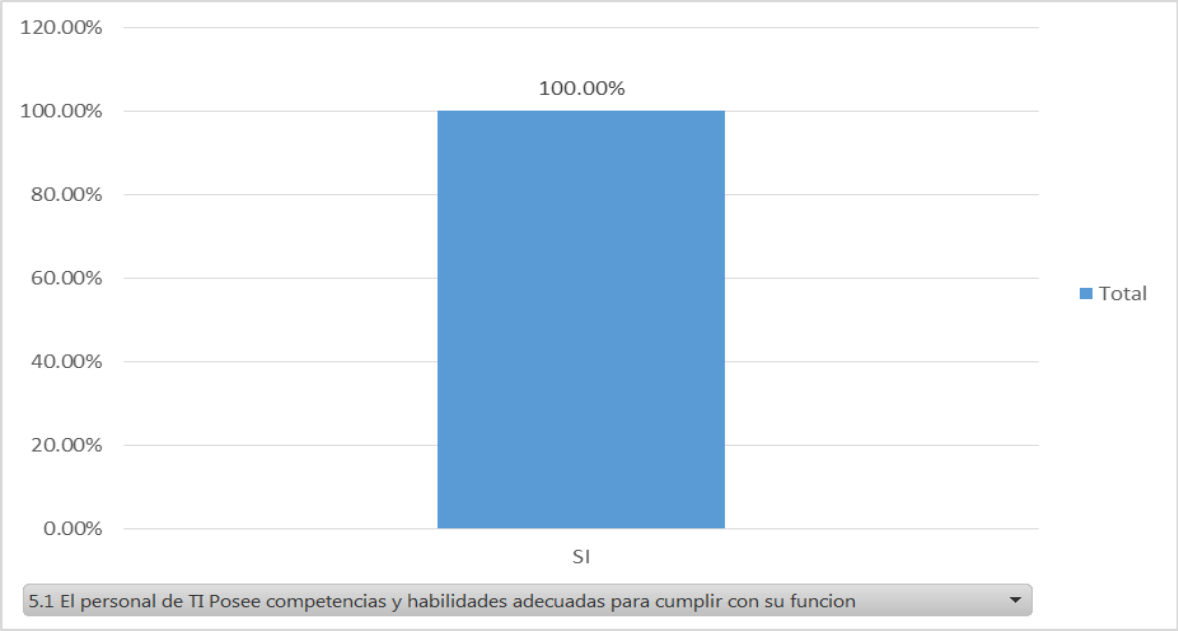


Gráfico 5.1: El personal de TI Posee competencias y habilidades adecuadas para cumplir con su función

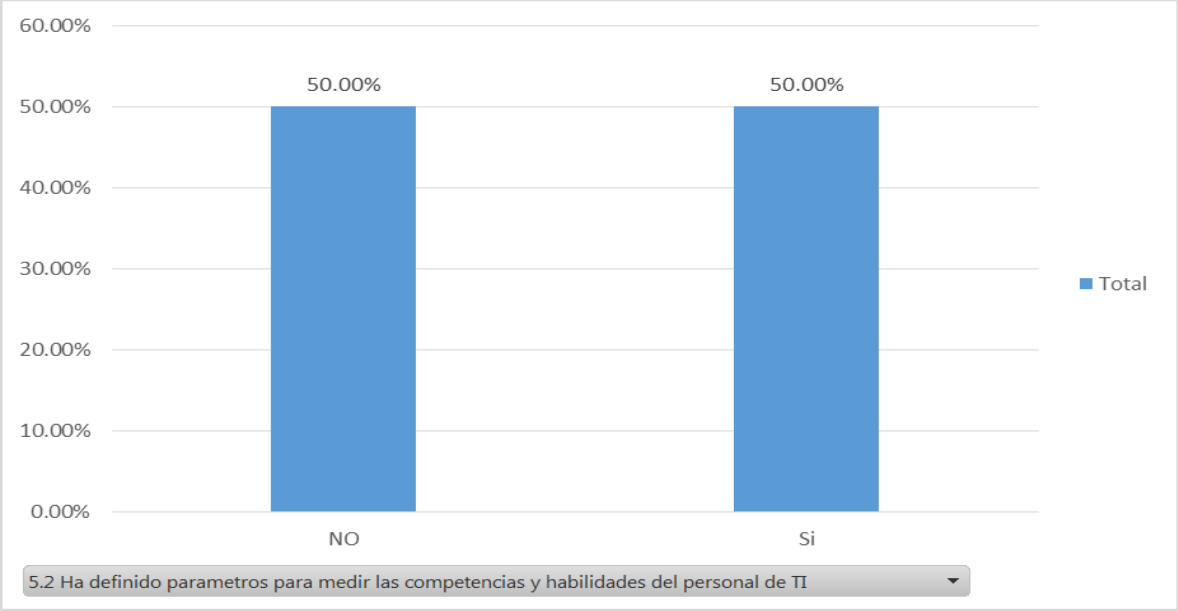


Gráfico 5.2: Ha definido parámetros para medir las competencias y habilidades del personal de TI

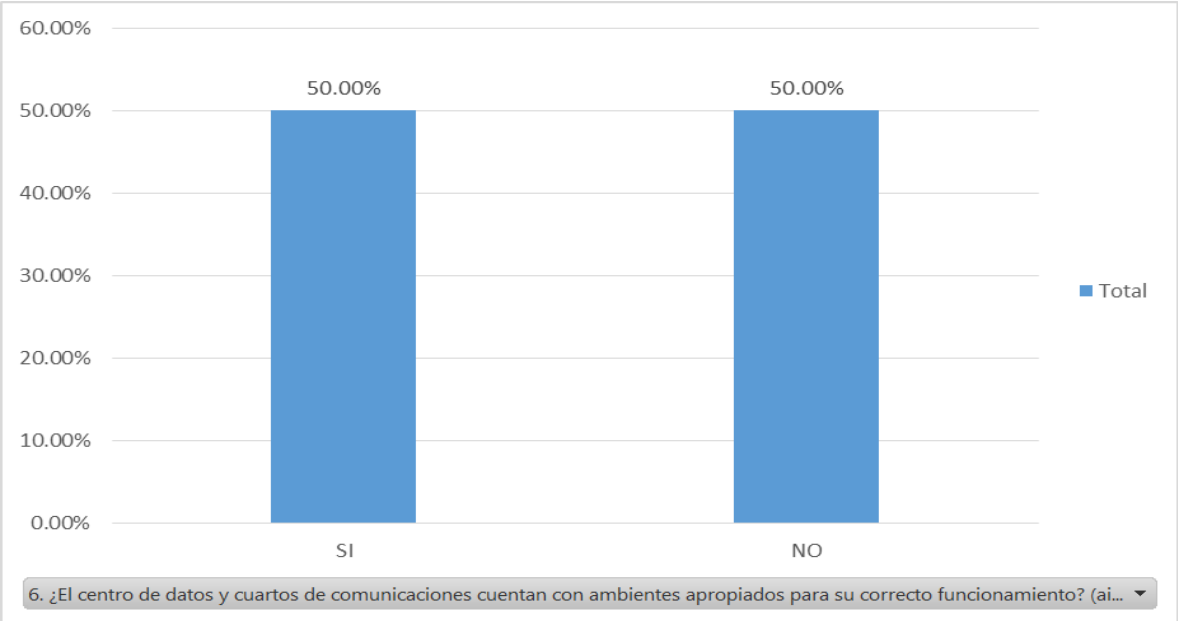


Gráfico 6: ¿El centro de datos y cuartos de comunicaciones cuentan con ambientes apropiados para su correcto funcionamiento?

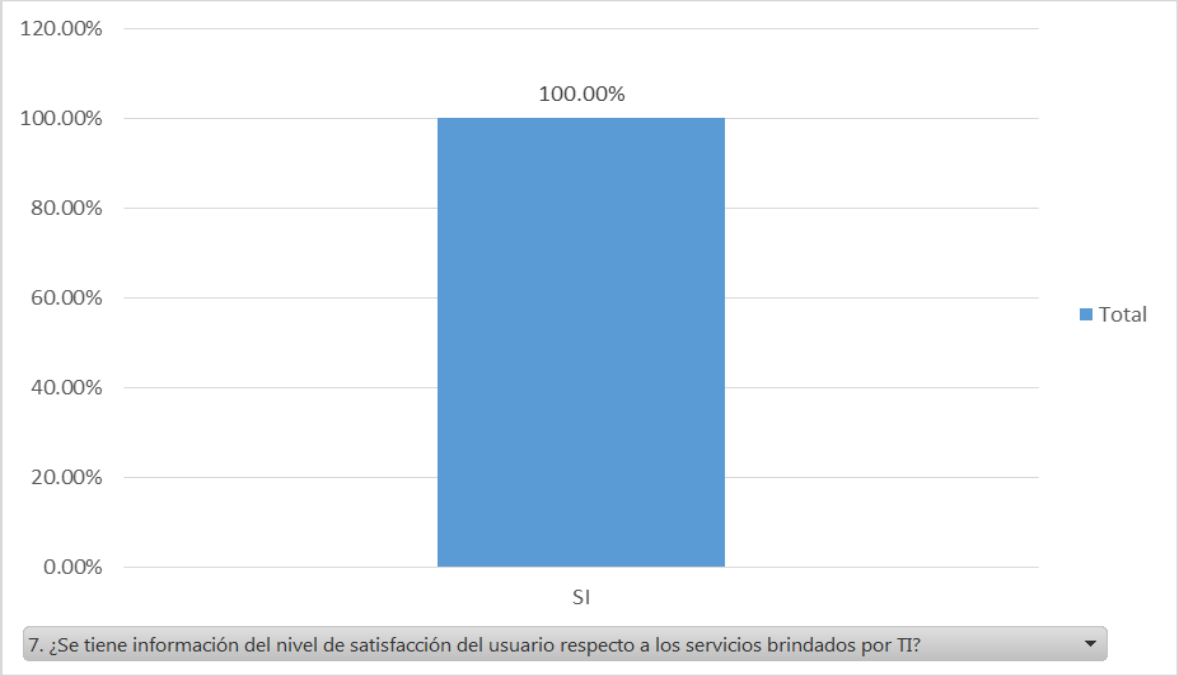


Gráfico 7: ¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados por TI?

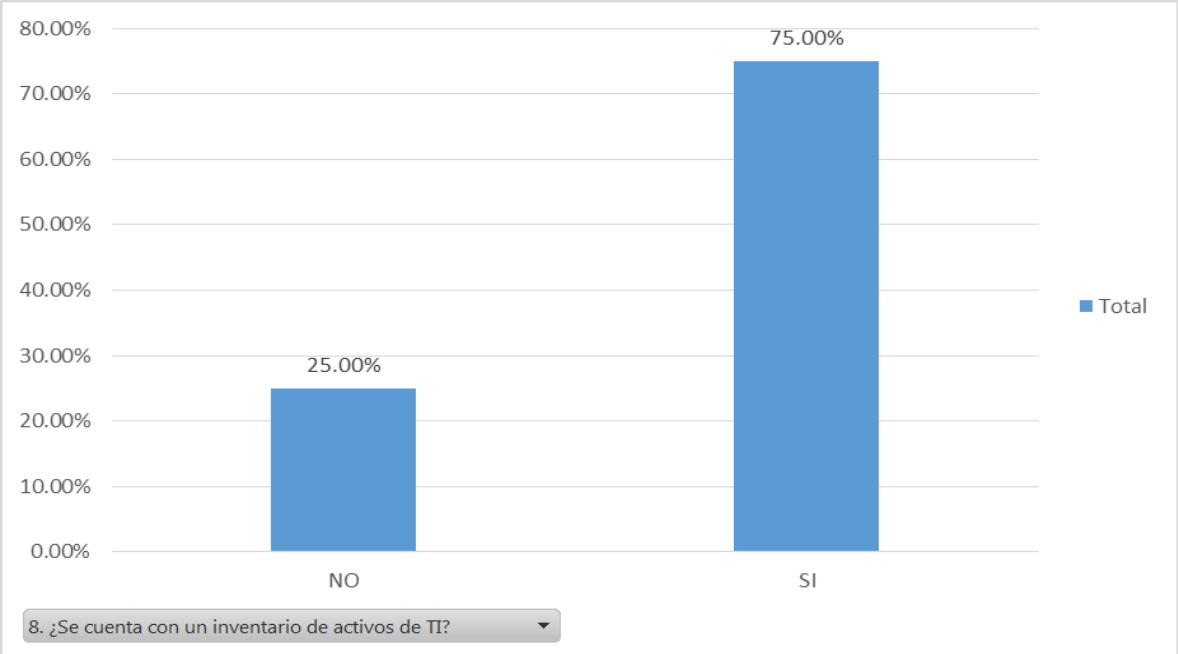


Gráfico 8: ¿Se cuenta con un inventario de activos de TI?

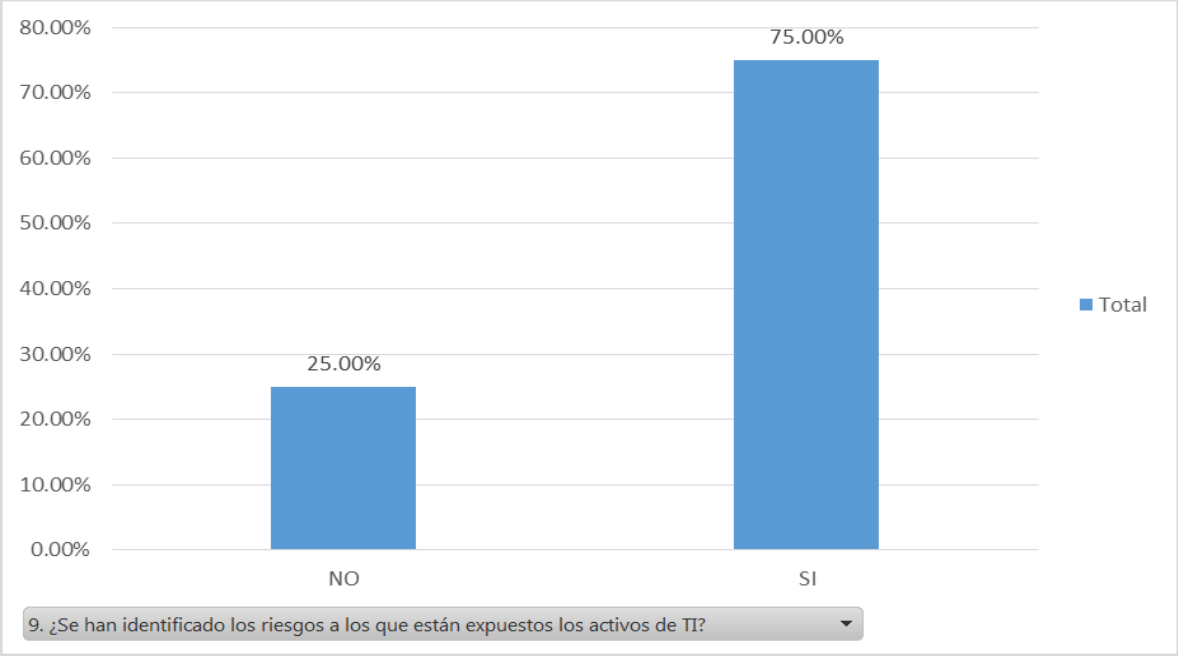


Gráfico 9: ¿Se han identificado los riesgos a los que están expuestos los activos de TI?

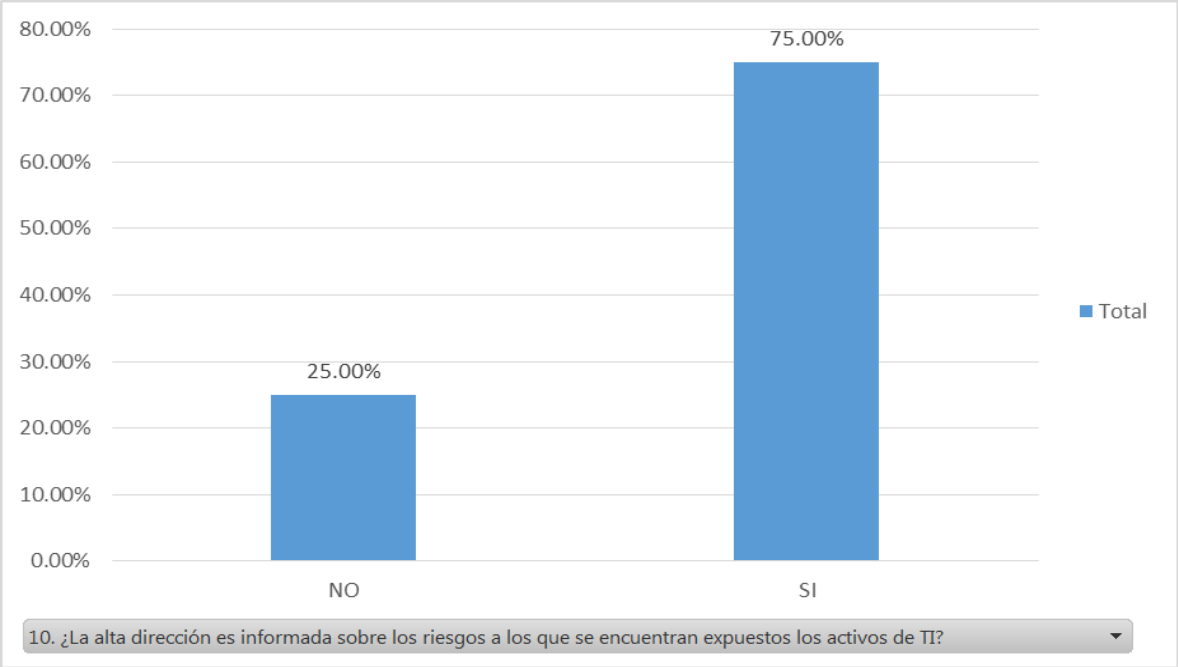


Gráfico 10: ¿La alta dirección es informada sobre los riesgos a los que se encuentran expuestos los activos de TI?

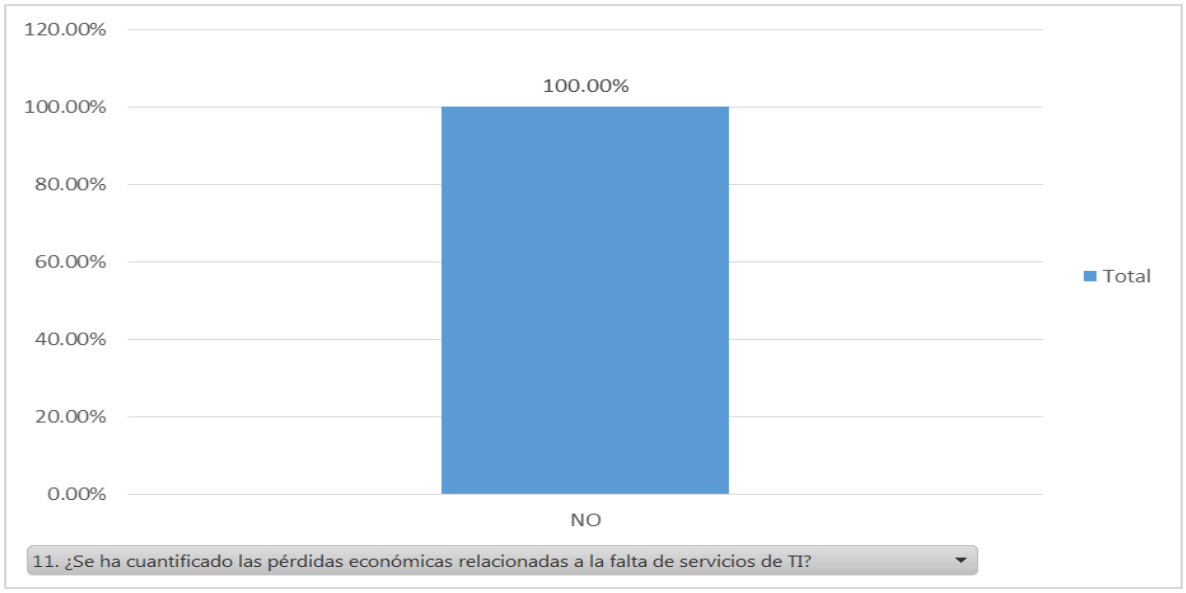


Gráfico 11: ¿Se ha cuantificado las pérdidas económicas relacionadas a la falta de servicios de TI?

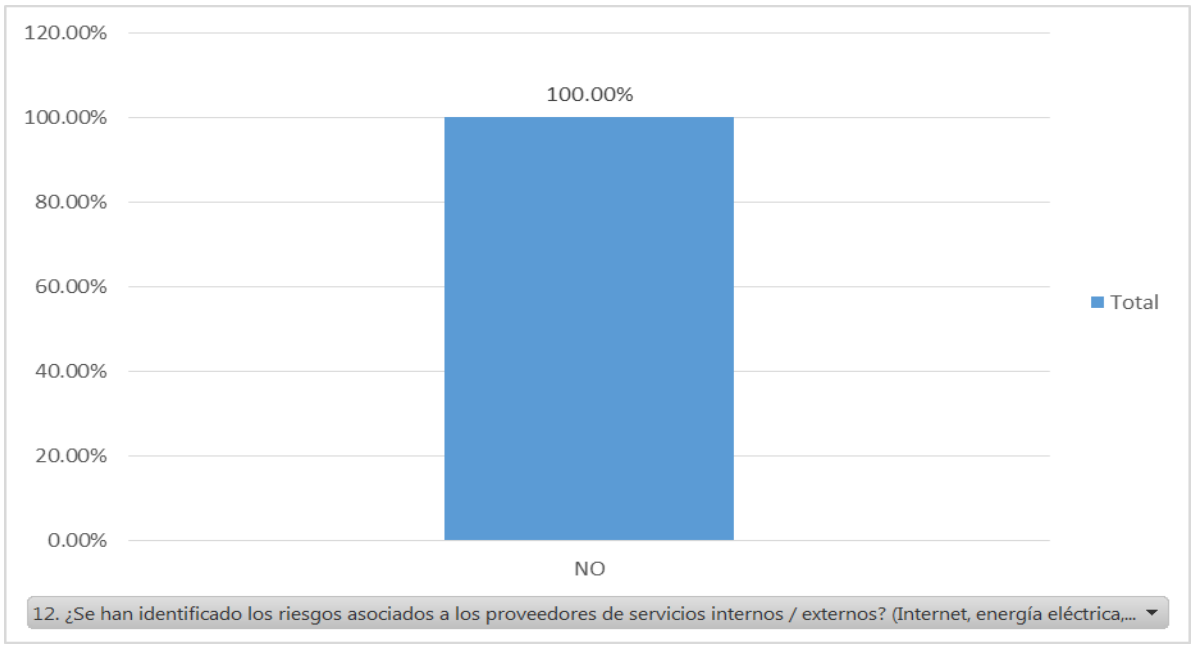


Gráfico 12: ¿Se han identificado los riesgos asociados a los proveedores de servicios internos / externos?

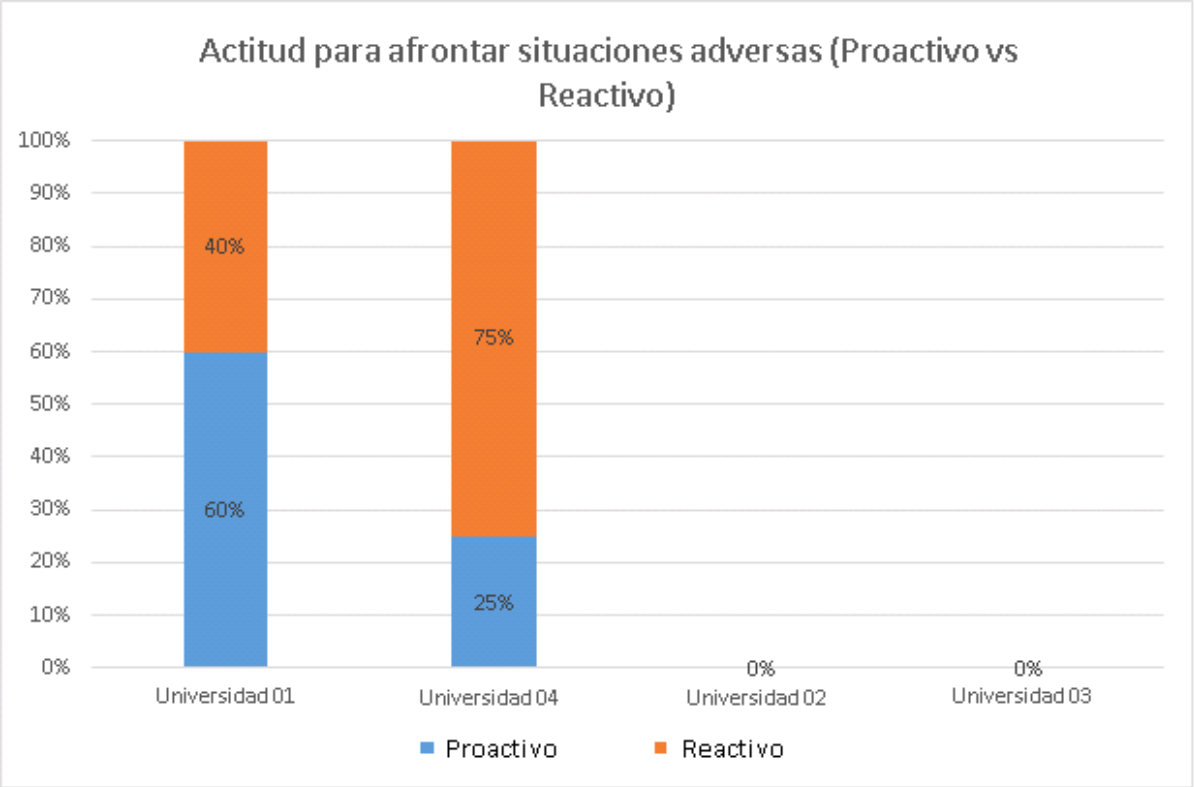


Gráfico 13: Actitud para afrontar situaciones adversas (Extraído de pregunta N°14 de Cuestionario para Director de TI)

ANEXO 4: Interpretación del resultado de las encuestas

Según lo encontrado en las encuestas se pudo observar que en un 75% las áreas de TI dependen de la Gerencia General, el 50% cuenta con un plan estratégico de TI, el 75% ha establecido sus objetivos pero solo el 25% ha definido parámetros para evaluar el logro de sus objetivos, evidenciando un escaso monitoreo que retroalimente la necesidad de revisiones periódicas en el área.

Las funciones del área de TI no se encuentran claramente definidas, se alinearon las funciones de TI según lo indicado por COBIT para poder comparar las diferentes realidades, de la cual se pudo determinar: que el 50% gestionan la innovación, el 50% gestionan su presupuesto, 50% gestionan sus recursos humanos, 50% gestionan sus riesgos, 50% gestionan la identificación y construcción de sus soluciones, 50% gestionan sus activos, 50% aseguran el establecimiento y mantenimiento del marco de gobierno, 25% administran la arquitectura empresarial, 25% aseguran la entrega de beneficios, 50% aseguran la optimización del riesgo, 25% gestionan la cartera de sus proyectos, 25% gestiona la aceptación del cambio y de la transición. Según los resultados se evidencia que en promedio no se han alcanzado los parámetros porcentuales que evidencien una efectiva gestión de los activos de TI, para garantizar la continuidad del negocio.

Con respecto al personal, el 100% indica que sus trabajadores tienen las habilidades y competencias adecuadas pero solo el 50% ha definido parámetros para medirlas, por lo tanto evidencia una respuesta subjetiva que pone en riesgo la gestión de los requerimientos de mejora, en respuesta al monitoreo y revisión.

El 50% indica que el ambiente de su centro de datos es el adecuado y 50% no tienen claro que debe tener un centro de datos para contar con un ambiente adecuado.

El 100% mide el nivel de satisfacción de sus usuarios, pero no evidencia resultados de retroalimentación continua.

El 75% cuenta con un inventario de activos de TI, han identificado los riesgos relacionados a estos activos y han informado a alta dirección sobre estos riesgos, sin embargo no se mide el índice de frecuencia por lo que no se valora la necesidad de invertir en las tecnologías de información.

El 100% desconoce el impacto económico de la ocurrencia de un riesgo, no se ha definido los riesgos que traen consigo sus proveedores.

ANEXO 5: Ejecución del modelo de gestión de riesgos caso de aplicación universidad privada XYZ

Fases I - Establecimiento de contextos

1.1. Contextos Internos

1.1.1. Cultural: Se define como el conjunto de conocimientos que permite identificar las características del negocio, para definir los escenarios de comportamiento en cuanto a los actores que pertenecen al mismo, como son: estudiantes, docentes, administrativos, padres de familia, tecnología de información y autoridades.

1.1.2. Partes internas involucradas: Se define como las interrelaciones que se establecen entre cada uno de los actores del sistema, mencionados en el punto anterior, dando lugar a los procesos soportados por las tecnologías de información que definen la naturaleza del giro del negocio agrupándose en procesos académicos y administrativos.

1.1.3. Estructura: Se define como el conjunto de componentes organizacionales de acuerdo a la función que se le asigna según los requerimientos de la institución, que para el caso de instituciones educativas de nivel superior son de tipo vertical por su estructuración, pero desde el sentido funcional es de forma transversal por su naturaleza colaborativa.

1.1.4. Recursos: Se define como el conjunto de activos que componen la infraestructura tecnológica que dan soporte a los procesos de las instituciones de superior privadas como servidores, equipos de cómputo escritorio o portátiles, equipos de red, sistema de protección eléctrica, etc.

1.1.5. Metas y objetivos: Se define como el conjunto de ideas rectoras de las instituciones educativas superior privadas que apuntan a la calidad educativa y a la acreditación universitaria.

1.2. Contextos Externos

1.2.1. Ambiente del negocio: es un conjunto de elementos existentes fuera de la organización que tienen el potencial de afectar en su desempeño como las fuentes laborales de las empresas, proveedoras de servicios e insumos.

Fuentes Laborales:

De Servicio:

- Molinos
- Restaurantes
- Hoteles
- Servicios Turísticos
- Transportes terrestre
- Hospitales

De Comercialización

- Farmacias
- Electrodomésticos
- Supermercados
- Equipos de Cómputo
- Entidades financieras

De Producción

- San Roque
- Backus
- Agroindustrias

Gubernamentales

- Gobierno Regional de Lambayeque
- Municipalidad de Chiclayo
- Municipalidad de Ferreñafe
- Municipalidad distrital de Etén
- Municipalidad distrital de Reque

RENIEC- Chiclayo

INEI – Chiclayo

1.2.2. Social y cultural:

Familias de niveles socioeconómicos A, B, C.

Empresas: grandes, medianas, pequeñas y micro.

1.2.3. Normativos y Financieros

ANR

SUNEDU

Ministerio de Educación

INDECI

SUNAT

Colegios Profesionales

Entidades de Acreditación

SBS

SUNARP

Poder Judicial-Lambayeque

1.2.4. Competencia:

Universidades Privadas de la región

Universidades Nacionales de la Región Norte.

1. Político:

Constitución Política del Perú

Código Deontológico de los colegios profesionales

Normas de revalidación Internacional

Fase II - Identificación de activos

1. Clasificación de activos**:**

1.1. Procesos de Negocio [P]:

Tabla Nº 1: Catálogo Proceso de Negocios

Ítem	Catálogo Procesos de Negocio	Etiqueta
1	Gestión de personal	[P_GEPer]
2	Gestión de pensiones	[P_GEPen]

3	Gestión de tutoría	[P_GETut]
4	Gestión administrativa	[P_GAdm]
5	Gestión de Contabilidad	[P GCont]
6	Gestión curricular	[P_GCurr]
7	Gestión académica	[P_GAcad]
8	Gestión Aula virtual	[P_GAula]

1.2. Servicios [S]:

Tabla Nº 2: Catálogo servicios

Ítem	Catálogo Servicio	Etiqueta
1	Servicio Campus Virtual	[S_CamVir]
2	Servicio Aula Virtual	[S_AulaVir]
3	Servicio correo electrónico	[S_Email]
4	Central telefónica	[S_CenTel]
5	Acceso Internet inalámbrico	[S_WIFI]

1.3. Aplicaciones y Software [App]:

Tabla Nº 3: Catálogo software

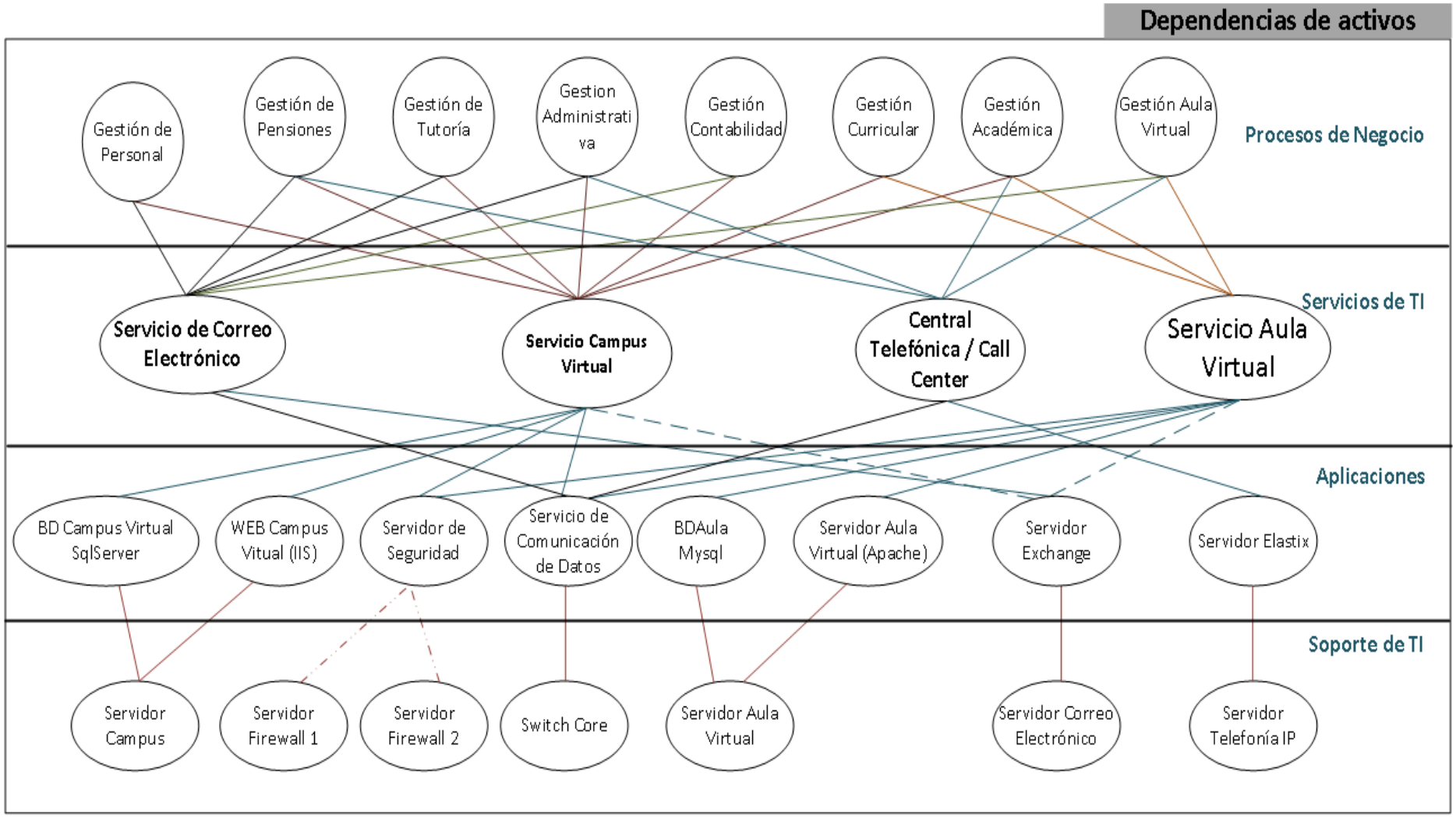
Ítem	Catálogo Software	Etiqueta
1	BD Campus Virtual	[App_BDCamp]
2	Web Campus Virtual	[App_WebCamp]
3	Servidor de seguridad	[App_Seg]
4	Servicio de comunicación de datos	[App_SrvCom]
5	BD Aula MySQL	[App_BDAula]
6	Servicio de Telefonía IP	[App_TelIP]

1.4. Soporte **de TI** [Sop]:

Tabla Nº 4: Catálogo soporte

Ítem	Catálogo Soporte	Etiqueta
1	Servidor Campus	[Sop_Camp]
2	Servidor Firewall 1	[Sop_FW1]
3	Servidor Firewall 2	[Sop_FW2]
4	Switch Core	[Sop_SWCore]
5	Servidor Aula Virtual	[Sop_Aula]
6	Servidor Correo electrónico	[Sop_Email]
7	Servidor telefonía IP	[Sop_TelIp]

2. Dependencia de activos:



3. Valoración de activo

Tabla Nº 5: Valoración de Criterio de Disponibilidad

DISPONIBILIDAD	
VALOR	CRITERIO
1	No aplica/No es relevante
2	Debe estar disponible al menos el 10% del tiempo
3	Debe estar disponible al menos el 50% del tiempo
4	Debe estar disponible al menos el 75% del tiempo
5	Debe estar disponible al menos el 95% del tiempo

Tabla Nº 6: Valoración de Criterio de Integridad

INTEGRIDAD	
VALOR	CRITERIO
1	No aplica / No es relevante
2	No es relevante los errores que tenga o la información que falte
3	Tiene que estar correcto y completo al menos en un 50%
4	Tiene que estar correcto y completo al menos en un 70%
5	Tiene que estar correcto y completo al menos en un 95%

Tabla Nº 7: Valoración de Criterio de Confidencialidad

CONFIDENCIALIDAD	
VALOR	CRITERIO
1	No aplica / No es relevante.
2	Daños muy bajos, el incidente no trascendiera del proceso afectado.
3	Daños bajos, el incidente no trascendiera del proceso afectado.
4	Los daños serían relevantes, el incidente implicaría a otros procesos
5	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas

Tabla Nº 8: Tabla de valoración de los niveles de criticidad de activos

Rango	Valor	Descripción	
1 – 3	1	Muy bajo	MB
4– 6	2	Bajo	B
7– 9	3	Medio	M
10 – 12	4	Alto	A
13 – 15	5	Muy alto	MA

Total de Valoración = Confidencialidad + Integridad + Disponibilidad

Tabla Nº 10: Cuadro valoración de activos

Cuadro de valoración de activos							
Activo			**Criterios**				
Categoría	**Código**	**Descripción**	**C**	**I**	**D**	**Total**	
[P]	[P_GEPer]	Gestión de Personal	5	5	5	15	MA
[P]	[P_GEPen]	Gestión de Pensiones	5	5	5	15	MA
[P]	[P_GETut]	Gestión de Tutoría	5	5	3	13	MA
[P]	[P_GEAdm]	Gestión Administrativa	5	5	5	15	MA
[P]	[P_GECont]	Gestión Contabilidad	5	5	5	15	MA
[P]	[P_GECurr]	Gestión Curricular	3	5	4	12	A
[P]	[P_GEAcad]	Gestión Académica	5	5	5	15	MA
[P]	[P_GAula]	Gestión Aula Virtual	5	5	5	15	MA
[S]	[S_CamVir]	Servicio Campus Virtual	5	5	5	15	MA
[S]	[S_AulaVir]	Servicio Aula Virtual	5	4	5	14	MA
[S]	[S_Email]	Servicio correo electrónico	5	4	4	13	MA
[S]	[S_CenTel]	Central telefónica	5	3	3	11	A
[S]	[S_Wifi]	Acceso Internet Inalámbrico	3	1	4	8	M
[App]	[App_BDCamp]	BD Campus Virtual	5	5	5	15	MA
[App]	[App_WebCamp]	Web Campus Virtual	5	3	5	13	MA
[App]	[App_Seg]	Servidor de seguridad	3	3	5	11	A
[App]	[App_SrvCom]	Servicio de comunicación de datos	2	2	5	9	M
[App]	[App_BDAula]	BD Aula MySQL	5	5	5	15	MA
[App]	[App_TelIp]	Servicio de Telefonía Ip	2	3	5	10	A
[Sop]	[Sop_Camp]	Servidor Campus	1	5	5	11	A

Cuadro de valoración de activos							
Activo			**Criterios**				
Categoría	**Código**	**Descripción**	**C**	**I**	**D**	**Total**	
[Sop]	[Sop_FW1]	Servidor Firewall 1	2	5	5	12	A
[Sop]	[Sop_FW2]	Servidor Firewall 2	2	5	5	12	A
[Sop]	[Sop_SWCore]	Switch Core	2	2	5	9	M
[Sop]	[Sop_Aula]	Servidor Aula Virtual	2	5	5	12	A
[Sop]	[Sop_Email]	Servidor Correo electrónico	2	5	5	12	A
[Sop]	[Sop_TelIp]	Servidor telefonía IP	2	5	5	12	A

Fase III – Análisis de riesgos

Nivel	Descripción	
1	Muy bajo	MB
2	Bajo	B
3	Medio	M
4	Alto	A
5	Muy alto	MA

Tabla 24: Nivel de impacto

Probabilidad	Valor	Descripción de probabilidad	
Cada varios años	1	Muy poco frecuente	MB
Una vez al año	2	Poco frecuente	B
Cuatro veces al año	3	Normal	M
Mensualmente	4	Frecuente	A
A diario	5	Muy frecuente	MA

Tabla 25: Probabilidad de ocurrencia

Tabla Nº 13: Categoría de Riesgo

VALOR	CRITERIO
1	Muy bajo
2	Bajo
3	Moderado
4	Alto
5	Muy alto

RANGO	NIVEL DE CRITICIDAD	DESCRIPCIÓN	VISTA SEMÁFORO
1 – 4	1	bajo	
5 - 10	2	Medio	
11 – 25	3	alto	

Tabla 26: Categoría de riesgo semaforizado

Tabla Nº 11: Cuadro identificación y valorización de riesgos

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
1.	[S_CamVir]	Servicio Campus Virtual	Error de usuario (A1)	Carencia de validación de datos entradas en los sistemas	4	M	4	A	R1	3 (16)	A
2.	[S_CamVir]	Servicio Campus Virtual	Escape de Información (A2)	Carencia de Políticas de seguridad	4	A	3	M	R2	3 (12)	A
3.	[S_CamVir]	Servicio Campus Virtual	Alteración accidental de información (A3)	Carencia de programas de capacitación al personal	5	MA	3	M	R3	3 (15)	A
4.	[S_CamVir]	Servicio Campus Virtual	Abuso de Privilegios(A4)	Carencia de Políticas de uso del sistema	5	MA	2	B	R4	2 (10)	M
5.	[S_CamVir]	Servicio Campus Virtual	Acceso no Autorizado (A5)	Ausencia de un sistema de aprovisionamiento de usuarios.	5	MA	2	M	R5	2 (10)	M

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
6.	[S_CamVir]	Servicio Campus Virtual	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos.	2	B	2	B	R6	1 (4)	B
7.	[S_AulaVir]	Servicio Aula Virtual	Error de usuario (A7)	Carencia de conocimiento de uso del aula virtual	2	MB	3	M	R7	2 (6)	M
8.	[S_AulaVir]	Servicio Aula Virtual	Escape de Información (A2)	Carencia de Políticas de seguridad	4	A	3	M	R8	3 (12)	A
9.	[S_AulaVir]	Servicio Aula Virtual	Alteración accidental de información (A3)	Carencia de programas de capacitación al personal	1	MB	3	M	R9	1 (3)	B
10.	[S_AulaVir]	Servicio Aula Virtual	Abuso de Privilegio (A4)	Carencia de Políticas de uso del sistema	5	MA	1	MB	R10	1 (5)	B

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
11.	[S_AulaVir]	Servicio Aula Virtual	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos.	2	B	2	B	R11	1 (4)	B
12.	[S_Email]	Servicio correo electrónico	Escape de Información (A2)	Carencia de Políticas de seguridad	4	A	1	MB	R12	1 (4)	B
13.	[S_Email]	Servicio correo electrónico	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos	2	B	2	B	R13	1 (4)	B
14.	[S_Email]	Servicio correo electrónico	Ingeniería social (A19)	Programas de concientización continua del personal responsable	3	M	3	M	R14	2	B
15.	[S_CenTel]	Central telefónica	Uso no previsto (A8)	Ausencia de políticas de uso del sistema.	2	B	3	M	R15	2	B

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
16.	[S_CenTel]	Central telefónica	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos	1	MB	1	MB	R16	1 (1)	B
17.	[S_Wifi]	Acceso Internet Inalámbrico	Uso no previsto (A8)	Ausencia de políticas de uso del sistema.	1	MB	3	M	R17	1 (3)	B
18.	[S_Wifi]	Acceso Internet Inalámbrico	Acceso no Autorizado (A5)	Ausencia de un sistema de aprovisionamiento de usuarios.	3	M	4	A	R18	3 (12)	A
19.	[S_Wifi]	Acceso Internet Inalámbrico	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos	1	MB	3	M	R19	1 (3)	B
20.	[App_BDCamp]	BD Campus Virtual	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	MA	1	MB	R20	1 (5)	B
21.	[App_BDCamp]	BD Campus Virtual	Propagación de malware (A10)	Ausencia de activación de alertas tempranas.	5	MA	1	MB	R21	1 (5)	B

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
22.	[App_BDCamp]	BD Campus Virtual	Vulnerabilidad de Software del sistema (A11)	Carencias políticas de actualización de software.	5	MA	2	B	R22	2 (10)	M
23.	[App_BDCamp]	BD Campus Virtual	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	5	MA	3	M	R23	3 (15)	A
24.	[App_WebCamp]	Web Campus Virtual	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	MA	1	MB	R24	1 (5)	B
25.	[App_WebCamp]	Web Campus Virtual	Propagación de malware (A10)	Ausencia de activación de alertas tempranas.	5	MA	1	MB	R25	1 (5)	B
26.	[App_WebCamp]	Web Campus Virtual	Vulnerabilidad de Software del sistema (A11)	Carencias políticas de actualización de software.	5	MA	2	MB	R26	2 (10)	M

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
27.	[App_WebCamp]	Web Campus Virtual	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	5	MA	3	M	R27	3 (15)	A
28.	[App_Seg]	Servidor de seguridad	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	MA	1	MB	R28	1 (5)	B
29.	[App_Seg]	Servidor de seguridad	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	MA	1	MB	R29	1 (5)	B
30.	[App_Seg]	Servidor de seguridad	Vulnerabilidad de Software del sistema (A11)	Carencia de un plan de gestión de cambios.	5	MA	2	MB	R30	2 (10)	M
31.	[App_Seg]	Servidor de seguridad	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	5	MA	3	M	R31	3 (15)	A

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
32.	[App_SrvCom]	Servicio de comunicación de datos	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	MA	1	MB	R32	1 (5)	B
33.	[App_SrvCom]	Servicio de comunicación de datos	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	MA	1	MB	R33	1 (5)	B
34.	[App_SrvCom]	Servicio de comunicación de datos	Vulnerabilidad de Software del sistema (A11)	Carencias políticas de actualización de software.	5	MA	2	MB	R34	2 (10)	M
35.	[App_SrvCom]	Servicio de comunicación de datos	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	5	MA	3	M	R35	3 (15)	A
36.	[App_BDAula]	BD Aula MySQL	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	MA	1	MB	R36	1 (5)	B
37.	[App_BDAula]	BD Aula MySQL	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	MA	1	MB	R37	1 (5)	B

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
38.	[App_BDAula]	BD Aula MySQL	Vulnerabilidad de Software del sistema (A11).	Carencia de un plan de gestión de cambios	5	MA	2	MB	R38	2 (10)	M
39.	[App_BDAula]	BD Aula MySQL	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	5	MA	3	M	R39	3 (15)	A
40.	[App_TelIp]	Servicio de Telefonía Ip	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	MA	1	MB	R40	1 (5)	B
41.	[App_TelIp]	Servicio de Telefonía Ip	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	MA	1	MB	R41	1 (5)	B
42.	[App_TelIp]	Servicio de Telefonía Ip	Vulnerabilidad de Software del sistema (A11)	Carencia de un plan de gestión de cambios	5	MA	2	MB	R42	2 (10)	A

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
43.	[App_TelIp]	Servicio de Telefonía Ip	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	5	MA	3	M	R43	3 (15)	A
44.	[Sop_Camp]	Servidor Campus	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	2	B	R44	2 (10)	M
45.	[Sop_Camp]	Servidor Campus	Condiciones inadecuadas de temperatura y humedad (A14)	Ausencia de sensores de medición de temperatura y humedad regulados	5	MB	2	B	R45	2 (10)	M
46.	[Sop_Camp]	Servidor Campus	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	5	MB	2	B	R46	2 (10)	M
47.	[Sop_FW1]	Servidor Firewall 1	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	2	B	R47	2 (10)	M

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
48.	[Sop_FW1]	Servidor Firewall 1	Condiciones inadecuadas de temperatura y humedad (A14)	Ausencia de sensores de medición de temperatura y humedad regulados	5	MB	2	B	R48	2 (10)	M
49.	[Sop_FW1]	Servidor Firewall 1	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	5	MB	2	B	R49	2 (10)	M
50.	[Sop_FW1]	Servidor Firewall 1	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	4	A	1	MB	R50	1 (4)	B
51.	[Sop_FW1]	Servidor Firewall 1	Análisis de tráfico de información (A17)	Carencia de un plan periódico de retroalimentación por el análisis de tráfico de información	5	MA	2	B	R51	2 (10)	M

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
52.	[Sop_FW1]	Servidor Firewall 1	Negación de servicio (A18)	Carencia de un sistema de información de administración de eventos	5	MA	1	MB	R52	1 (5)	B
53.	[Sop_FW2]	Servidor Firewall 2	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	2	B	R53	2 (10)	M
54.	[Sop_FW2]	Servidor Firewall 2	Condiciones inadecuadas de temperatura y humedad (A14)	Ausencia de sensores de medición de temperatura y humedad regulados	5	MB	2	B	R54	2 (10)	M
55.	[Sop_FW2]	Servidor Firewall 2	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	5	MB	2	B	R55	2 (10)	M
56.	[Sop_FW2]	Servidor Firewall 2	Caída de servicio por agotamiento de recursos (A16)	Carencia del plan de redimensionamiento de recursos de hardware	4	A	1	MB	R56	1 (4)	B

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
57.	[Sop_FW2]	Servidor Firewall 2	Análisis de tráfico de información (A17)	Carencia de un plan periódico de retroalimentación por el análisis de tráfico de información	5	MA	2	B	R57	2 (10)	M
58.	[Sop_FW2]	Servidor Firewall 2	Negación de servicio (A18)	Carencia de un sistema de información de administración de eventos	5	MA	1	MB	R58	1 (5)	B
59.	[Sop_SWCore]	Switch Core	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	1	MB	R59	1 (5)	B
60.	[Sop_SWCore]	Switch Core	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	5	MB	2	B	R60	2 (10)	M
61.	[Sop_SWCore]	Switch Core	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	MA	1	MB	R61	1 (5)	B

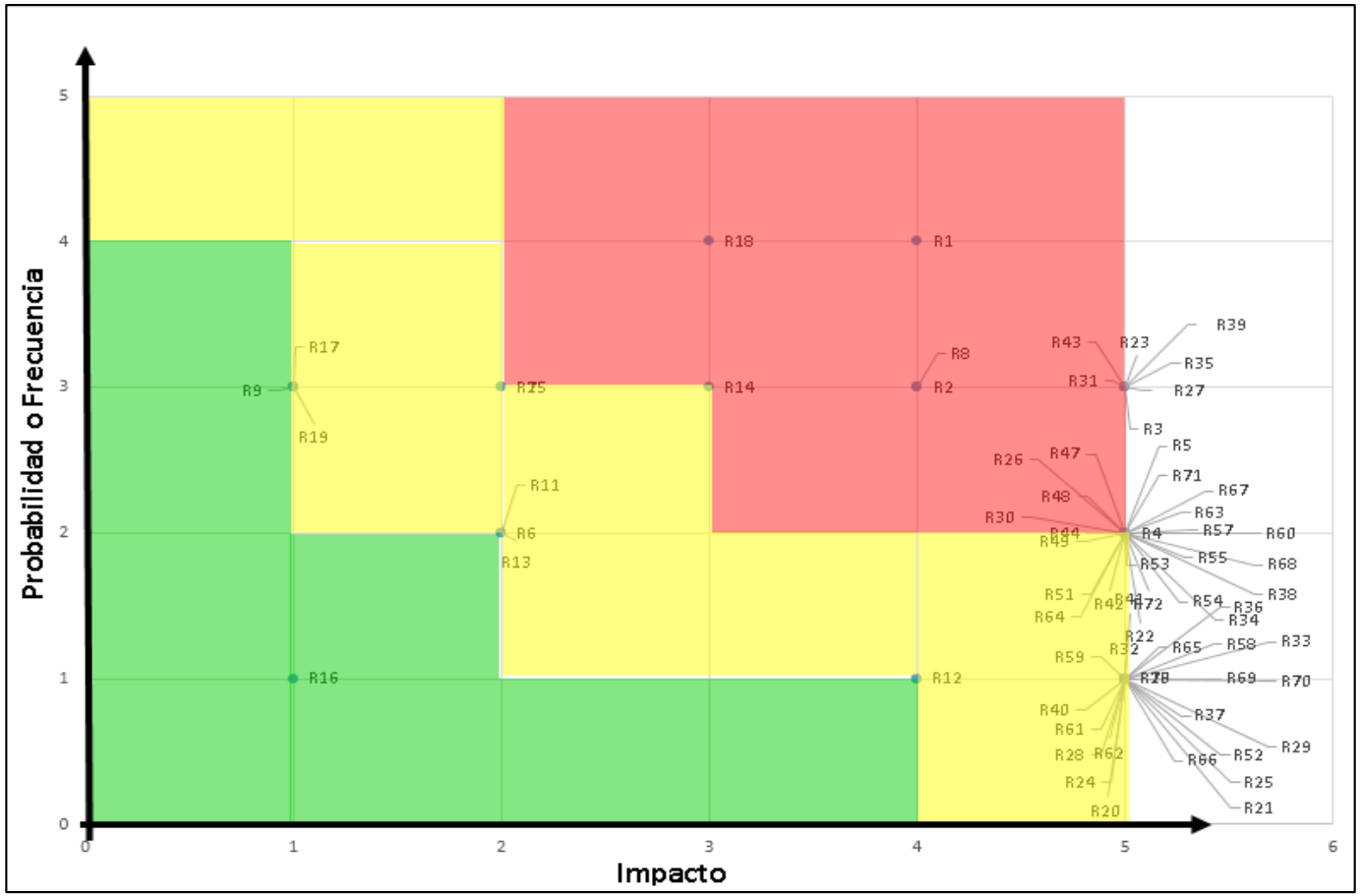
Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
62.	[Sop_Aula]	Servidor Aula Virtual	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	1	MB	R62	1 (5)	B
63.	[Sop_Aula]	Servidor Aula Virtual	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	5	MB	2	B	R63	2 (10)	M
64.	[Sop_Aula]	Servidor Aula Virtual	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	5	MB	2	B	R64	2 (10)	M
65.	[Sop_Aula]	Servidor Aula Virtual	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	MA	1	MB	R65	1 (5)	B
66.	[Sop_Email]	Servidor Correo electrónico	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	1	MB	R66	1 (5)	B

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
67.	[Sop_Email]	Servidor Correo electrónico	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	5	MB	2	B	R67	2 (10)	M
68.	[Sop_Email]	Servidor Correo electrónico	Falla en dispositivos de almacenamiento (A16)	Nivel de redundancia de dispositivos de almacenamiento	5	MB	2	B	R68	2 (10)	M
69.	[Sop_Email]	Servidor Correo electrónico	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	MA	1	MB	R69	1 (5)	B
70.	[Sop_TelIp]	Servidor telefonía IP	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	MA	1	MB	R70	1 (5)	B
71.	[Sop_TelIp]	Servidor telefonía IP	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	5	MB	2	B	R71	2 (10)	M

Nro.	Código activo	Activo	Amenaza	Vulnerabilidad	Impacto		Probabilidad		Riesgo		
					Nivel	Descrip.	Nivel	Categoría	Cód.	Nivel	Categorí
72.	[Sop_TelIp]	Servidor telefonía IP	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	5	MB	2	B	R72	2 (10)	M
73.	[Sop_TelIp]	Servidor telefonía IP	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	MA	1	MB	R73	1 (5)	B

Tabla 27: Tabla priorización del riesgo

Fase IV – Valoración del Riesgo



Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
A	R1	[S_CamVir]	Servicio Campus Virtual	Error de usuario (A1)	Carencia de validación de datos entradas en los sistemas	16	10	15	Intolerable
A	R3	[S_CamVir]	Servicio Campus Virtual	Alteración accidental de información (A3)	Carencia de programas de capacitación al personal	15	10	15	Tolerable
A	R23	[App_BDCamp]	BD Campus Virtual	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	9	16	Tolerable
A	R27	[App_WebCamp]	Web Campus Virtual	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	10	15	Tolerable
A	R31	[App_Seg]	Servidor de seguridad	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	10	15	Tolerable
A	R35	[App_SrvCom]	Servicio de comunicación de datos	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	10	20	Tolerable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
A	R39	[App_BDAula]	BD Aula MySQL	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	9	15	Tolerable
A	R43	[App_TelIp]	Servicio de Telefonía Ip	Errores en mantenimiento y actualización de software (A12)	Carencia de un plan de gestión de cambios / transición.	15	10	20	Tolerable
A	R2	[S_CamVir]	Servicio Campus Virtual	Escape de Información (A2)	Carencia de Políticas de seguridad	12	10	15	Tolerable
A	R8	[S_AulaVir]	Servicio Aula Virtual	Escape de Información (A2)	Carencia de Políticas de seguridad	12	10	15	Tolerable
A	R18	[S_Wifi]	Acceso Internet Inalámbrico	Acceso no Autorizado (A5)	Ausencia de un sistema de aprovisionamiento de usuarios.	12	10	20	Tolerable
M	R4	[S_CamVir]	Servicio Campus Virtual	Abuso de Privilegios(A4)	Carencia de Políticas de uso del sistema	10	10	15	Aceptable
M	R5	[S_CamVir]	Servicio Campus Virtual	Acceso no Autorizado (A5)	Ausencia de un sistema de aprovisionamiento de usuarios.	10	10	15	Aceptable
M	R22	[App_BDCamp]	BD Campus Virtual	Vulnerabilidad de Software del sistema (A11)	Carencias políticas de actualización de software.	10	9	16	Tolerable
M	R26	[App_WebCamp]	Web Campus Virtual	Vulnerabilidad de Software del sistema (A11)	Carencias políticas de actualización de software.	10	10	15	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
M	R30	[App_Seg]	Servidor de seguridad	Vulnerabilidad de Software del sistema (A11)	Carencia de un plan de gestión de cambios.	10	10	15	Aceptable
M	R34	[App_SrvCom]	Servicio de comunicación de datos	Vulnerabilidad de Software del sistema (A11)	Carencias políticas de actualización de software.	10	10	20	Aceptable
M	R38	[App_BDAula]	BD Aula MySQL	Vulnerabilidad de Software del sistema (A11).	Carencia de un plan de gestión de cambios	10	9	15	Tolerable
A	R42	[App_TelIp]	Servicio de Telefonía Ip	Vulnerabilidad de Software del sistema (A11)	Carencia de un plan de gestión de cambios	10	10	20	Aceptable
M	R44	[Sop_Camp]	Servidor Campus	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	10	10	15	Aceptable
M	R45	[Sop_Camp]	Servidor Campus	Condiciones inadecuadas de temperatura y humedad (A14)	Ausencia de sensores de medición de temperatura y humedad regulados	10	10	15	Aceptable
M	R46	[Sop_Camp]	Servidor Campus	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	10	10	15	Aceptable
M	R47	[Sop_FW1]	Servidor Firewall 1	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	10	10	15	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
M	R48	[Sop_FW1]	Servidor Firewall 1	Condiciones inadecuadas de temperatura y humedad (A14)	Ausencia de sensores de medición de temperatura y humedad regulados	10	10	15	Aceptable
M	R49	[Sop_FW1]	Servidor Firewall 1	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	10	10	15	Aceptable
M	R51	[Sop_FW1]	Servidor Firewall 1	Análisis de tráfico de información (A17)	Carencia de un plan periódico de retroalimentación por el análisis de tráfico de información	10	10	15	Aceptable
M	R53	[Sop_FW2]	Servidor Firewall 2	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	10	10	15	Aceptable
M	R54	[Sop_FW2]	Servidor Firewall 2	Condiciones inadecuadas de temperatura y humedad (A14)	Ausencia de sensores de medición de temperatura y humedad regulados	10	10	15	Aceptable
M	R55	[Sop_FW2]	Servidor Firewall 2	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	10	10	15	Aceptable
M	R57	[Sop_FW2]	Servidor Firewall 2	Análisis de tráfico de información (A17)	Carencia de un plan periódico de retroalimentación por el análisis de tráfico de información	10	10	15	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
M	R60	[Sop_SWCore]	Switch Core	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	10	10	15	Aceptable
M	R63	[Sop_Aula]	Servidor Aula Virtual	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	10	10	15	Aceptable
M	R64	[Sop_Aula]	Servidor Aula Virtual	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	10	10	15	Aceptable
M	R67	[Sop_Email]	Servidor Correo electrónico	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	10	10	15	Aceptable
M	R68	[Sop_Email]	Servidor Correo electrónico	Falla en dispositivos de almacenamiento (A16)	Nivel de redundancia de dispositivos de almacenamiento	10	10	15	Aceptable
M	R71	[Sop_TelIp]	Servidor telefonía IP	Condiciones inadecuadas de temperatura y humedad (A14)	Componentes electrónicos susceptibles a daños por calor y humedad	10	10	15	Aceptable
M	R72	[Sop_TelIp]	Servidor telefonía IP	Falla en dispositivos de almacenamiento (A15)	Nivel de redundancia de dispositivos de almacenamiento	10	10	15	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
M	R14	[S_Email]	Servicio correo electrónico	Ingeniería social (A19)	Programas de concientización continua del personal responsable	9	10	15	Aceptable
M	R7	[S_AulaVir]	Servicio Aula Virtual	Error de usuario (A7)	Carencia de conocimiento de uso del aula virtual	6	10	15	Aceptable
M	R15	[S_CenTel]	Central telefónica	Uso no previsto (A8)	Ausencia de políticas de uso del sistema.	6	10	20	Aceptable
M	R10	[S_AulaVir]	Servicio Aula Virtual	Abuso de Privilegio (A4)	Carencia de Políticas de uso del sistema	5	10	15	Aceptable
M	R20	[App_BDCamp]	BD Campus Virtual	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	9	16	Aceptable
M	R21	[App_BDCamp]	BD Campus Virtual	Propagación de malware (A10)	Ausencia de activación de alertas tempranas.	5	9	16	Aceptable
M	R24	[App_WebCamp]	Web Campus Virtual	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	10	15	Aceptable
M	R25	[App_WebCamp]	Web Campus Virtual	Propagación de malware (A10)	Ausencia de activación de alertas tempranas.	5	10	15	Aceptable
M	R28	[App_Seg]	Servidor de seguridad	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	10	15	Aceptable
M	R29	[App_Seg]	Servidor de seguridad	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	10	15	Aceptable
M	R32	[App_SrvCom]	Servicio de comunicación de datos	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	10	20	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
M	R33	[App_SrvCom]	Servicio de comunicación de datos	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	10	20	Aceptable
M	R36	[App_BDAula]	BD Aula MySQL	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	9	15	Aceptable
M	R37	[App_BDAula]	BD Aula MySQL	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	9	15	Aceptable
M	R40	[App_TelIp]	Servicio de Telefonía Ip	Error en configuración (A9)	Carencia de un plan de gestión de cambios.	5	10	20	Aceptable
M	R41	[App_TelIp]	Servicio de Telefonía Ip	Propagación de malware (A10)	Ausencia de activación de alertas tempranas	5	10	20	Aceptable
M	R52	[Sop_FW1]	Servidor Firewall 1	Negación de servicio (A18)	Carencia de un sistema de información de administración de eventos	5	10	15	Aceptable
M	R58	[Sop_FW2]	Servidor Firewall 2	Negación de servicio (A18)	Carencia de un sistema de información de administración de eventos	5	10	15	Aceptable
M	R59	[Sop_SWCore]	Switch Core	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	10	15	Aceptable
M	R61	[Sop_SWCore]	Switch Core	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	10	15	Aceptable
M	R62	[Sop_Aula]	Servidor Aula Virtual	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	10	15	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
M	R65	[Sop_Aula]	Servidor Aula Virtual	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	10	15	Aceptable
M	R66	[Sop_Email]	Servidor Correo electrónico	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	10	15	Aceptable
M	R69	[Sop_Email]	Servidor Correo electrónico	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	10	15	Aceptable
M	R70	[Sop_TelIp]	Servidor telefonía IP	Corte Energía Eléctrica (A13)	Tiempo de autonomía del sistema UPS	5	10	15	Aceptable
M	R73	[Sop_TelIp]	Servidor telefonía IP	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	5	10	15	Aceptable
B	R6	[S_CamVir]	Servicio Campus Virtual	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos.	4	10	15	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
B	R11	[S_AulaVir]	Servicio Aula Virtual	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos.	4	10	15	Aceptable
B	R12	[S_Email]	Servicio correo electrónico	Escape de Información (A2)	Carencia de Políticas de seguridad	4	10	15	Aceptable
B	R13	[S_Email]	Servicio correo electrónico	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos	4	10	15	Aceptable
B	R50	[Sop_FW1]	Servidor Firewall 1	Caída de servicio por agotamiento de recursos (A16)	Carencia de del plan de redimensionamiento de recursos de hardware	4	10	15	Aceptable
B	R56	[Sop_FW2]	Servidor Firewall 2	Caída de servicio por agotamiento de recursos (A16)	Carencia del plan de redimensionamiento de recursos de hardware	4	10	15	Aceptable
B	R9	[S_AulaVir]	Servicio Aula Virtual	Alteración accidental de información (A3)	Carencia de programas de capacitación al personal	3	10	15	Aceptable
B	R17	[S_Wifi]	Acceso Internet Inalámbrico	Uso no previsto (A8)	Ausencia de políticas de uso del sistema.	3	10	20	Aceptable

Clasificación Riesgo	Cód. Riesgo	Código activo	Activo	Amenaza	Vulnerabilidad	Magnitud Riesgo	Apetito	Tolerancia	Valorización
B	R19	[S_Wifi]	Acceso Internet Inalámbrico	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos	3	10	20	Aceptable
B	R16	[S_CenTel]	Central telefónica	Negación de acciones (A6)	Carencia de un sistema de información de administración de eventos	1	10	20	Aceptable

Fase III - Tratamiento de los riesgos y Monitoreo

Nombre del Proyecto: PRY01	
Estrategia	**Implementar los controles de validación de datos de entrada en cada uno de los módulos de gestión según estándares de calidad de desarrollo de software**
Riesgo que se trata:	R1
Categoría de Riesgo:	Alto
Objetivo:	Reducir el índice de errores de usuario en el ingreso de datos en cada uno de los módulos.
Responsable:	Dirección de TI
Recursos requeridos:	Personal de la jefatura de desarrollo de sistemas
Presupuesto:	Número de personas*tiempo*costohora = 02 * 320 * 1 0 = S/. 6400
Procesos de negocios afectado	Gestión de personal / Gestión de pensiones / Gestión de tutoría / Gestión Administrativa / Gestión de contabilidad / Gestión curricular / Gestión Académica.
Tiempo de ejecución	320 horas (40 días hábiles x 8 horas)
Anexos:	--

Monitoreo y revisión	
Verificación:	**Variables a controlar:**
Implementación de políticas de verificación por usuario para determinar el índice de errores por entrada de datos	Ingreso de datos en cada uno de los módulos por usuario.
Indicadores:	

Número de incidencias reportados errores de usuario en el ingreso de datos por cada módulo.
Acciones para mejorar el proyecto
Evaluar los resultados por semestre con respecto a la disminución del índice de errores por usuario en el ingreso de datos.

Nombre del Proyecto: PRY02			
Estrategia	**Implementación de políticas de seguridad basadas en el estándar ISO 27000 para reducir la frecuencia escape de información**		
Riesgo que se trata:	R2	R8	R12
Categoría de Riesgo:	Alto		Bajo
Objetivo:	**Reducir el nivel de escape de información por carencia de políticas de seguridad.**		
Responsable:	Dirección de TI		
Recursos requeridos:	Asistente de Dirección de TI		
Presupuesto:	Número de horas * Costo.hora = 480 * 10 = S/. 4800		
Procesos de negocios afectado	Gestión de personal / Gestión de pensiones / Gestión de tutoría / Gestión Administrativa / Gestión de contabilidad / Gestión curricular / Gestión Académica / Gestión Aula Virtual		
Tiempo de ejecución	480 horas (60 días hábiles * 8 horas)		
Anexos:	--		
Monitoreo y revisión			
Verificación:	**Variables a controlar:**		

Actividades implementadas en base a la ISO27000, para verificar acciones de escape de información. Acciones a ejecutar para obtener datos para el procesamiento de los indicadores.	Frecuencia de escape de información. Identificación de características del objetivo del proyecto para determinar el indicador de medición.
Indicadores:	
Número de incidencias relacionadas a escape de información.	
Acciones para mejorar el proyecto	
Procesos de retroalimentación por los resultados obtenidos en nivel de información protegida.	

Nombre del Proyecto: PRY03		
Estrategia	Implementar programas de capacitación al personal, según segregación de funciones para evitar alteraciones accidentales de información.	
Riesgo que se trata:	R3	R9
Categoría de Riesgo:	Alto	Bajo
Objetivo:	Reducir el nivel de frecuencia de alteraciones accidentales de información provocadas por desconocimiento del usuario.	
Responsable:	Dirección de TI	
Recursos requeridos:	Personal especializado por módulos	
Presupuesto:	Número de capacitadores*frecuencia*tiempo* costo.hora = 2 * 2 * 8 * 60 = S/. 1920	
Procesos de negocios afectado	Gestión de personal / Gestión de pensiones / Gestión de tutoría / Gestión Administrativa / Gestión de	

	contabilidad / Gestión curricular / Gestión Académica / Gestión Aula Virtual
Tiempo de ejecución	16 hrs por año
Anexos:	--

Monitoreo y revisión	
Verificación:	**Variables a controlar:**
Actividades implementadas para la identificación de alteraciones accidentales.	Alteraciones accidentales de información provocadas por desconocimiento del usuario.
Indicadores:	
Número de incidencias relacionadas a alteraciones accidentales de información provocadas por desconocimiento del usuario.	
Acciones para mejorar el proyecto	
Medir el nivel de frecuencia de alteraciones, por período para aplicar medidas correctivas que generen la reducción de la información alterada.	

Nombre del Proyecto: PRY04		
Estrategia	Implementar un sistema de aprovisionamiento de usuarios, según segregación de funciones aplicando el estándar ITIL.	
Riesgo que se trata:	R5	R18
Categoría de Riesgo:	medio	alto
Objetivo:	Reducir el número de accesos no autorizados por ausencia de aprovisionamiento de usuarios.	
Responsable:	Dirección de TI	
Recursos requeridos:	Personal especialista	
Presupuesto:	Número de especialista*Número de horas * Costo.hora = 2 * 480 * 10	

	= S/. 9600
Procesos de negocios afectado	Gestión de personal / Gestión de pensiones / Gestión de tutoría / Gestión Administrativa / Gestión de contabilidad / Gestión curricular / Gestión Académica
Tiempo de ejecución	480 Hrs. (60 días hábiles x 8 horas)
Anexos:	--

Monitoreo y revisión	
Verificación:	**Variables a controlar:**
Implementación de políticas de aprovisionamiento de usuarios, según segregación de funciones.	Sistema de aprovisionamiento de usuarios, según segregación de funciones aplicando el estándar ITIL.
Indicadores:	
Número de incidencias relacionadas a intento de accesos no autorizados por ausencia de aprovisionamiento de usuarios.	
Acciones para mejorar el proyecto	
Evaluar en función de la reducción del número de accesos, las actividades correctivas de aprovisionamiento de usuarios según segregación de funciones basado en el estándar ITIL	

Nombre del Proyecto: PRY05						
Estrategia:	Errores en mantenimiento y actualización de software (A12)/Carencia de un plan de gestión de cambios / transición.					
Riesgo que se trata:	R23	R27	R31	R35	R39	R43
Categoría de Riesgo:	Alto					
Objetivo:	Implementar plan de mantenimiento y actualización de software considerando ITIL para la gestión de Cambio y Transición.					
Responsable:	Jefe de Desarrollo de Sistemas					

Recursos requeridos:	Asesor externo experto en implementación de ITIL
Presupuesto:	S/. 8000
Procesos de negocios afectado	Gestión de Personal, Gestión de Pensiones, Gestión de Tutoría, Gestión Administrativa, Gestión de Contabilidad, Gestión Curricular, Gestión Académica, Gestión Aula Virtual.
Tiempo de ejecución	640 horas (80 días hábiles * 8 horas)
Anexos:	

Monitoreo y revisión	
Verificación:	**Variables a controlar:**
Implementación de políticas de mantenimientos y actualización de software por parte del personal de TI, para determinar el índice de errores.	Actividades de mantenimientos y actualización de software.
Indicadores:	
Número de incidencias relacionados con errores en los procesos de mantenimiento y actualización de software.	
Acciones para mejorar el proyecto	
Evaluar los resultados por trimestre con respecto a la disminución del índice de errores en los procesos de mantenimiento y actualización de software.	

ANEXO 06: Matriz de consistencia de validación de expertos

El objetivo de la presente matriz de consistencia es contrastar la validez del modelo de gestión riesgos de TI aplicadas en universidades privadas de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario a partir de la investigación de las distintas metodologías y estándares de gestión de Riesgos, un modelo simplificado y flexible que promueva su aplicación, en la intención que se desarrolle una cultura organizacional de acción preventiva en la gestión de las tecnologías de información de las universidades. El procedimiento planteado configura plantillas que permiten que la gestión de riesgos de TI, sea viable en distintos contextos de baja, media o alta complejidad determinada por el tamaño de la organización.

Escala: 1:En total desacuerdo, 2: En desacuerdo, 3: Ni de acuerdo ni en desacuerdo, 4: De acuerdo, 5: Totalmente de acuerdo

Por favor marcar con X, según la opción elegida.

Fase I: Establecimiento de Contexto										
			Escala							
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones		
Contextos Internos (pág 9)	Conocer los factores internos que influencian en el comportamiento de la organización	Nivel suficientes de elementos por cada factor (cultural, partes involucradas, estructura, recursos, metas y objetivos)				X		Corregir las observaciones encontradas.		
Contextos Externos (pág 10)	Conocer los factores externos que influencian en el comportamiento de la organización	Nivel suficientes de elementos por cada factor (ambiente del negocio, social y cultural, reglamentos, competitivo, financiero y político)				X		Corregir las observaciones encontradas.		
Fase II: Identificación de Activos										
			Escala							
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones		
Clasificación de activos (pág 11 - 13)	Definir los catálogos de clasificación de activos en una institución universitaria privada	Número de catálogos suficientes según el tipo de institución(proceso de negocio, servicios, aplicaciones y ~~software~~, soporte de TI)					X			
		Número de activos indentificación por catálogo según el tipo de institución				X				

Fase II: Identificación de Activos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Dependencia de activos (pág 14 - 15)	Dar a conocer el nivel de criticidad de los activos de TI según la relación con los procesos de negocio.	Número de relaciones de dependencia entre los activos de soporte de TI y los procesos de negocio analizados.				X		Calzar las dependencias con las tablas.
Valorización de Activos (pág 16 - 21)	Determinar las escalas de valoración de cada activo.	Número de criterios determinados (Confidencialidad, Integridad y Disponibilidad)					X	
		Número de escalas suficientes para calcular nivel de criticidad de activos.					X	
	Dar a conocer el cuadro de valorización de activos según categoría	Nivel simplicidad para realizar la valoración de activos según los criterios (confidencialidad, Integridad y disponibilidad)					X	
Fase III: Análisis de Riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Tablas de niveles de valorización.	Determinar los niveles de valoración para la identificación del riesgo	Número de valores suficientes para valorar el nivel de impacto.					X	
		Número de valores suficientes para valorar el índice de probabilidad o frecuencia de ocurrencia.					X	
		Número de categorías de riesgo suficientes para la valorización.					X	

Fase III: Análisis de Riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Identificación de riesgo	Dar a conocer el cuadro para la identificación de la naturaleza del riesgo	Nivel de practicidad del cuadro de identificación de la naturaleza de riesgo					X	Es practico y simple.
	Determinar los niveles de priorización de riesgos según rango de riesgos por tipos de amenazas.	Nivel simplicidad para realizar la identificación de riesgos según la valoración del impacto y la probabilidad o frecuencia de ocurrencia.					X	Es practico y simple.
Fase IV: Valoración de Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Priorización de riesgo	Determinar el nivel de priorización de riesgos, según la valoración	Nivel simplicidad para calificar el nivel de priorización de riesgos					X	
	Identificación de riesgos según mapa de calor	Nivel de densidad del número de riesgos identificados por nivel de valoración					X	
Valoración de Riesgos	Valorar en respecto a la comparación de los resultados del análisis del riesgo con sus criterios y determinar si se acepta o se tolera	Nivel de practicidad para valorar del riesgo en respecto a su rango de apetito, tolerancia y capacidad.				X		Evaluar si en el modelo es posible incorporar una valoración general que permita al usuario seleccionar que valoración utiliz
Fase V: Tratamiento de los Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Determinación de estrategias para tratamiento de riesgos	Determinar si la adopción de las estrategias de tratamiento son sufiecientes para el rubro de negocio de universidades privadas	Nivel de suficiencia con respecto a las denominación de evitar, mitigar, transferir, aceptar para las estrategias de tratamiento.					X	

Fase V: Tratamiento de los Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Establecimiento de los Proyectos	Formular criterios suficientes para el establecimiento del proyecto de tratamiento.	Número de criterios suficientes para la formulación del proyecto					X	
Fase VI: Monitoreo y revisión de riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
	ejecutar para obtener datos para el procesamiento de los indicadores.	Nivel de simplicidad para identificar acciones para el procesamiento de indicadores					X	
Monitoreo	Identificar las características del objetivo del proyecto para determinar el indicador de medición.	Nivel de simplicidad para identificar las variables a controlar.				X		Detallar las diferencias entre Monitoreo y revision
	Identificar la medida de lo logrado en la aplicación del procesamiento	Nivel de simplicidad para identificar los indicadores.					X	
Revisión	Identificar medidas correctivas para mejorar los resultados obtenidos.	Nivel de simplicidad para identificar las medidas correctivas.						

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	X

MGTR. GONZALO MARTÍN VALDIVIA BENITES
PROFESIONAL EXPERTO

El objetivo de la presente matríz de consistencia es contrastar la validez del modelo de gestión riesgos de TI aplicadas en universidades privadas de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario a partir de la investigación de las distintas metodologías y estándares de gestión de Riesgos, un modelo simplificado y flexible que promueva su aplicación, en la intención que se desarrolle una cultura organizacional de acción preventiva en la gestión de las tecnologías de información de las universidades. El procedmiento planteado configura plantillas que permiten que la gestión de riesgos de TI, sea viable en distintos contextos de baja, media o alta complejidad determinada por el tamaño de la organización.

Escala: **1:En total desacuerdo, 2: En desacuerdo, 3: Ni de acuerdo ni en desacuerdo, 4: De acuerdo, 5: Totalmente de acuerdo**

Por favor marcar con X, según la opción elegida.

Fase I: Establecimiento de Contexto								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Contextos Internos (pág 9)	Conocer los factores internos que influencian en el comportamiento de la organización	Nivel suficientes de elementos por cada factor (cultural, partes involucradas, estructura, recursos, metas y objetivos)				X		Realizar ajustes.
Contextos Externos (pág 10)	Conocer los factores externos que influencian en el comportamiento de la organización	Nivel suficientes de elementos por cada factor (ambiente del negocio, social y cultural, reglamentos, competitivo, financiero y político)				X		Realizar ajustes.
Fase II. Identificación de Activos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Clasificación de activos (pág 11 - 13)	Definir los catálogos de clasificación de activos en una institución universitaria privada	Número de catálogos suficientes según el tipo de institución(proceso de negocio, servicios, aplicaciones y software, soporte de TI)				X		Realizar ajustes.
		Número de activos indentificación por catálogo según el tipo de institución				X		Realizar ajustes a cantidad de procesos. Homogeneizar.

Fase II: Identificación de Activos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Dependencia de activos (pág 14 - 15)	Dar a conocer el nivel de criticidad de los activos de TI según la relación con los procesos de negocio.	Número de relaciones de dependencia entre los activos de soporte de TI y los procesos de negocio analizados.				X		Homogenizar.
Valorización de Activos (pág 16 - 21)	Determinar las escalas de valoración de cada activo.	Número de criterios determinados (Confidencialidad, Integridad y Disponibilidad)					X	
		Número de escalas suficientes para calcular nivel de criticidad de activos.					X	
	Dar a conocer el cuadro de valorización de activos según categoría	Nivel simplicidad para realizar la valoración de activos según los criterios (confidencialidad, Integridad y disponibilidad)					X	
Fase III: Análisis de Riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Tablas de niveles de valorización.	Determinar los niveles de valoración para la identificación del riesgo	Número de valores suficientes para valorar el nivel de impacto.					X	
		Número de valores suficientes para valorar el índice de probabilidad o frecuencia de ocurrencia.				X		Evaluar definición actual de frecuencia de ocurrencia
		Número de categorías de riesgo suficientes para la valorización.						

Fase III: Análisis de Riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Identificación de riesgo	Dar a conocer el cuadro para la identificación de la naturaleza del riesgo	Nivel de practicidad del cuadro de identificación de la naturaleza de riesgo					X	
	Determinar los niveles de priorización de riesgos según rango de riesgos por tipos de amenazas.	Nivel simplicidad para realizar la identificación de riesgos según la valoración del impacto y la probabilidad o frecuencia de ocurrencia.					X	
Fase IV: Valoración de Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Priorización de riesgo	Determinar el nivel de priorización de riesgos, según la valoración	Nivel simplicidad para calificar el nivel de priorización de riesgos					X	
	Identificación de riesgos según mapa de calor	Nivel de densidad del número de riesgos identificados por nivel de valoración					X	
Valoración de Riesgos	Valorar en respecto a la comparación de los resultados del análisis del riesgo con sus criterios y determinar si se acepta o se tolera	Nivel de practicidad para valorar del riesgo en respecto a su rango de apetito, tolerancia y capacidad.				X		Plantear models alternativos.
Fase V: Tratamiento de los Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Determinación de estrategias para tratamiento de riesgos	Determinar si la adopción de las estrategias de tratamiento son sufiecientes para el rubro de negocio de universidades privadas	Nivel de suficiencia con respecto a las denominación de evitar, mitigar, transferir, aceptar para las estrategias de tratamiento.				X		

Fase V: Tratamiento de los Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Establecimiento de los Proyectos	Formular criterios suficientes para el establecimiento del proyecto de tratamiento.	Número de criterios suficientes para la formulación del proyecto				X		
Fase VI: Monitoreo y revisión de riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Monitoreo	ejecutar para obtener datos para el procesamiento de los indicadores.	Nivel de simplicidad para identificar acciones para el procesamiento de indicadores			X			Replantear enfoque de Monitoreo
	Identificar las características del objetivo del proyecto para determinar el indicador de medición.	Nivel de simplicidad para identificar las variables a controlar.				X		
	Identificar la medida de lo logrado en la aplicación del procesamiento	Nivel de simplicidad para identificar los indicadores.			X			Replantear monitoreo.
Revisión	Identificar medidas correctivas para mejorar los resultados obtenidos.	Nivel de simplicidad para identificar las medidas correctivas.			X			Replantear monitoreo

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	✓

MGTR. JUAN DÁVILA RAMÍREZ
PROFESIONAL EXPERTO

El objetivo de la presente matriz de consistencia es contrastar la validez del modelo de gestion riesgos de TI aplicadas en universidades privadas de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario a partir de la investigación de las distintas metodologías y estándares de gestión de Riesgos, un modelo simplificado y flexible que promueva su aplicación, en la intención que se desarrolle una cultura organizacional de acción preventiva en la gestión de las tecnologías de información de las universidades. El procedmiento planteado configura plantillas que permiten que la gestión de riesgos de TI, sea viable en distintos contextos de baja, media o alta complejidad determinada por el tamaño de la organización.

Escala: **1:En total desacuerdo, 2: En desacuerdo, 3: Ni de acuerdo ni en desacuerdo, 4: De acuerdo, 5: Totalmente de acuerdo**

Por favor marcar con X, según la opción elegida.

Fase I: Establecimiento de Contexto								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Contextos Internos (pág 9)	Conocer los factores internos que influencian en el comportamiento de la organización	Nivel suficientes de elementos por cada factor (cultural, partes involucradas, estructura, recursos, metas y objetivos)					X	
Contextos Externos (pág 10)	Conocer los factores externos que influencian en el comportamiento de la organización	Nivel suficientes de elementos por cada factor (ambiente del negocio, social y cultural, reglamentos, competitivo, financiero y político)					X	
Fase II: Identificación de Activos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Clasificación de activos (pág 11 - 13)	Definir los catálogos de clasificación de activos en una institución universitaria privada	Número de catálogos suficientes según el tipo de institución(proceso de negocio, servicios, aplicaciones y software, soporte de TI)					X	
		Número de activos indentificación por catálogo según el tipo de institución						

Fase II: Identificación de Activos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Dependencia de activos (pág 14 - 15)	Dar a conocer el nivel de criticidad de los activos de TI según la relación con los procesos de negocio.	Número de relaciones de dependencia entre los activos de soporte de TI y los procesos de negocio analizados.					X	
Valorización de Activos (pág 16 - 21)	Determinar las escalas de valoración de cada activo.	Número de criterios determinados (Confidencialidad, Integridad y Disponibilidad)					X	
		Número de escalas suficientes para calcular nivel de criticidad de activos.					X	
	Dar a conocer el cuadro de valorización de activos según categoría	Nivel simplicidad para realizar la valoración de activos según los criterios (confidencialidad, Integridad y disponibilidad)					X	
Fase III: Análisis de Riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Tablas de niveles de valorización.	Determinar los niveles de valoración para la identificación del riesgo	Número de valores suficientes para valorar el nivel de impacto.					X	
		Número de valores suficientes para valorar el índice de probabilidad o frecuencia de ocurrencia.					X	
		Número de categorías de riesgo suficientes para la valorización.					X	

Fase III: Análisis de Riesgo								
		Escala						
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Identificación de riesgo	Dar a conocer el cuadro para la identificación de la naturaleza del riesgo	Nivel de practicidad del cuadro de identificación de la naturaleza de riesgo					X	
	Determinar los niveles de priorización de riesgos según rango de riesgos por tipos de amenazas.	Nivel simplicidad para realizar la identificación de riesgos según la valoración del impacto y la probabilidad o frecuencia de ocurrencia.					X	
Fase IV: Valoración de Riesgos								
		Escala						
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Priorización de riesgo	Determinar el nivel de priorización de riesgos, según la valoración	Nivel simplicidad para calificar el nivel de priorización de riesgos					X	
	Identificación de riesgos según mapa de calor	Nivel de densidad del número de riesgos identificados por nivel de valoración					X	
Valoración de Riesgos	Valorar en respecto a la comparación de los resultados del análisis del riesgo con sus criterios y determinar si se acepta o se tolera	Nivel de practicidad para valorar del riesgo en respecto a su rango de apetito, tolerancia y capacidad.					X	
Fase V: Tratamiento de los Riesgos								
		Escala						
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Determinación de estrategias para tratamiento de riesgos	Determinar si la adopción de las estrategias de tratamiento son sufiecientes para el rubro de negocio de universidades privadas	Nivel de suficiencia con respecto a las denominación de evitar, mitigar, transferir, aceptar para las estrategias de tratamiento.					X	

Fase V: Tratamiento de los Riesgos								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Establecimiento de los Proyectos	Formular criterios suficientes para el establecimiento del proyecto de tratamiento.	Número de criterios suficientes para la formulación del proyecto					X	
Fase VI: Monitoreo y revisión de riesgo								
			Escala					
Subfase	Objetivo	Descripción del Indicador	1	2	3	4	5	Observaciones
Monitoreo	ejecutar para obtener datos para el procesamiento de los indicadores.	Nivel de simplicidad para identificar acciones para el procesamiento de indicadores					X	
	Identificar las características del objetivo del proyecto para determinar el indicador de medición.	Nivel de simplicidad para identificar las variables a controlar.					X	
	Identificar la medida de lo logrado en la aplicación del procesamiento	Nivel de simplicidad para identificar los indicadores.					X	
Revisión	Identificar medidas correctivas para mejorar los resultados obtenidos.	Nivel de simplicidad para identificar las medidas correctivas.					X	

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	X

MGTR. JESSIE BRAVO JAICO
PROFESIONAL EXPERTO