UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

Modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos

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

AUTOR

Jefferson James Milian Saavedra

ASESOR

Maria Ysabel Aranguri Garcia

https://orcid.org/0000-0001-9220-5801

Chiclayo, 2024

Modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos

PRESENTADA POR

Jefferson James Milian Saavedra

A la Escuela de Posgrado de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR

Gregorio Manuel Leon Tenorio
PRESIDENTE

Ricardo David Iman Espinoza
SECRETARIO

Maria Ysabel Aranguri Garcia
VOCAL

DEDICAROTIA

Dedico el desarrollo de esta tesis, primeramente, a Dios quien es el que permite que todas las cosas sucedan, el que me guio y me dio la sabiduría para poder terminar esta investigación

A mis padres Genaro Milián Flores y Carmen Saavedra Santa Cruz quienes con su ejemplo, valores y virtudes me fueron formando y que siempre creyeron en mí y me brindaron su apoyo para lograr mis objetivos propuestos.

También a mis hermanos porque de alguna manera estuvieron conmigo brindándome su apoyo para continuar a pesar de cualquier circunstancia

19%	19%	3%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	7%
2	tesis.usat.edu.pe Fuente de Internet	2%
3	repositorio.ucv.edu.pe Fuente de Internet	2%
4	vsip.info Fuente de Internet	1%
5	manglar.uninorte.edu.co Fuente de Internet	1%
6	vlex.com.pe Fuente de Internet	1%
7	www.minedu.gob.pe Fuente de Internet	1%

Índice

Resumen

Esta investigación tiene como caso de estudio a los institutos de educación superior tecnológicos públicos, la cual propone un modelo de gestión de riesgos de TI para garantizar la continuidad del servicio en sus principales procesos, en donde se analizó a 3 institutos públicos para poder determinar el estado actual de los procesos de dichos institutos, obteniendo como resultados que las áreas de TI no tienen identificado los riesgos a los que están expuestas las instituciones y no cuentan con un plan estratégico de TI, lo que genera que dentro de los institutos no exista una mejora en sus procesos organizacionales.

El modelo se basa en la armonización de estándares o marcos de trabajo que tienen referencia a la gestión de riesgos, los cuales se analizaron de forma general para determinar la afectación en la gestión de riesgos de TI para garantizar la continuidad del servicio en los procesos organizacionales, de los cuales se seleccionaron solo 3 de una lista de 6. El modelo fue validado por juicio de expertos, los cuales se basaron en los indicadores de suficiencia, claridad, coherencia y relevancia para dar la valides y aceptación del modelo propuesto.

Finalmente, el modelo fue aplicado en un instituto el cual permitió mejorar la gestión de riesgos de TI y garantizar la continuidad del servicio de sus procesos organizacionales, a través del cumplimiento de los requisitos de la CBC de licenciamientos.

Palabras clave: Institutos de educación superior, CBC de Licenciamientos, gestión de riesgos, marcos o estándares de trabajo.

Abstract

This research has public technological higher education institutes as a case study, which proposes an IT risk management model to guarantee the continuity of the service in its main processes, where 3 public institutes were analyzed to determine the current state of the processes of those institutes, obtaining as results that the IT areas have not identified the risks to which the institutions are exposed and they do not have a strategic IT plan, which generates that within the institutes there is no improvement in their organizational processes.

The model is based on the harmonization of standards or frameworks that refer to risk management, which were analyzed in a general way to determine the impact on IT risk management to guarantee the service continuity in the organizational processes, of which only 3 were selected from a list of 6. The model was validated through expert judgment, which was based on the indicators of sufficiency, clarity, coherence and relevance to give the validity and acceptance of the proposed model.

Finally, the model was applied in an institute which allowed it to improve IT risk management and guarantee the continuity of the service of its organizational processes, through compliance with the CBC licensing requirements.

Keywords: Higher education institutes, CBC Licensing, risk management, frameworks or work standards.

Introducción

En la actualidad la tecnología[1] está abarcando más del 94% de las áreas existentes de una entidad u organismo; según la investigación[2] la tecnología es la herramienta que se encarga de facilitar los procesos, a su vez dicha tecnología presenta riesgos potenciales de impacto muy alto, entre ellos se encuentra el riesgo informático en la forma de sustracción de información, cuentas importantes vulneradas, pérdida de archivos y de control de los sistemas, entre otros. Sin embargo, los mencionados anteriormente no son los únicos riesgos que el área de TI y la administración empresarial pueden enfrentar.

También en la investigación [3] nos menciona que el empleo de tecnología es común para la selección de estrategias dentro de las organizaciones, generando el incremento del uso y dependencia de información electrónica. Lo que permite que la tecnología se convierta en una parte fundamental para la operación de las entidades. Permitiendo a las organizaciones implantar modernas tácticas, procesos e instrumentos para optimizar los aspectos importantes como lo son la planeación, administración, operación, etc.

El sector educativo está expuesto a una constante transformación, lo que lleva a buscar herramientas existentes para poder soportar los diferentes tipos de necesidades y poder alcanzar un óptimo nivel en el mundo tecnológico.

Actualmente, según la investigación [4] mantener segura la información es un tema que aqueja mucho en las instituciones de educación, puesto que se realizó estudios que demuestras las falencias en las organizaciones en Colombia

Debido al avance de la tecnología, se presenta una serie de cambios a nivel operacional. Motivo que lleva a las organizaciones a optar mejoras en sus sistemas de gestión para cumplir sus normativas que rigen actualmente.

La información segura [3] dentro de las instituciones de educación superior, están pasando por muchos tipos de seguridad informática tanto físico como lógica. la que se ha visto expuesta a los diferentes tipos de amenazas por carecer de herramientas y metodologías que ayuden a reducir dichas vulnerabilidades.

En el ámbito nacional según el estudio[5] la tecnología de información y comunicación (TIC) viene siendo una de las herramientas fundamentales dentro de la educación superior

tecnológico y también en la parte funcional de las organizaciones. Por tanto, las organizaciones educativas requieren nuevos modelos para gestionar su información teniendo una gran eficiencia, eficacia, confidencialidad, integridad, disponibilidad y confiabilidad, asegurándose de hacer cumplir las normas internas y externas de las entidades educativas. concluyendo que las TIC son herramientas fundamentales para el desarrollo de sus procesos.

En el trabajo de investigación [6] menciona que actualmente los múltiples riesgos posibles de equipos y sistemas no presentan un plan de respaldo. También menciona que todo el territorio peruano no está indiferente a soportar inseguridades de TI que perturban concisamente a la garantía de datos de las entidades del estado y particulares. También menciona sobre medidas técnicas que sirven para distinguir amenazas, estimarlas, cuantificarlas y poder definir niveles que permitan combatir la influencia negativa en las organizaciones, lo que concluye que gracias a la aplicación de metodologías de riesgo las organizaciones pueden contar con criterios para poder controlar sus recursos y contener inseguridades.

Es sabido que actualmente las entidades de formación superior están implementando TI en la gestión del desarrollo de sus actividades de forma empírica, para la ejecución de todas sus actividades, pero no cuenta con modelo de gestión de riesgos de tecnología de información, que permita dar respuesta inmediata ante algún suceso que pueda afectar a las entidades, como pérdida de información, afectación de activos, etc. Por ende, todo proceso que utiliza TI es totalmente vulnerables frente a las ocurrencias perjudiciales en la institución.

Teniendo en cuenta la investigación [7] donde menciona que los riesgos y amenazas pueden afectar a cualquier recurso de la organización, generando así pérdidas tanto de nivel económico como de nivel de servicios

Con la situación problemática descrita anteriormente, se plantea la siguiente interrogante: ¿De qué manera la implementación de un modelo de gestión de riesgos de tecnología de información influye para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos?, para dar una respuesta a la problemática se plantea la siguiente hipótesis “Si se desarrolla el modelo de gestión de riesgos de tecnología de información, entonces garantizará la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos

públicos". Con la finalidad de alcanzar el propósito se establece como objetivo general implementar un modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos, teniendo como objetivos específicos: armonizar los marcos de trabajo de la gestión de riesgos de TI, con base en los criterios para adaptarlos al contexto de los institutos de educación superior tecnológicos públicos, analizar los procesos organizacionales para evaluar los servicios que permitan formular los componentes del modelo de gestión de riesgos de TI, proponer el modelo de gestión de riesgos con el propósito de contribuir con la continuidad del servicio en los procesos organizacionales, validar el modelo propuesto a través de juicio de expertos con la finalidad de garantizar su aplicación y contribución en el IESTP-Chongoyape e implementar el modelo de gestión de riesgos de TI para garantizar la continuidad del servicio en los procesos organizacionales en el IESTP-Chongoyape.

La implementación del modelo, permite dar un uso adecuado a la infraestructura y servicios de TI. Además, no solo ayudara al área de TI, si no a todas las demás áreas, debido a que agilizaría los procesos, evaluaría las diferentes amenazas y mantendría la información segura y disponible ante cualquier ocurrencia que se pueda generar.

I. Revisión de literatura

1.1. Antecedentes

1.1.1. Antecedentes internacionales

En [8], se desarrolló la mejora del servicio de la gestión interna de calidad sujeto a la Norma ISO 9001:2015, enfocándose en optimizar y mejorar de manera permanente los procesos de funciones sustantivas en la educación superior, tanto en la enseñanza como en el presente estudio. Se elaboró el modelo de gestión de calidad, proponiendo los elementos guía, luego se procedió con el trazado de los procesos principales y se culminó con un plan de implementación. El trabajo está relacionado con la investigación, por que propone un modelo de gestión de calidad, aplicada a institutos de educación superior tecnológicos, teniendo como finalidad optimizar el desempeño interno de trabajo, en donde muestra unos objetivos de manera precisa y una estructura de trabajo enfocada en la norma antes mencionada, la que sirvió de guía para poder elaborar dicho modelo.

En [9], se desarrolló un modelo competente para administrar y tramitar los riesgos de TI en las universidades de carácter público, que permitió establecer tareas para evaluar, identificar, reducir, pronosticar, así como predecir riesgos y amenazas que afecten directa o indirectamente, con sucesos que establezcan escenarios de feedback o forward, dado que son los Institutos los que tienen el compromiso de estar capacitados activamente para afrontar las amenazas que perturben el resultado final de los procesos de la entidad. El trabajo en mención guarda una relación con la presente investigación, debido a que plantea la implementación de un modelo de gobierno y gestión de riesgos de TI, que ayudará a tomar medidas frente a las amenazas de seguridad en los diferentes procesos organizacionales de las universidades públicas de Colombia.

Revisando en [10], se representa un modelo de gobierno y gestión de arquitectura empresarial, para instituciones públicas del nivel técnico profesional, el cual estaba enfocado en fortalecer procesos, a través de sus alineaciones con TI, teniendo como principal objetivo que dicho modelo soporte las operaciones y actividades que se desarrollan en cada una de sus dependencias, apoyándose en estándares y marcos de referencia, desarrollando un modelo de gobierno y gestión de arquitectura empresarial,

jugando un papel principal y definitivo en dichos procesos, el cual consiste en cumplir en todo momento con los procesos del negocio. Este trabajo se relaciona con la investigación en curso, ya que requiere fortalecer procesos, a través de la aplicación de un modelo de gobierno y gestión teniendo como alineación las tecnologías de la información y la comunicación, buscando dar soporte a los procedimientos y actividades llevados a cabo en cada una de sus dependencias, apoyándose en estándares y marcos de referencia que lo hagan posible.

1.1.2. Antecedentes regionales

Tomando a [6], quien realizó un trabajo que tiene como finalidad determinar la incidencia del modelo de gestión de riesgos de TI en la seguridad de la información de una institución del estado, Lima, 2022. El caso de estudio es de tipo básica, nivel descriptivo, con un enfoque cuantitativo, con un diseño no experimental, transversal y de corte correlacional causal, teniendo como población y muestra a 80 trabajadores de una institución del estado, como técnica utilizó la encuesta y como instrumento de recopilación de datos el cuestionario. Este trabajo se relaciona con la investigación en curso, ya que pretende establecer la incidencia del modelo de gestión de riesgos de TI en la seguridad de la información de una institución del estado, basándose en la utilización de técnicas y métodos científicos para recopilar datos, analizarlos y demostrar su validez y confiabilidad a través software SPSS. Con la finalidad de aplicar un método que gestione las causas de TI basada en la norma ISO/IEC 27005:2018 para salvaguardar la información de una entidad del Estado.

En [11], se realizó un trabajo en donde su principal objetivo fue desarrollar un modelo de gestión de servicios de TI, que permitió mejorar las estrategias de fidelización de los estudiantes en los Institutos de Educación Superior Pedagógicos de la Región Cajamarca. Para lo cual, se propuso el desarrollo de un modelo sobre la gestión de los servicios de TI, iniciando previamente en el análisis y comparación de varios marcos de trabajo de TI y metodologías de marketing educativo. Dicho modelo contiene las fases, procesos y actividades, teniendo como referencia a los marcos COBIT5, ITILv3 y

metodologías de marketing educativo apoyada en Customer Relatioship Management. La investigación presentada es cuantitativa, el diseño es no experimental, el tipo de investigación es Aplicada. Este trabajo se relaciona con la investigación en curso, por el desarrollo de un modelo de gestión de servicio de TI en donde se planteó como punto principal mejorar la gestión de servicios de TI para mejor las estrategias de fidelización de estudiantes en los Institutos de Educación Superior Pedagógicos, cuya finalidad es mejorar su servicio de atención y gestionar la fidelización de los estudiantes.

1.1.3. Antecedentes locales

En tanto [12], presenta un trabajo que se orienta en la obligación de incorporar un modelo de gestión apoyado en el tiempo de vida del uso de tecnologías de información (TI) en las instituciones educativas particulares (IEP) de la región Lambayeque. Para ello, se ejecutó un estudio de ideas y técnicas reconocidas, las que están vinculadas con la gestión de servicios, los cuales se adaptaron en el ámbito de IEP de tal forma que proporciona medios precisos para el avance de sus procesos. Dentro de la investigación se diseña un modelo basado en un planeamiento que impacte de manera objetiva en la forma de cómo se componen las TI en las tareas de los usuarios por medio del suministro de servicios. La investigación determinó que gracias a la ejecución de ITIL, pudo orientar a la entidad a la producción de una cartera de servicios. Este trabajo tiene relación con la presente investigación, porque plantea el establecimiento de un modelo fundado en un periodo de vida de servicio de TI con la finalidad de optimizar los procesos dentro de las IEP de la región Lambayeque, planteando la producción del mismo fundado en metodologías y estándares adaptados como la metodología antes mencionada, que tengan particularidades que optimicen los servicios de TI en el contexto de IEP.

Tomando[13], realizó un trabajo que tiene como finalidad apoyar en el resguardo de datos monetarios de las módulos de gestión educativa en la región Lambayeque, ya que dichos establecimientos no cuentan con un modelo para sus activos de datos monetarios. Se analizó como están en el presente estos elementos, se comprobó que demandan

implantar controles que colaboren a salvaguardar dichos datos, para poder así reducir los efectos de los peligros a las que están expuestos. Este trabajo tiene relación con la presente investigación, ya que tiene como finalidad apoyar en el progreso del resguardo de los datos monetarios, en donde se plantea un modelo, apoyándose en el análisis de ámbitos de trabajo y esquemas internacionales congruentes con este estudio, para poder adecuarlo al contexto de la unidad de gestión educativa local.

Según [7], realizó un trabajo teniendo como principal propósito establecer en las entidades educativas un modelo que les posibilite mermar las diferentes amenazas de los métodos que son sobrellevados por el área de TI, en donde se efectuó un estudio a 5 entidades de formación básica regular para poder descubrir el contexto actual, llegando a la conclusión que los sectores de TI no poseen un registro de los distintos servicios que proporciona a las entidades, tampoco de los bienes que dan apoyo a los mismos, creando un crecimiento de sucesos a posibles inseguridades que causen las paralizaciones en los procesos prestados, deteniendo distintas diligencias dentro de la entidad. En dicha investigación se efectuó una mezcla de esquemas, técnicas o modelo de trabajo que formen afectación en la gestión de riesgo, las que se emplearon como fundamento para la creación del modelo cuyo propósito es disminuir inseguridades que alcancen influenciar a las funciones que brindan soporte a los procesos de las entidades de formación. Este trabajo tiene relación con la presente investigación en curso, ya que la investigación evaluó los diferentes retos que los sectores de TI pueden enfrentan en las entidades de formación básica regular, lo que lleva a tornarse en un socio de valor para la entidad, los cuales necesitan estar incluidos con la entidad. Para así poder afrontar cualquier tipo de riesgos con la finalidad de detenerlos o mitigarlos.

En [14], donde realizó un trabajo teniendo como primordial estudio a la gestión de bienes de tecnología de información en entidades privadas de formación básica regular de Lambayeque. A través del resultado de un prototipo de 4 entidades se determinó que no cuenta con una estrategia de trabajo ni registro importante con relación a métodos o procesos que se ofrezca a beneficiarios tanto internos como externos; dando respuesta ante algún solicitud o suceso de manera incorrecta al no poseer un sustento de

información con la cual orientarse, aumentando la posibilidad de pérdidas económicas. La investigación tiene como prioridad optimizar la categoría de actividades de atención del sector de TI en las entidades educativas, creando una proposición de modelo de gestión de servicios de TI referido en esquemas, pautas de trabajo y métodos adaptados, que provean información específica para el soporte en el transcurso de la investigación. Este trabajo tiene relación con la presente investigación en curso, ya que respalda a la formación de métodos apropiados para disponer un modelo que aprueba tener un control apropiado de los sistemas; implantando un sustento de información la cual admitirá evaluar el nivel de la función que se ofrece y así establecer las estrategias de excelencia de servicio y el continuo avance del mismo, constituyendo efecto en los factores internos y externos.

En [15] presenta un trabajo que se orienta a la gestión de servicios de TI para dar soporte a continuidad del servicio en instituciones educativas públicas, el cual está enfocado en dar solución a las brechas digitales que afecten la continuidad del servicio educativo en especial en la gestión de servicios de TI. Este trabajo se relaciona con la presente investigación ya que tiene como finalidad la continuidad del servicio de las instituciones a través de gestión de riesgos de TI, aplicando estándares y marcos de trabajo para su elaboración.

1.2. Bases Teóricas conceptuales

1.2.1. Sistema de educación superior

1.2.1.1. Educación de nivel superior

Según MINEDU[16] “La Educación Superior está predestinada a la indagación, fundación y propagación de sapiencias; para la sociedad; al lograr desarrollar capacidades competitivas de gran nivel, de la mano con la demanda y la insuficiencia del avance razonable del país

Existen 2 tipos:”

- **Publicas:** Encargo inmediato por jurisdicciones del lado de educación o de distintos partes de entidades del Estado

- **Privadas:** Son entidades legales de derecho privativo, fundadas por decisión de personas naturales o jurídicas, acreditadas por parte de la comunidad educativa. El régimen en coherencia con la independencia de enseñanza y el impulso de la diversidad del mercado educativo, distingue, considera y controla la enseñanza privada.

1.2.1.2. Clasificación de institutos de nivel superior

Se tienen las siguientes clasificaciones según MINEDU [16]

- **Institutos de Educación Superior: "**Los institutos de Educación Superior (IES) son instituciones educativas de la segunda etapa del sistema educativo nacional, con énfasis en una formación aplicada.

  Los IES brindan formación de carácter técnico, debidamente fundamentada en la naturaleza de un saber que garantiza la integración del conocimiento teórico e instrumental a fi n de lograr las competencias requeridas por los sectores productivos para la inserción laboral. Brindan, además, estudios de especialización, de perfeccionamiento profesional en áreas específicas y otros programas de formación continua, y otorgan los respectivos certificados.
  La gestión de los IES públicos está a cargo del Organismo de Gestión de Institutos y Escuelas de Educación Superior Tecnológica Públicos (Educatec)".

- **Escuelas de Educación Superior: "**Las escuelas de educación superior (EES) son instituciones educativas que brindan formación altamente especializada. Se clasifican de la siguiente forma: escuelas de educación superior pedagógica (EESP) y escuelas de educación superior tecnológica (EEST)."

1.2.1.3. Norma y ley de gobierno de educación superior

Se tiene las siguiente norma y ley de gobierno:

- **Condiciones básicas de calidad (CBC) para el procedimiento de licenciamientos de los institutos de educación superior y las escuelas de educación superior tecnológica.**

  Son los mínimos estándares[17] para poder brindar el servicio de educación. Siendo el cumplimento de carácter obligatorio, para la obtención de la licencia de funcionamiento de los institutos de educación superior tecnológicos públicos.

- **Ley de Gobierno Digital**

  Conjunto de normas y principios[18] utilizados por las entidades públicas, para la digitalización de sus procesos organizacionales y prestación de servicios digitales, mejorando la prestación y acceso a los servicios en condiciones interoperables.

1.2.1.4.Procesos de Régimen Académico

Entre los procesos de los IES[19] se encuentran los siguientes:

- **Admisión:** Procedimiento que realizan los estudiantes para poder alcanzar una vacante de un determinado programa de estudios que ofrecen los IES y EEST. Dicha actividad es tarea directa de cada entidad.

- **Matrícula:** Procedimiento que debe de realizar una persona para poder pertenecer a un programa de estudios en un IES o EEST, al realizar dicho proceso la persona recibe la categoría de estudiante.

- **Convalidaciones:** Medio que permite a los IES o EEST admitir los conocimientos obtenidos por una persona en el entorno pedagógico.

- **Traslados:** Trámite que los estudiantes matriculados en un determinado programa de estudios pueden realizar siempre y cuando existan plazas disponibles. A otro programa en la misma entidad o en otra entidad**.**

1.2.2. Gestión de riesgos de TI

1.2.2.1.Gestión

La definición de gestión[20] lleva ligada la noción de acción para que los propósitos establecidos se realicen. los componentes principales para proceder algo se sintetizan en él.

1.2.2.2.Riesgo

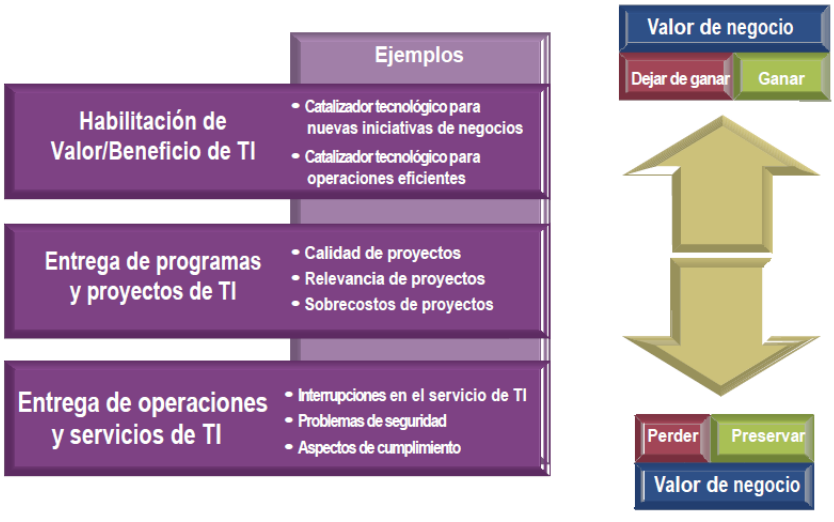
Es la probabilidad de que ocurra algún acontecimiento con factores negativos. Según la ISO 27000.es. El riesgo a menudo se determina por la dependencia a posibles "eventos" y "consecuencias" o una asociación entre ambos.[21]

Para COBIT 5[22], Riesgo habitualmente se especifica como la asociación de la posibilidad entre un suceso y sus efectos. Los efectos causan que los objetivos de las entidades no sean logrados.

1.2.2.3.Riesgo de TI

Los riesgos de TI son fallas o incidentes probables, que afectan a las diferentes organizaciones y en diferentes niveles, COBIT 5[23] “menciona el riesgo de TI como una inseguridad dentro de la industria, individualmente, el riesgo de negocio asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en una empresa. El riesgo de TI consiste de eventos relacionados a TI que potencialmente podrían impactar al negocio. El riesgo de TI puede darse con una frecuencia e impacto inciertos, generando desafíos en el logro de las metas y los objetivos estratégicos.”

Figura 1: Categoría en riesgos [23]



1.2.2.4.Gestión de riesgo de TI

Es el proceso de detectar las posibles amenazas que puede pasar el área de TI de alguna determinada organización, donde se evalúa el nivel de impacto que una organización puede resistir.

Según la ISO 31000, define la gestión de riesgos como “actividades coordinadas para dirigir y controlar la organización con relación al riesgo”.

1.2.2.5.Administración de riesgos de TI

La administración de los riesgos[24] facilita a las entidades la toma de decisiones y suministra la información adecuada para el establecimiento de itinerarios de acción y para favorecer actividades de realimentación y enseñanza basado en casos. Así mismo, el proceso de administración de riesgos permitirá asegurar que los controles aplicados para mitigar los riesgos sean asertivos y que se correspondan con el plan estratégico organizacional.

Figura 2: Valor Agregado de la administración de riesgos[24]

1.2.2.6.Metodologías de gestión de riesgos

Se mencionarán las distintas metodologías que permitirán identificar y reducir los diferentes riesgos que hoy en día el área de TI enfrenta en las diferentes organizaciones.

Con la finalidad de enfocarlos hacia los institutos de educación superior tecnológicos públicos

1.2.2.6.1. COBIT FOR RISK

COBIT en este ejemplar de riesgos toma como punto principal a la información de cualquier organización, menciona que la información es fundamental desde el momento en que se produce hasta el momento en que se desaparece, además la tecnología hoy en día en fundamental y está siempre presente en las empresas de cualquier entorno común, público y corporativo.

COBIT 5[23] contiene un marco completo que ayuda a las entidades a lograr sus metas para la administración y la gestión de la tecnología de información (TI). En resumen, COBIT 5 favorece a las entidades a generar valor ideal a partir de las TI a través del sostenimiento de una proporción entre la obtención de beneficios y la optimización de los niveles de riesgo y del uso de recursos. Facilita la administración y trabajo de TI en forma completa para toda la entidad, teniendo en recuento el negocio extremo a extremo y las áreas funcionales de la responsabilidad TI y teniendo en cuenta los beneficios involucrados con las TI de los segmentos interesados tanto internas como externas.

1.2.2.6.2. AS/NZ 4360:204

Norma que suministra una orientación genérica para la gestión del riesgo. Que se puede emplear a una escala extensa de tareas, fallos u procedimientos de alguna entidad estatal, particular o corporativa, en todos los periodos de la duración de una acción, cargo, proyecto o producto. El gran rendimiento suele obtenerse empleando el proceso de gestión de riesgos desde el principio.

AS/NZ 4360:204[25] tiene como objetivo brindar orientación para permitir que empresas, grupos e individuos públicos, privados o comunitarios logren un sustento seguro y estricto para la toma de medidas y de organización; un buen reconocimiento de posibilidades y riesgos; y adquirir valor a partir de la inseguridad y la inestabilidad.

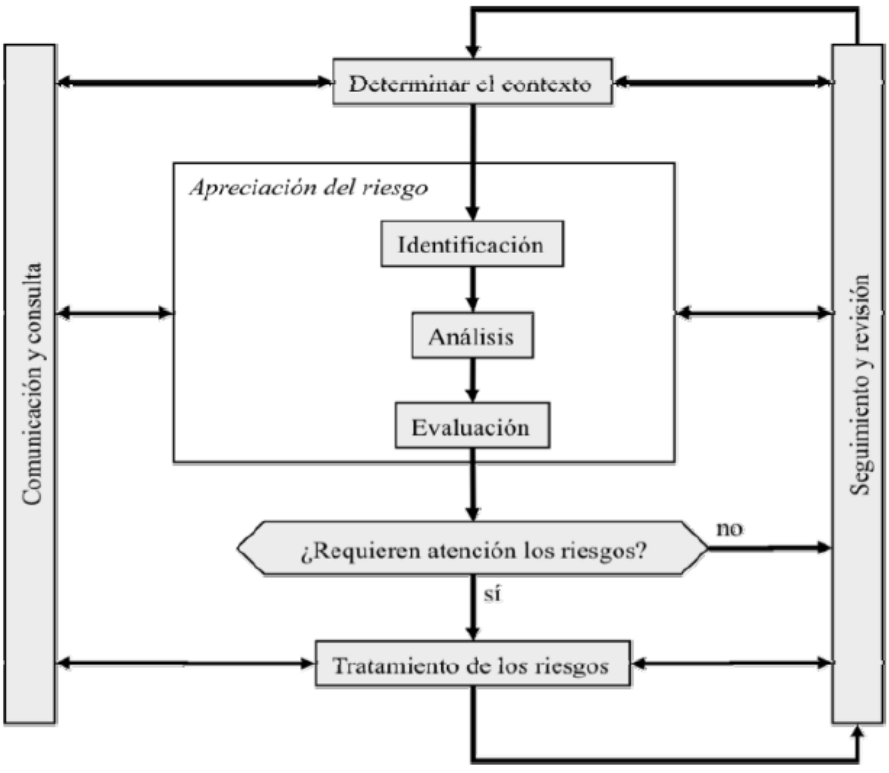
1.2.2.6.3. MAGERIT

La metodología tiene como objetivo directo que: el personal responsable de las áreas de TI conozca la existencia de los riesgos y saber cómo mitigarlos. Por lo que efectúa el proceso de administración de riesgos dentro de un marco de trabajo para que los miembros de gobierno tomen disposiciones teniendo en cuenta los riesgos derivados del uso de TI.

Se deben de realizar dos tareas de suma importancia: que vienen a ser el análisis de riesgos y el tratamiento de los riesgos; ambas actividades, se combinan en el proceso denominado Gestión de Riesgos.

La primera tarea permite evaluar estos componentes de forma metódica para alcanzar conclusiones con fundamento y proceder a la fase de tratamiento. Se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión. Formalmente, la gestión de los riesgos está estructurada de forma metódica en las normas ISO

Figura 3: Método de gestión de riesgos[26]



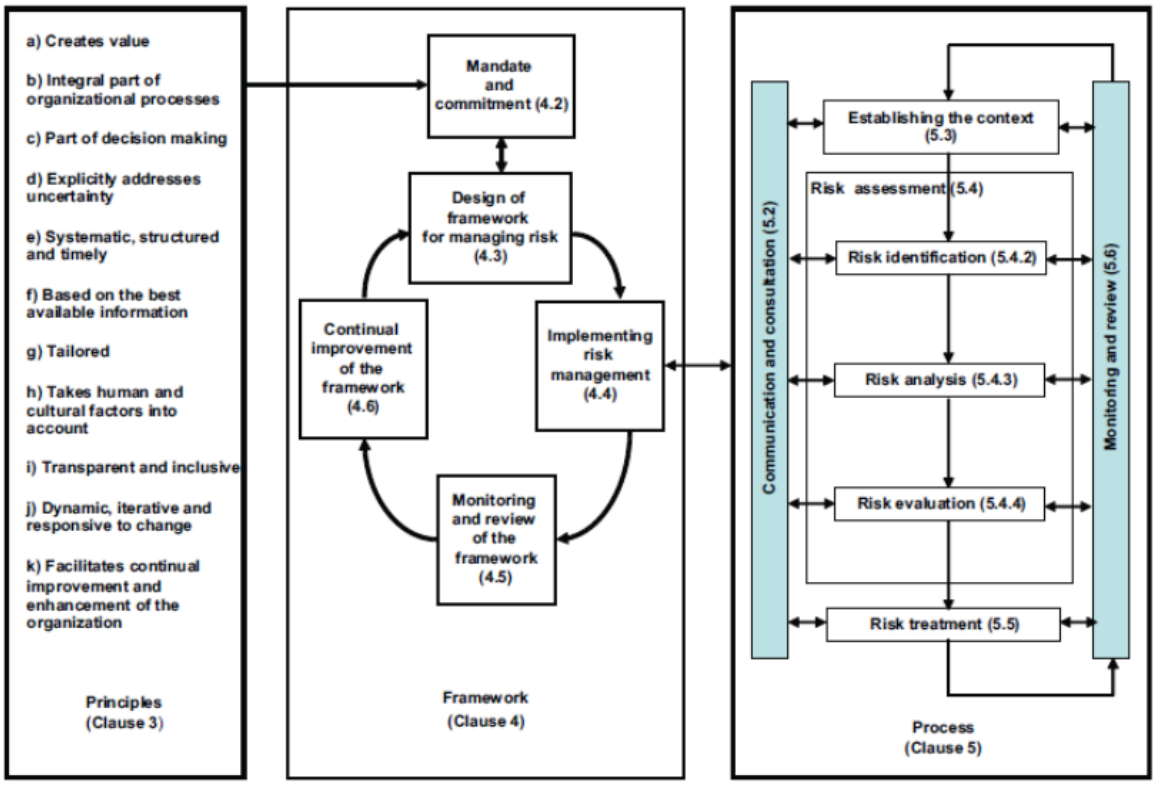
La presente metodología es tomada en cuenta porque resalta la importancia de conocer los riesgos dentro de las entidades, para poder así ejecutar un procedimiento de gestión de incidentes. Guiándonos de la forma en que se muestra en la figura 3.

1.2.2.7. Estándares ISO para la gestión de riesgo

1.2.2.7.1. ISO 31000

La presente norma [27] implanta una estructura que se debe de cumplir para poder gestionar correctamente los riesgos. también sugiere a las organizaciones implementar y optimizar permanentemente un esquema con el propósito de agrupar el desarrollo de gestión de riesgos en la gobernanza general de la entidad, planificación y estrategia, de gestión, procesos de información, las políticas, valores y cultura. El implementar gestionar riesgos se da para toda una entidad, incluyendo cada una de sus componentes y no se tiene que especificar algún tiempo determinado.

Figura 4: Proceso de riesgos y actividades que se realizan[27]



1.2.2.7.2. ISO 27000

Es una serie de estándares[28] que fueron diseñados para proteger los activos de información de las entidades. ISO 27000 brinda una descripción habitual de un Sistema de gestión de seguridad de la información (SGSI), especificando y detallando la serie de procesos evidentemente constituidos que encaminen a las entidades para organizar sus propósitos y finalidades comerciales con su garantía de la información.

Su función principal es la de guiar a las organizaciones a lo largo de su gestión de riesgos de seguridad de la información, desde la formulación hasta la ejecución, supervisión, ajuste, evaluación y mantenimiento, para garantizar que los activos de información confidencial estén protegidos, ya sea que son datos de primera mano o secundarios.

1.2.2.8. ITIL

Modelo que propone el funcionamiento continuo de los elementos y procesos para cualquier entidad para así, proporcionar el aumento de producción a través de actividades brindados por TI.

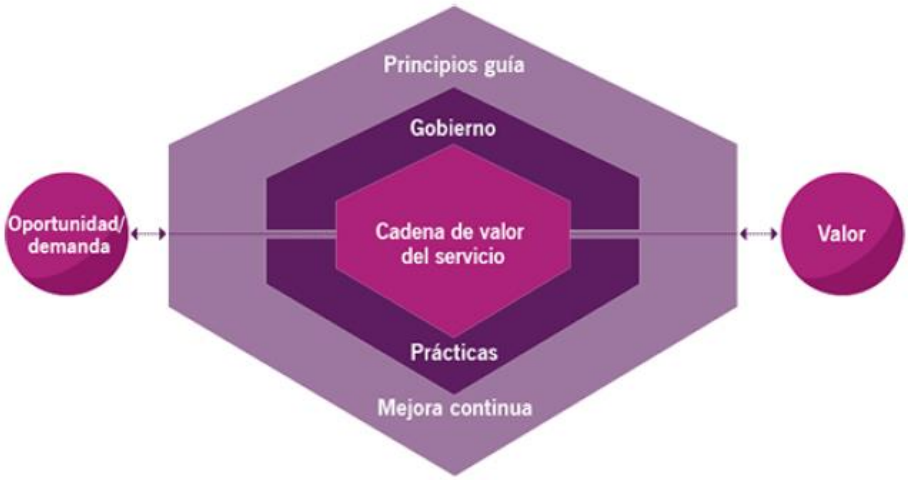
ITIL 4 [29] brinda las recomendaciones necesarias a las entidades para poder afrontar los desconocidos desafíos de la gestión de servicios y aplicar toda la capacidad de la tecnología innovadora. Se ha elaborado para garantizar un proceso compuesto, sistematizado y adaptable para alcanzar un servicio y una administración competente de los procesos proporcionados para TI.

Los elementos principales que conforman el esquema ITIL 4 son el sistema de valor del servicio (SVS) de ITIL y el modelo de las cuatro dimensiones.

Sistema de valor del Servicio [29]**:** Constituye la forma de trabajo de manera incorporada los variados elementos y procesos de la entidad para fomentar la producción de valor mediante procesos proporcionados para TI. Estos pueden acoplarse de manera adaptable, lo que debe de realizarse de forma conjunta y ordenada para preservar la congruencia de la entidad. El SVS de ITIL proporciona esta unificación y coherencia, y

facilita a la entidad una orientación a continuar concentrada en el valor, agrupada y consistente.

Figura 5: El sistema de valor de servicios[29]



El modelo de las cuatro dimensiones[29]: ITIL 4 enfatiza cuatro dimensiones de la gestión de servicios de las que se debería tomar en cuenta en cada componente del SVS. Estas dimensiones son:

- Organizaciones y personas
- Información y tecnología
- Socios y proveedores
- Procesos y flujos de valor.

Teniendo en cuenta cada componente, las entidades aseguran que su SVS sea de manera proporcional y eficaz.

II. Materiales y métodos

2.1. Tipo y nivel de investigación

El presente estudio es cuantitativo, puesto que se aplica el análisis estadístico, y es de tipo aplicada, ya que haciendo uso de las bases teóricas se proyecta emplear un modelo de gestión de riesgos que se adecue a las actividades de los institutos de educación superior tecnológicos públicos que permita poder minimizar riesgos a los que se encuentren expuesto y mejorar el desempeño organizacional. Por la necesidad de

rescatar información necesaria para el estudio, también se aplicó el instrumento de la entrevista

2.2. Diseño de investigación

El presente estudio será cuasi experimental, ya que se desarrolla con una variable independiente denominada modelo de gestión de riesgos de tecnología de información, para poder ver su efecto con una variable dependiente, garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos, se puede considerar el esquema cuasi experimental:

G 01X02

Donde:

- **G:** Grupo de estudio.
- **O1:** Continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos antes de la aplicación del modelo
- **X:** Modelo de gestión de riesgos de tecnología de información.
- **O2:** Continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos después de la aplicación del modelo.

2.3. Población, muestra y muestreo

2.3.1. Población

La población objetivo la conforman los institutos de educación superior tecnológicos públicos de la región Lambayeque (que son un total de 11 institutos)

TABLA 1: Listado de institutos públicos

NOMBRE DE IEST	DIRECCIÓN	DISTRITO
Chongoyape	Calle Miguel Iglesias n° 380	Chongoyape
República Federal de Alemania	Avenida Elvira García y García n° 755	Chiclayo
Edilberto Rivas Vasquez	28 de Julio	Cayaltí
Pascual Saco y Oliveros	Calle 2 de Mayo n° 548	Lambayeque
Motupe	Avenida Juan Pablo II n° 468	Motupe
Yatraywasi	Carretera Trocha Carrozable la Playa km 0.39	Incahuasi
Monsefu	Avenida Bernardo Alcedo n° 220	Monsefu
Ciudad Eten	Calle Mariscal Castilla s/n mz 104 lote 1	Eten
Íllimo	Calle 22 de Noviembre s/n	Íllimo
Olmos	Pasaje San Agustin s/n	Olmos
Enrique Lopez Albujar	Víctor Raúl Haya de la Torre #214	Ferreñafe

2.3.2. Muestra

La muestra que se considera a tener en cuenta en la investigación es el IEST Chongoyape caso de estudio conformado por 13 profesionales entre administrativos y docentes: de los cuales 4 son nombrados y 9 contratados. Distribuidos entre las áreas académica administrativa, en los programas de estudio de enfermería Técnica y arquitectura de plataforma de servicios de tecnología de la información (APSTI)

TABLA 2: Descripción de roles y responsables de la entidad

ROLES	RESPONSABLES
Dirección general	1
Unidad administrativa	1
Unidad académica	1
Secretaria académica	1
Coordinador de área de enfermería técnica	1
Coordinador de área de APSTI	1
Docentes	7
Total	**13**

2.3.3. Muestreo

En la presente investigación se usará el muestreo no probabilístico, ya que se tiene como caso de estudio al IEST-Chongoyape por el motivo de acceso a datos disponible.

2.4. Criterios de Selección

2.4.1. Variable independiente

Modelo de gestión de riesgos de tecnología de información

2.4.2. Variable dependiente

Garantizar la continuidad del servicio en los procesos organizacionales

2.5. Operacionalización de variables

La Operacionalización se aplica a la variable dependiente como se muestra a continuación en la tabla

TABLA 3: Operacionalización de variable dependiente

Definición Nominal	**Definición Operacional**		
Variable	**Dimensión**	**Indicadores**	**Escala de medición**
Continuidad del servicio en los procesos organizacionales	✓ Gestión de incidentes	✓ Número de incidentes registrados mensualmente	✓ Escala de razón
		✓ Tiempo en el que se recupera el servicio por incidencia	✓ Escala de intervalos
		✓ Tiempo de respuesta por incidencia	✓ Escala de intervalos
	✓ Gestión de riesgos de TI	✓ Identificación de riesgos internos y externos	✓ Escala nominal
		✓ Número de registro de riesgos	✓ Escala de la razón
		✓ Prioridad de riesgos	✓ Escala nominal

2.6. Técnica e instrumento de recolección de datos

Los instrumentos que se usarán en esta investigación son dos, una encuesta existente la que fue extraída de la alineación de la estrategia propuesta con los procesos catalizadores de COBIT, el cual consta de 24 preguntas a las que se agregó una escala de Likert, la segunda fue una entrevista que salieron del mismo instrumento antes mencionado, estas servirán para medir las dos dimensiones: gestión de incidentes y gestión de riesgos de TI.

2.7. Plan de Procedimiento análisis de datos

La información se almacenará en repositorio de datos para posteriormente analizar dichos datos, utilizando el software Excel para el tratamiento de datos necesarios en el diagnóstico del sector y así como tambien en la parte de validación del modelo. Los resultados se mostrarán mediante estadística descriptiva en cuadros con porcentaje.

2.8. Consideraciones Éticas

Se tomaron los criterios que se encuentran estipulados en norma de integridad científica **Integridad:** los temas que se presentan en la investigación son totalmente íntegros, con la finalidad de poder contribuir con las investigaciones en la región Lambayeque.

Honestidad intelectual: Dentro de toda la investigación sobre los procesos que se abarcan para poder realizar los objetivos esperados, se está trabajando de manera honesta sin alterar ni manipular información a conveniencia.

Transparencia: La presente investigación se está realizando de forma clara recabando información y realizando los procesos sin ningún interés económico o monetario.

2.9. Matriz de consistencia

Se presenta la matriz de consistencia de la presente investigación, en donde detallamos puntos específicos y que guardan relación entre sí.

TABLA 4: Matriz de consistencia de la presente investigación

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES
PROBLEMA GENERAL: ¿De qué manera la implementación de un modelo de gestión de riesgos de tecnología de información influyen para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación	**OBJETIVO GENERAL:** Implementar un modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos **OBJETIVOS ESPECÍFICOS:** a. Armonizar los marcos de trabajo de la gestión de riesgo de TI, con base en los criterios para adaptarlo al contexto de los Institutos de Educación Superior Tecnológicos Públicos.	**HIPÓTESIS GENERAL:** Si se desarrolla el modelo de gestión de riesgos de tecnología de información, entonces se garantiza la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos	**VARIABLES DE ESTUDIO:** **VARIABLE INDEPENDIENTE:** Modelo de gestión de riesgos de tecnología de información **VARIABLE DEPENDIENTE:**

superior tecnológicos públicos.?	b. Analizar los procesos organizacionales para evaluar los servicios que permitan formular los componentes del modelo de gestión de riesgos de TI c. Proponer el modelo de gestión de riesgos con el propósito de contribuir con la continuidad del servicio en los procesos organizacionales. d. Validar el modelo propuesto a través de juicio de expertos con la finalidad de garantizar su aplicación y contribución en el IESTP-Chongoyape e. Implementar el modelo de gestión de riesgos de TI para garantizar la continuidad del servicio en los procesos organizacionales en el IESTP-Chongoyape		Garantizar la continuidad del servicio en los procesos organizacionales

2.10. Cronograma de actividad y Presupuestos

Cronograma: Se muestra el cronograma que se tendrá en cuenta para la presente investigación

TABLA 5: Cronograma de la presente investigación

ACTIVIDADES	2022								2023																			
	NOVIEMBRE				DICIEMBRE				ENERO				JUNIO				JULIO				NOVIEMBRE				DICIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
FASE EJECUCIÓN																												
Definición de problemática																												
Definición del plan de investigación																												
Recaudación de información																												
Procesamiento de información																												
Definición de metodología de investigación																												
FASE COMUNICACIÓN																												
Análisis e interpretación de resultados																												
Redacción del informe																												
Presentación del Informe																												

Presupuesto:

Bienes: Se listan los bienes necesarios para la elaboración de la investigación en cada una de sus fases.

TABLA 6: Bienes que se utilizaran en la presente investigación

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO (S/.)	PRECIO TOTAL (S/.)
01	Paquete de hojas A4	S/15.00	S/15.00
05	Lapiceros	S/03.00	S/15.00
01	Cuaderno de apuntes	S/05.00	S/05.00
01	Libro ITIL V4	S/76.00	S/76.00
12	Laptop HP (depreciación mensual)	S/43.75	S/525.00
	TOTAL		**S/636.00**

Servicios: Se listan a continuación los servicios necesarios para la elaboración de la presente investigación

TABLA 7: Servicios que se utilizaran en la presente investigación

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO (S/.)	PRECIO TOTAL (S/.)
12	Pasajes /1 persona	S/36.00	S/432.00
12	Alimentación	S/10.00	S/120.00
12	Plan de internet mensual	S/70.00	S/840.00
01	Procesamiento de datos	S/300.00	S/300.00
01	Copias e impresiones	S/30.00	S/30.00
	TOTAL		**S/1722.00**

General: Descripción general de los bienes y servicios necesarios para la presente investigación

TABLA 8: Resumen de bienes y servicios

MESES	SUB TOTAL
Bienes	S/636.00
Servicios	S/1722.00
TOTAL	**S/ 2358.00**

III. Resultados y discusión

Se va desarrollar la explicación de cada objetivo específico establecido en la presente investigación, iniciando con la parte de diagnóstico del sector, a pesar de no ser uno de los objetivos, pero es de suma importancia para esta investigación realizar dicho diagnóstico.

3.1. Diagnóstico del sector de educación superior tecnológico público.

Se estable el contexto de las instituciones educativas, del sector público del nivel superior tecnológico de la región de Lambayeque, las que fueron elegidas para efectuar el análisis del contexto con el fin de optimizar la planificación para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos.

Las instituciones educativas de nivel superior tecnológicas seleccionadas con más de 30 años de servicio, cuentan con sus planes estratégicos donde se estipulan su misión visión, valores, objetivos estratégicos y su plan de trabajo PEI. (Ver anexo 02)

Para realizar el diagnóstico de la gestión de riesgos de TI en los institutos tecnológicos públicos de la región Lambayeque, se aplicó una encuesta (ver anexo 03) la que estaba

dirigida al personal directivo y administrativo. También se aplicó una entrevista la que estaba dirigida a la alta dirección, ambos instrumentos están basados en COBIT.

El diagnóstico parte de la aplicación de una encuesta a la muestra de estudio con la finalidad de diagnosticar como se encuentran sus procesos organizacionales obtenido como resultado lo siguiente:

Conforme a los resultados adquiridos del instrumento encuesta, muestra que un 38% tiene conocimiento de la existencia de un plan estratégico; mientras que un 25 % no. Por lo que se concluye que los institutos no tienen claramente definido un plan estratégico de TI.

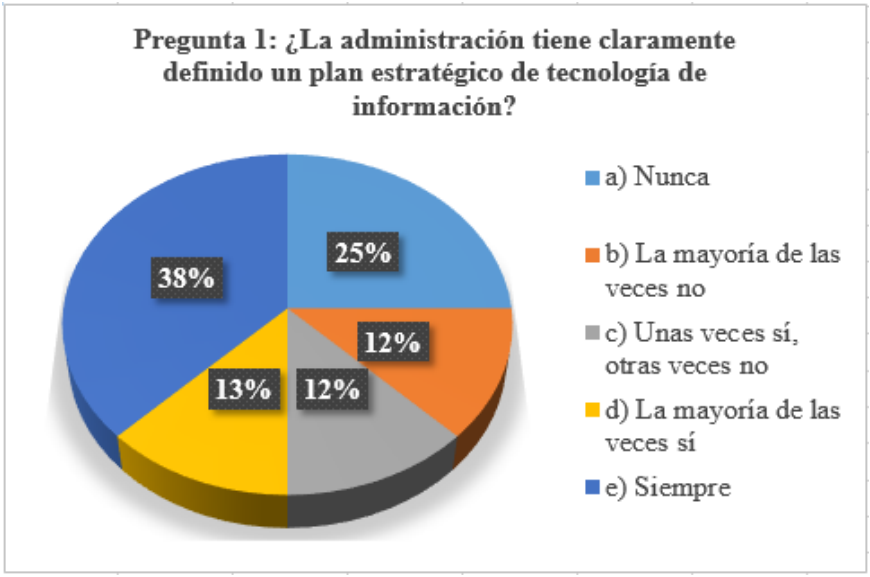


Figura 7: Análisis de plan estratégico

Por otra parte, el 37% de encuestados concuerdan en que no se efectúan evaluaciones a los planes estratégicos de TI; también destacaron que no cuentan con un plan para la adquisición o restructuración de TI. además, el 62 % expresaron que en algunas ocasiones se definen procesos para informar al personal sobre la adquisición e implementación de TI.

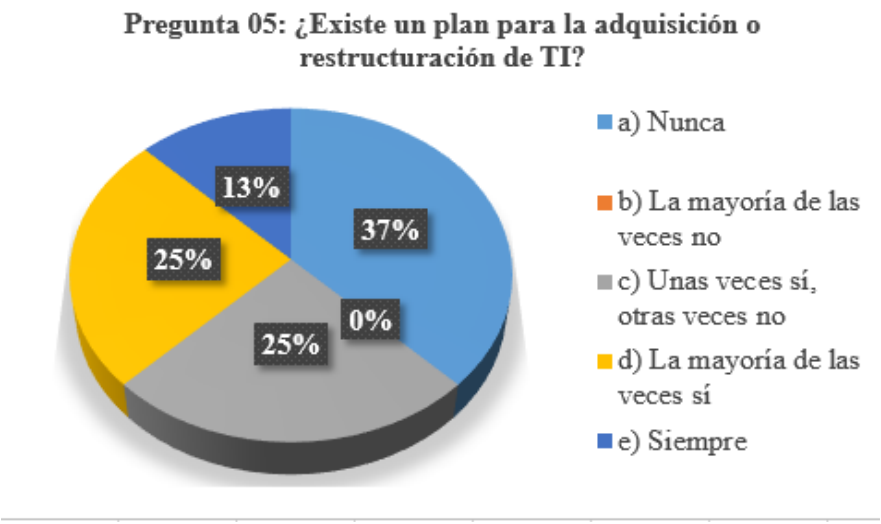


Figura 8: Información de existencia de plan de adquisición de TI

Por otro lado, el 50 % menciona que no se han definido, planeado e implementado medios para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con TI, siendo esto de vital importancia para la mejora de sus procesos organizacionales. Además, el 50 % menciona que no se administran y controlan los riesgos relacionados con TI, a pesar de que es una parte fundamental que se debería de realizar para asegurar la continuidad de los procesos organizacionales.

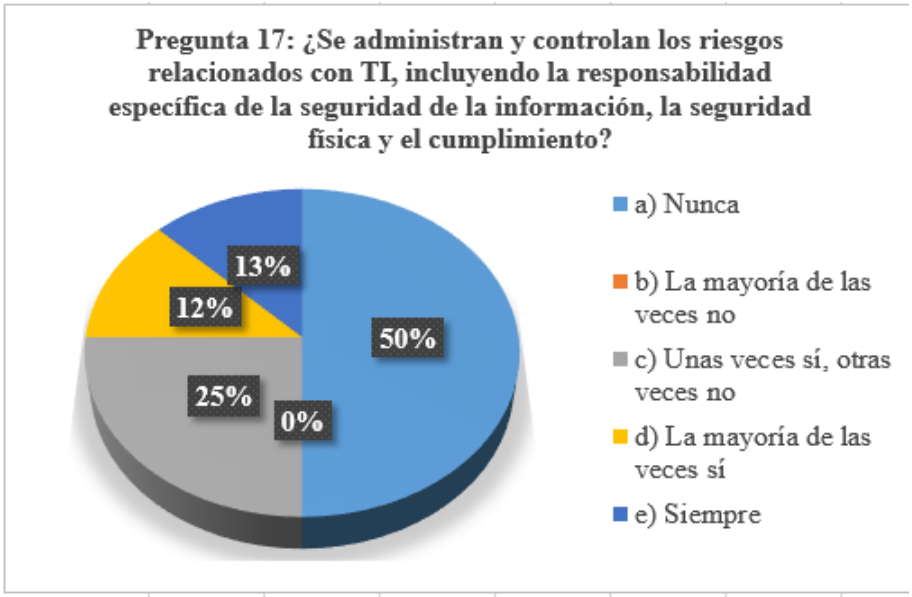


Figura 9: Información de administración y control de riesgos

También el 50% mencionan que no se ha definido una estrategia de distribución de los planes de contingencia ante riesgos, generando dificultades dentro de los procesos ante una reacción contra algún riesgo que se presente. Además, el 37% hace mención que no se encuentran definidos dichos sucesos (amenazas y vulnerabilidades) con impacto potencial sobre los objetivos o las actividades de los institutos.

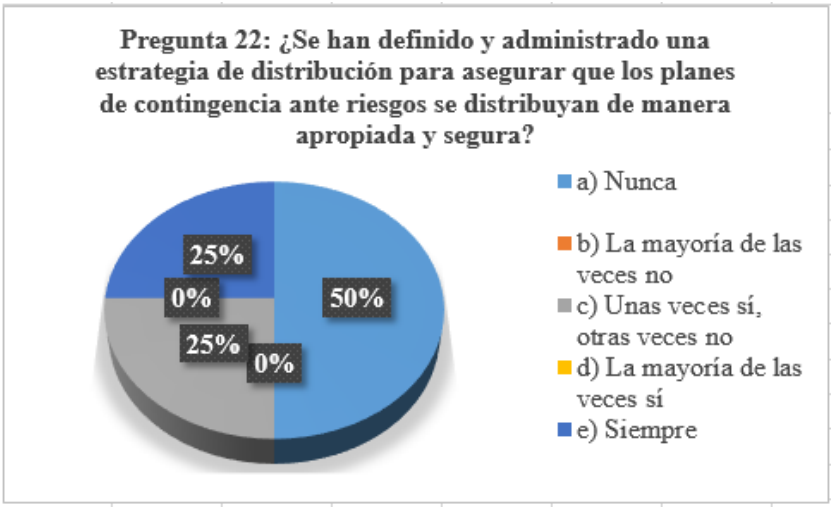


Figura 10: Información sobre definición y administración de estrategias

De los resultados de la entrevista (ver anexo 03) que se le aplico a la alta dirección en los institutos seleccionados con la finalidad de obtener información mucho más relevante para el caso de estudio se puede concluir con lo siguiente:

Los institutos cuentan con un plan de trabajo que realizan actividades referidas a un plan estratégico de TI; muestran dificultades en la revisión y manejo de los activos de TI, ya que no cuenta con indicadores de evaluación de los procesos, generando una baja inversión en tecnología, debido a la deficiencia de sus procesos y de la falta de presupuesto anual dedicado a TI.

Respecto a la continuidad y mejora de TI, no cuenta con un plan de mejora de sus servicios, no cuenta con un plan de capacitación de concientización de sus colaboradores respecto a TI, generando que dentro de los institutos no exista una mejora en sus procesos organizacionales.

3.2. Armonización de marcos de trabajo, metodologías, estándares y normas de gestión de riesgos de TI.

Para poder realizar la propuesta del modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos, se analizaron las siguientes estándares y marcos de trabajo:

- COBIT FOR RISK
- ITIL
- MAGERIT
- ISO 31000
- ISO 27000
- AS/NZ 4360:204

Una vez definidas los estándares o marcos de trabajo se analizaron de forma general para determinar la afectación en la gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales; además de cada estándar o marco de trabajo se determinó su enfoque y su viabilidad de uso.

Estos estándares o marcos comparten el objetivo común de gestionar los riesgos de TI para garantizar la confidencialidad, integridad y disponibilidad de los activos de información. Sin embargo, difieren en cuanto a su alcance y enfoque de la administración de riesgos.

En la siguiente tabla se observa la comparación entre los estándares o marcos elegidas para el desarrollo del modelo:

TABLA 9: Comparación de estándares o marcos

	COBIT FOR RISK 5	ITIL 4	MAGERIT 3.0	ISO 31000-2018	ISO 27000-2016	AS/NZ 4360:204
Objetivo	Proporcionar un marco para la gestión de riesgos de TI. Y alinear la gestión de riesgos con los objetivos comerciales	Proporcionar una orientación sobre la gestión de servicios y procesos de TI	Proporcionar una enfoque sistemático para la gestión de riesgos,	Proporcionar un marco de gestión de riesgos y directrices para la gestión de riesgos en todo tipo de organizaciones	Proporcionar un marco para gestionar los riesgos de seguridad de la información.	Proporcionar pautas sobre la gestión de riesgos en todo tipo de organizaciones
Alcance	Centrado en la gestión de riesgos de TI dentro del contexto de los objetivos comerciales	Centrado en un conjunto de mejores prácticas para la gestión de servicios de TI	Centrado en la identificación, el análisis, la evaluación, el tratamiento y el seguimiento de los riesgos	Centrado en implantar una estructura que se debe de cumplir para poder gestionar correctamente los riesgos	Centrado en establecer las mejores prácticas vinculados a la gestión de la seguridad de la información	Centrado en una guía genérica para el establecimiento e implementación del proceso de administración de riesgos

Características	-Conjunto integrado de controles -Gestiona y evalúa riesgos -Es flexible	-Calidad de servicio mejorada -Mayor eficiencia -Mejor comunicación -Mejora la satisfacción del cliente. -Mejora la prestación de servicios de TI	-Gestión de riesgos -Flexibilidad -Seguridad de la información -Marco integrado	-Marco integral para la gestión de riesgos -Ofrece mejora continua -Enfoque holístico -El estándar fomenta el pensamiento basado en el riesgo -Enfatiza la importancia de la comunicación y la consulta en la gestión de riesgos	-Adopta un enfoque basado en riesgos -Es un estándar flexible y adaptable a cualquier organización -Integración de gestión de seguridad de información -Enfatiza la importancia de la mejora continua en la gestión de seguridad	-Marco integral para la gestión de riesgos -Es un marco flexible -Mejora continua en la gestión de seguridad

Beneficios	-Gestión de riesgos -Riesgos estandarizados -Mejores tomas de decisiones -Mayor transparencia	-Mejora la calidad de servicio -Gestión de servicios de TI y reducción de costos -Gestión de riesgos mejorada -Mejora la medición y rendimiento de TI	-Enfoque en la seguridad de la información -Basado en las mejores prácticas internacionales -Análisis integral de riesgos -Flexibilidad -Integración con otros marcos	-Gestión integral de riesgos -Mejora la alineación de los procesos -Mejora la concientización de riesgos -Mejora los planes de contingencia	-Seguridad de la información mejorada -Cumplimiento de las normas y estándares -Mayor confianza de las partes interesadas	-Riesgo mejorado -Mejora de decisiones -Eficiencia mejorada Cumplimiento de estándares
Enfoque	Se enfoca en administrar los riesgos de TI y alinearlos con los objetivos comerciales	Se Enfoca principalmente en mejorar la prestación de servicios y la satisfacción del cliente	Se Enfoca en riesgos de seguridad de la información dentro del marco de gestión de riesgos organizacionales	Se enfoca en los principios, el marco y el proceso de gestión de riesgos.	Se enfoca en la orientación sobre evaluación de riesgos, tratamiento de riesgos y	Se enfoca en la orientación sobre identificación, evaluación, tratamiento y

	monitoreo de riesgos, entre otras cosas	seguimiento de riesgos.

Se procedió a realizar una distinción de cada uno de los estándares y marcos seleccionados, con la finalidad de poder establecer si hacen referencia a la gestión de riesgos. Obteniendo como resultado la selección de tres de ellos, las que se analizarán de manera más minuciosa para poder determinar la construcción del nuevo modelo.

TABLA 10: Armonización de estándares o marcos de trabajo seleccionados

DIMENSIONES	COBIT FORT RISK 5	ISO 31000-2018	MAGERIT 3.0
Estructura del marco	Marco basado en procesos con cinco fases: Identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento de riesgos, monitoreo y revisión de riesgos	Marco basado en principios con tres componentes: Marco de gestión de Riesgos, proceso de gestión de riesgos, cultura de gestión de riesgos	Marco basado en procesos con cuatro fases: Inicio, análisis, evaluación, tratamiento
Procesos de gestión de riesgos	- Identificación de riesgos - Análisis de riesgos - Evaluación de riesgos - Tratamiento de riesgos - Seguimientos y revisión de riesgos	- Establecimiento del contexto - Evaluación de riesgos - Tratamiento de riesgos - Comunicación y consulta de riesgos	- Identificación de riesgos - Análisis de riesgos - Evaluación de riesgos - Tratamientos de riesgos - Seguimiento de riesgos
	Utiliza terminologías específicas de TI, como: - Riesgo de TI	Utiliza terminologías generales de gestión de riesgos: - Apetito por el riesgo	Utiliza terminología especifica de seguridad de la información:

Terminología de gestión de riesgos	- Gobierno de TI - Control de TI - Cumplimiento de TI	- Tolerancia al riesgo - Criterios de riesgo - Comunicación de riesgos	- Nivel de seguridad - Activo - Amenaza - Vulnerabilidad - Medida de seguridad
Fortalezas	Proporciona una guía detallada sobre la gestión de riesgos de TI	Proporciona una perspectiva amplia sobre la gestión de riesgos en toda la organización	Proporciona un marco integral para la gestión de riesgos de seguridad de la información en el sector público

Los marcos seleccionados otorgan una visión de gestión de riesgos más completa. Por ejemplo, COBIT FORT RISK 5 brinda una guía detallada sobre la gestión de riesgos de TI, mientras que ISO 31000-2018 brinda un criterio más extenso sobre la administración de riesgos en la entidad completa, por su parte MAGERIT 3.0 proporciona un marco integral para la gestión de riesgos de seguridad de la información en el sector público. Al combinar las fortalezas de estos marcos, las organizaciones pueden desarrollar un enfoque más sólido e integral para la administración de riesgos que se ajuste a sus requerimientos y contexto específico.

3.3. Análisis de los procesos organizacionales del sector de educación superior tecnológico público.

Se realizó el análisis de los procesos organizacionales de los institutos públicos de la región Lambayeque. En donde se identificó que sus procesos específicos son admisión, desarrollo curricular, reclutamiento de profesionales, servicios de apoyo o convenios con instituciones para beneficios de los estudiantes, garantizar calidad y planificación estratégica a través de la actualización de su infraestructura ya sea tangible o intangible.

Gracias a los instrumentos de recolección de datos como fueron la entrevista y encuesta se deduce que los procesos antes mencionados, no tienen una buena eficiencia debido a la falta de mejoras en sus procesos. Además, no cumplen con los lineamientos que demanda las normas del estado, es decir desarrollan los procesos, pero con falencias de control, planificación y documentación. Tambien se evidenció la falta de un plan de acción ante la presencia de algún posible riesgo.

Es por este motivo que se plantea la propuesta del modelo de esta tesis, para mejorar y hacer cumplir los lineamientos que las autoridades de educación disponen, por ejemplo, las condiciones básicas de calidad para el proceso de licenciamiento de los institutos, los estándares de calidad académicos y las políticas gubernamentales de contexto educativo.

3.4. Propuesta de modelo de gestión de riesgos con el propósito de contribuir con la continuidad del servicio en los procesos organizacionales.

Bajo el análisis mencionado en el punto anterior la propuesto del modelo producto de esta tesis es la siguiente:

Figura11: Modelo de gestión de riesgos de TI para institutos

3.4.1. Desarrollo de la propuesta

Se propone el desarrollo de un modelo teniendo como mención a los marcos de trabajo de riesgos de TI seleccionados en el punto anterior, para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos. Lo que permitirá diagnosticar los posibles escenarios de riesgos a lso que pueden estar comprometidos las actividades que soporta la.

Se procede a describir el modelo propuesto (ver figura 11):

Fase 01: Descripción del contexto

En esta fase se definen los componentes internos y externos identificados en el objeto de estudio, también se establece los alcances y criterios de riesgos, asi como los roles y responsabilidades dentro de las entidades pedagógicas superiores. Para asegurar la continuidad de estos servicios ante posibles disrupciones.

Proceso DC01: Contexto interno

Para poder definir este proceso, las entidades tienen que alinear sus procesos actividades que se desarrolla en el objeto de estudio que son los institutos.

- **Estructura institucional**

  Se emplea para comprender el organigrama de la organización y poder determinar las áreas de institutos involucradas en la continuidad de los procesos organizacionales. Lo que permite determinar las estrategias para lograr la obtención de los objetivos.

  Fuente de información: organigrama institucional, MOF

- **Metas institucionales**

  Se implementa para identificar las metas necesarias que se deben de cumplir en las instituciones educativas. (Actividad que se necesita para poder establecer la meta)

  Fuente de información: PEI institucional

- **Incidencias relacionadas con TI**

  Son los diferentes hechos que se formulan desde las áreas para atención de TI en las instituciones. Tales como, pérdida de datos, errores en los procesos, recursos de TI que no an recibido mantenimiento preventivo, el uso de los recursos de TI de manera empírica por parte del personal.

Para poder realizar el proceso 1 del modelo, se establece una plantilla, donde intervienen los directivos de las instituciones y personal de TI

Figura 12: Contexto interno

LOGO DE INSTITUTO	**NOMBRE DE INSTITUTO**			
	FASE 01:	Descripción del contexto	FECHA DE ELABORACIÓN	___/___/___
	Proceso DC01 :	Contexto Interno	FECHA DE APLICACIÓN	___/___/___
OBJETIVO:	Descripción del contexto interno de la institución para poder mejorar las estrategias institucionales.			
ESTRUCTURA INSTITUCIONAL				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
EI_01	Organigrama Institucional		Se emplea para determinar los activos de la institución, permitiendo determinar estrategias para lograr sus objetivos.	
METAS INSTITUCIONALES				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
MI_01	Proyecto educativo institucional (PEI)		Se enumeran las metas de la institución que deben de ser cumplidas.	
INCIDENTES RELACIONADOS CON TI				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
IR_01	Incidentes vinculados con TI		Incidentes vinculados con TI, como pérdida de datos, error en los procesos.	
RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**	
NOMBRE	Nombre completo del responsable de la creación de la plantilla.	Nombre completo del responsable de la revisión de la plantilla.	Nombre completo del responsable de la aprobación de la plantilla.	
FECHA				
FIRMA				

Proceso DC02: Contexto Externo

En este proceso las instituciones deberán de abarcar el entorno externo lo que le servirá para poder utilizar las oportunidades y prevenir los riesgos institucionales.

- **Cultura:** Nos mostrará el nivel socioeconómico de los apoderados y estudiantes de acuerdo a su zona de desempeño. Fuente de información: INEI
- **Política:** Mostrará las normas y leyes que rigen a las entidades de educación superior y a los entes reguladores como el MINEDU Y GRE
- **Tecnológico:** Se define la actualización de la tecnología que se puede implementar para garantizar la continuidad de los servicios en los procesos organizacionales de las instituciones en estudio.

  Fuente de información: Publicaciones de nuevas tecnologías (Hardware y Software)

Figura13: Contexto Externo

<table>
<tr><td rowspan="2">LOGO DE INSTITUTO</td><td colspan="4">NOMBRE DE INSTITUTO</td></tr>
<tr><td>FASE 01:</td><td>Descripción del contexto</td><td>FECHA DE ELABORACIÓN</td><td>___/___/___</td></tr>
<tr><td></td><td>PROCESO DC02:</td><td>Contexto Externo</td><td>FECHA DE APLICACIÓN</td><td>___/___/___</td></tr>
<tr><td>OBJETIVO:</td><td colspan="4">Descripción del contexto externo de la institución para poder prevenir las amenazas a la que están expuestas</td></tr>
<tr><td colspan="5">CULTURA</td></tr>
<tr><td>CODIGO</td><td colspan="2">ESTRUCTURA</td><td colspan="2">DESCRIPCIÓN</td></tr>
<tr><td>CU_01</td><td colspan="2">Datos de INEI</td><td colspan="2">Se emplea para determinar los niveles socioeconómicos.</td></tr>
<tr><td colspan="5">POLÍTICA</td></tr>
<tr><td>CODIGO</td><td colspan="2">ESTRUCTURA</td><td colspan="2">DESCRIPCIÓN</td></tr>
<tr><td>PO_01</td><td colspan="2">MINEDU Y GRE</td><td colspan="2">Marco normativo que deben de cumplir las instituciones</td></tr>
<tr><td colspan="5">TECNOLÓGICO</td></tr>
<tr><td>CODIGO</td><td colspan="2">ESTRUCTURA</td><td colspan="2">DESCRIPCIÓN</td></tr>
<tr><td>TE_01</td><td colspan="2">Publicaciones de nuevas tecnologías</td><td colspan="2">Tecnologías existente para la mejora de los procesos organizacionales de los institutos</td></tr>
<tr><td>RESPONSABLE</td><td>ELABORADO</td><td colspan="2">REVISADO</td><td>APROBADO</td></tr>
</table>

NOMBRE	Nombre completo del responsable de la creación de la plantilla.	Nombre completo del responsable de la revisión de la plantilla.	Nombre completo del responsable de la aprobación de la plantilla.
FECHA			
FIRMA			

Proceso DC03: Definición de alcance y criterios de riesgo

Consiste en identificar y analizar las amenazas comunes y los requerimientos de seguridad vinculados con el sector de la entidad; para validar si la implementación generara la continuidad del servicio para las organizaciones. Para ello deben de disponer criterios para evaluar sus activos: Disponibilidad, confidencialidad e Integridad. Los cuales nos basaremos de COBIT teniendo como valor (1-5) donde 1 es el valor más bajo y 5 el valor más crítico.

TABLA 11: Nivel de disponibilidad

NIVEL	DISPONIBILIDAD
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

TABLA 12: Nivel de Confidencialidad

NIVEL	CONFIDENCIALIDAD
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

TABLA 13: Nivel de Integridad

NIVEL	INTEGRIDAD
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Criterios de Riesgo

Donde los institutos deben de establecer los métodos para la estimación de riesgos. El proceso debe analizar la probabilidad y el impacto de cada riesgo identificado, teniendo en cuenta el contexto especifico y las características de cada instituto público.

Paso 1: Criterio de Probabilidad: Define la ocurrencia de algún evento de riesgo que se pueda presentar en los institutos tecnológicos; contando con una escala del 1 al 5 y con una probabilidad de frecuencia de ocurrencia (que puede ser en meses o años) establecida por consenso del equipo de TI, de la forma como se muestra en la siguiente tabla.

Figura 14: Criterios de probabilidad

CRITERIO DE PROBABILIDAD			
ID	NIVEL	ESCENEARIO	COLOR
1	Muy bajo	01 vez cada 5 años	
2	Bajo	01 vez cada 3 años	
3	Medio	01 vez al año	
4	Alto	01 vez por semestre	
5	Muy alto	01 vez cada mes	

Paso 2: Criterio de Impacto: Define el daño o pérdida potencial que puede resultar de algún evento de riesgo como pérdidas financieras, interrupción de procesos, entre otros. Cuenta con una escala del 1 al 5 y el impacto establecida por consenso del equipo de TI según lo mencionado al inicio sobre la pérdida.

Figura 15: Criterio de impacto

CRITERIO DE IMPACTO			
ID	**NIVEL**	**ESCENEARIO**	**COLOR**
1	Muy bajo	Impacto insignificante en el logro de los objetivos de los institutos	
2	Bajo	Impacto menor, fácilmente remediable para los institutos	
3	Medio	Se afectan algunos objetivos estratégicos de los institutos	
4	Alto	Algunos objetivos estratégicos no serán logrados en los institutos	
5	Muy alto	La mayoria de los objetivos estratégicos no serán logrados en los institutos	

Paso 3: Análisis de Riesgos: Define la forma como los institutos deben de analizar sus riesgos una vez definidos la probabilidad y el impacto

Figura 16: Análisis de riesgos

Análisis de Riesgo			
Probabilidad	**Impacto**	**P * I**	**Categoria**
1	1	1	
2	2	4	
3	3	9	
4	4	16	
5	5	25	

Paso 4: criterio de aceptabilidad

Se establecen los indicadores de riesgos, que les permitirá a los institutos tomar una decisión respecto al riesgo que están dispuestos a aceptar para poder establecer estrategias de continuidad en sus procesos, o por otra parte establecer medidas contra el riesgo; para ello el equipo de TI de los institutos de acuerdo al desarrollo de sus procesos tienen que definir el apetito y la tolerancia para que puedan evaluar los riesgos que se les presenten.

Apetito: nivel de riesgo que el equipo de TI de los institutos está dispuesto a asumir para la continuidad de sus procesos.

Tolerancia: máximo nivel de riesgo que los institutos están dispuestos a asumir antes de que se vuelva inaceptable el riesgo.

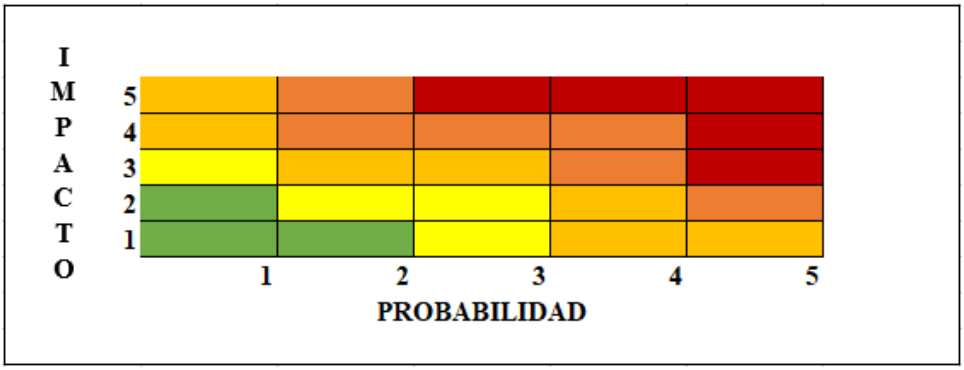
Los institutos después de realizar el análisis de la probabilidad por el impacto, deberán de decidir de acuerdo a sus criterios establecidos, para poder determinar su nivel de aceptabilidad.

Figura 17: Criterio de aceptabilidad

CRITERIO DE ACEPTABILIDAD DE RIESGOS			
ID	**NIVEL**	**COLOR**	**CRITERIO**
1	Muy bajo		ACEPTABLE
2	Bajo		ACEPTABLE
3	Medio		NO ACEPTABLE
4	Alto		NO ACEPTABLE
5	Muy alto		NO ACEPTABLE

Una vez que las instituciones ya tienen definido los puntos anteriores, proceden a comparar los resultados de la probabilidad por el impacto con los criterios de aceptación; para determinar que riesgos son aceptables y que riesgos no; para ello se muestra a continuación una plantilla con la que pueden verificar el mapa de calor para cada riesgo:

Figura 18: MATRIZ DE CALOR DE RIESGOS:



Proceso DC04: Definición de roles y responsabilidades

Este proceso se basa en COBIT FOR RISK, donde especifica que un marco de gestión de riesgos efectivo, debe de involucrar funciones y responsabilidades claras para todas las personas involucradas en los diferentes procesos de los institutos.

Los roles y responsabilidades se refieren a las tareas y actividades específicas que el personal y los grupos son responsables para llevar a cabo para identificar, evaluar y gestionar los riesgos. Lo que incluye responsabilidad para definir políticas y procedimientos, asignar tareas sobre gestión de riesgos a personal o equipos específicos para asegurar que las actividades se ejecuten de forma coherente y competente en toda la organización.

Figura 19: Formato de definición de roles y responsabilidades

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 01:	Descripción del contexto	FECHA DE ELABORACIÓN	___/___/___
	PROCESO DC04:	Definición de Roles y responsabilidades	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Contiene la matriz de roles y responsabilidades del personal involucrado en los diferentes procesos de los institutos: Director (D), Responsable (R), Supervisor (S), Ejecutor (E), Informado (I)			
CÓDIGO	**ROL Y RESPONSABILIDAD**		**RESPONSABLE**	
01	D	Especificar el rol o responsabilidad	Especificar el nombre del responsable de dicha actividad	
02	S		…	
..	...		…	
#N..	...		...	
RESPONSABLE	**ELABORADO**		**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla		Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA				
FIRMA				

Proceso DC05: Documentación de la fase

Consiste en documentar cada proceso anterior con la finalidad de llevar un control de actividades programadas y cumplidas, ya que es parte de los requerimientos de las condiciones básicas de calidad para el licenciamiento de institutos.

Figura 20: Documentación de la fase

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 01:	Descripción del contexto	FECHA DE ELABORACIÓN	___/___/___
	PROCESO DC05:	Documentación de la fase 01	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Contiene la matriz de roles y responsabilidades de los procesos con sus respectivos responsables de la fase 01			
FASE	**ROL Y RESPONSABILIDAD**		**RESPONSABLE**	**ESTADO DE FASE**
FA1_01				
FA1_02				
FA1_03				
FA1_04				
RESPONSABLE	**ELABORADO**		**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla		Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA				
FIRMA				

Fase 02: Gestión de valoración

Esta fase tiene como prioridad definir un plan integral de gestión de riesgos que describa el enfoque de la entidad para gestionar los riesgos. Adaptándose a las necesidades

específicas de la organización y debe de revisarse y actualizarse periódicamente para garantizar que sigue siendo eficaz en la gestión de riesgos.

Proceso GV01: Identificación de activos

Este proceso consiste en identificar y clasificar los activos de TI en función de su valor, criticidad y sensibilidad (ver tabla 11. 12 y 12), esto ayuda a las organizaciones a comprender qué activos son más importantes para sus operaciones y priorizar los esfuerzos de gestión de riesgos. También es importante conservar un inventario actualizado de los activos y comprender las independencias entre otros activos para garantizar que los riesgos se gestionen adecuadamente.

Los procesos que se contemplan en el documento de CBC de licenciamiento, servirá para identificar con cuál de los procesos cuentan los institutos.

Para el desarrollo de este proceso se especifica el siguiente formato:

Figura 21: Identificación de procesos

<table>
<tr><td rowspan="3">LOGO DE INSTITUTO</td><td colspan="5">NOMBRE DEL INSTITUTO</td></tr>
<tr><td>FASE 02:</td><td>Gestión de valoración</td><td>FECHA DE ELABORACIÓN</td><td colspan="2">___/___/___</td></tr>
<tr><td>PROCESO GV01:</td><td>Identificación de procesos</td><td>FECHA DE APLICACIÓN</td><td colspan="2">___/___/___</td></tr>
<tr><td>OBJETIVO</td><td colspan="5">Identificar con cuáles de los procesos de CBC del licenciamiento, cuentan los institutos</td></tr>
<tr><td>Área</td><td colspan="2"></td><td>Responsable</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Código</td><td colspan="2" rowspan="2">Proceso</td><td colspan="2">Respuesta</td><td rowspan="2">Observación</td></tr>
<tr><td>Si</td><td>No</td></tr>
<tr><td>CBC-I</td><td colspan="5">Gestión institucional</td></tr>
</table>

	Gestión estratégica			
	Estructura organizativa			
	Régimen académico			
	Registro de información académica			
	Bienestar estudiantil			
	Seguimiento al egresado			
CBC-II	**Gestión académica y programas de estudios pertinentes**			
	Gestión académica			
	Pertinencia de los programas de estudios			
	Gestión de investigación			
CBC-III	**Infraestructura Física**			
	Disponibilidad de infraestructura y equipamiento			
	Disponibilidad de recurso o materiales bibliográficos			
	Disponibilidad de servicios básicos, telefonía e internet			
CBC-IV	**Previsión económica y financiera compatible con los fines**			
	Provisión económica y financiera			

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA			
FIRMA			

Una vez identificados los procesos de los institutos, se procede a la identificación de activos que el Área de TI ofrece a las diferentes áreas para garantizar la continuidad de los procesos organizacionales:

- **Activo Software**: Hace referencia a todas las aplicaciones de las áreas de los institutos que TI tiene a cargo. Las cuales son utilizadas por las áreas de los institutos para poder garantizar la continuidad de sus servicios.
- **Activo Hardware**: Hace referencia a todas los equipos o parte de equipos informáticos de TI. Los que son utilizados para dar soporte a los procesos de las diferentes áreas de los institutos
- **Activo servicio:** Hace referencia al mantenimiento y soporte continuo de los sistemas, aplicaciones e infraestructura de tecnologías, incluyendo tareas como monitorear el rendimiento de los sistemas, solucionar problemas, aplicar parches y actualizaciones y garantizar la continuidad de los procesos organizacionales.

A continuación, se le presenta la siguiente plantilla en la figura 22, la que le servirá para determinar los activos de los institutos:

Figura 22: Identificación de Activos

LOGO DE INSTITUTO	**NOMBRE DEL INSTITUTO**			
	FASE 02:	Gestión de valoración	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GV01:	Identificación de Activos	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Identificar los activos con los que cuentan los institutos			

ACTIVO	**SOFTWARE**				
CÓDIGO	**NOMBRE**	**DESCRIPCIÓN**	**ESTADO**	**UBICACIÓN**	**RESPONSABLE**
SO_01	Sistema operativo	Windows 10	Operativo	Lab_01	Coordinador académico
SO_02	..	..			
…	…	…	…	..	…
ACTIVO	**HARDWARE**				

CÓDIGO	NOMBRE	DESCRIPCIÓN	ESTADO	UBICACIÓN	RESPONSABLE
HW_01	Teclado	Genius S/M	Operativo	Lab_01	Coordinador académico
HW_02	…	….			
HW_03	…	….	..		…
ACTIVO	SERVICIO				
CÓDIGO	NOMBRE	DESCRIPCIÓN	ESTADO	UBICACIÓN	RESPONSABLE
SE_01	Mantenimiento preventivo	Para evitar pérdidas de información y de procesos	Operativo	Diferentes ambiente	Responsable de TI
SE_02	…	…	..	..	..
SE_03	….	…	..	..	..
RESPONSABLE	ELABORADO		REVISADO		APROBADO
NOMBRE	Nombre completo del responsable de la creación de plantilla		Nombre Completo del responsable de la revisión de la plantilla		Nombre completo del responsable de la aprobación de la plantilla
FECHA					
FIRMA					

Proceso GV02: Gestión de valoración de activos de TI

Los activos de TI se evaluarán respecto a la confidencialidad, integridad y disponibilidad, para los procesos de alcance del modelo de gestión de riesgo, para garantizar la continuidad de los servicios.

Para la implementación del presente proceso se debe de tomar en cuenta la fase 01 descripción del contexto en el proceso DC03 definición de alcance y criterios, (ver tabla 11, 12 y 13)

Figura 23: Valoración de activos

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 02:	Gestión de valoración	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GV02:	Gestión de valoración de activos	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Identificar la valoración de los activos de los institutos			

CÓDIGO	**ACTIVOS**	**USO**	**CRITERIO**				**OBSERVACIÓN**
			D	**C**	**I**	**TOTAL**	
VA_SO	Sistemas operativos						
…							
VA_HD	Teclado						
..							
VA_SE	Mantenimiento preventivo						

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA			
FIRMA			

Proceso GV03: Documentación de la fase

Los procesos anteriores deberán de ser debidamente documentados para poder llevar un control, en donde se verificará el estado de los procesos anteriores con la finalidad de poder cerciorarse que todas las actividades propuesta fueron alcanzadas. Para asi

garantizar la continuidad de los procesos y a su vez cumplir con lo requerido que establece el documento de CBC para el licenciamiento.

Para poder alcanzar este proceso se le muestra la siguiente tabla:

TABLA 14: Criterio de Documentación

.

CRITERIO DE DOCUMENTACIÓN	
ID	**ESTADO**
1	Iniciado
2	En proceso
3	Interrumpido
4	Retomado
5	Culminado

Figura 24: Documentación de la fase

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 02:	Gestión de valoración	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GV03:	Documentación de la fase 02	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Contiene el listado de las actividades de los procesos con sus respectivos responsables de la fase 02 y su nivel			
FASE	**ROL Y RESPONSABILIDAD**		**RESPONSABLE**	**ESTADO DE FASE**
FA2_PR01	…		…	…
FA2_PR02	…		…	…
RESPONSABLE	**ELABORADO**		**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla		Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA				
FIRMA				

Fase 03: Gestión de riesgos

Proceso GR01: Gestionar los activos en riesgos

En este proceso se inicia con el reconocimiento de los escenarios de riesgos a los que pueden estar expuestos los activos de los institutos. El propósito principal es que los institutos deben de reconocer y conservar conocimiento de los escenarios de riesgo notables según sus necesidades y sus elementos de riesgos reconocidos. Para el desarrollo de este proceso se toma como referencia a COBIT asociándolo junto con las CBC para el procesamiento de licenciamiento. Las que se listan en la tabla 15.

TABLA 15: Escenarios de riesgos

ESCENARIOS DE RIESGOS	
N°	**ESCENARIO**
01	Toma de decisiones sobre inversiones en TI
02	Administración de ciclo de vida de programas
03	Incidentes de infraestructura operativa de TI
04	Problemas en la adopción y uso de software
05	Incidentes de hardware
06	Fallas en el software
07	Ataques lógicos (hacking, malware, etc.)
08	Innovación basada en tecnología
09	Administración de datos e información
10	…

Una vez listado los posibles escenarios de riesgos a los que los institutos pueden estar expuestos. Se calcula el impacto y la probabilidad de que se materialice el escenario de riesgo, para ello se utilizara de la fase 01 definición de alcance y criterios, específicamente las figuras 14, 15 y 16, como se propone en el siguiente formato:

Figura 25: Análisis de escenarios de riesgos

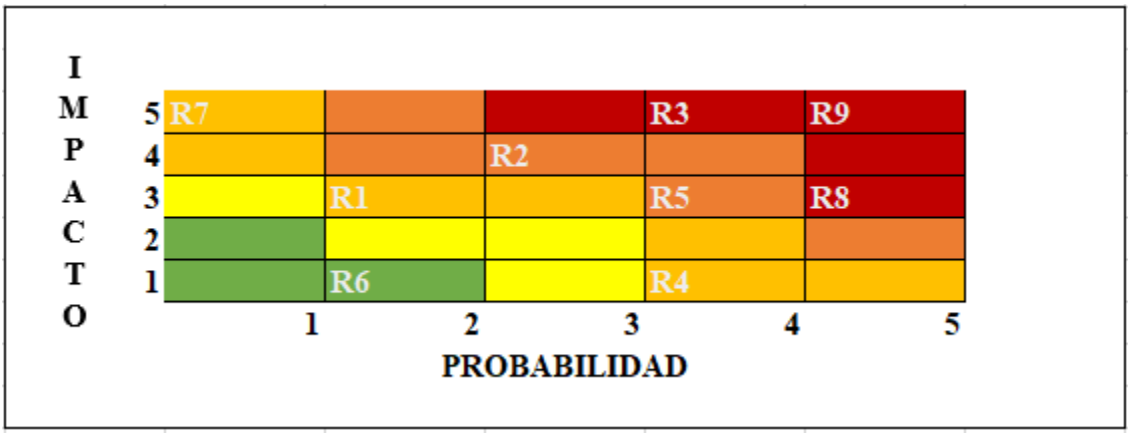
LOGO DE INSTITUTO		NOMBRE DEL INSTITUTO					
		FASE 03:	**Gestión de riesgos**	FECHA DE ELABORACIÓN			__/__/____
		PROCESO GR01:	**Gestionar los activos en riesgos**	FECHA DE APLICACIÓN			__/__/____
OBJETIVO:		Identificar, evaluar y reducir periódicamente los riesgos relacionados con TI de los institutos					
CÓDIGO	**ACTIVO**	**ESCENARIO**		**ANÁLISIS**			
		AMENAZA	**VULNERABILIDAD**	**IMPACTO (1-5)**	**PROBABILIDAD (1-5)**	**I*P**	**RIESGO**
GR01_01: Toma de decisiones no planificadas en inversiones de TI	**VA_HD17, VA_HD22, …**	Acceso no autorizado	Seguridad de la red	**3**	**5**	**15**	**R001**
GR01_02: . .	**VA_SO1, VA_SO5**	…	...	**5**	**5**	**25**	**R002**
. . .	. . .	. . .	. . .	.	.	.	. . .
.	.	.	.	.	.	.	.
RESPONSABLE		**ELABORADO**	**REVISADO**		**APROBADO**		
NOMBRE		Nombre completo del responsable de la creación de la plantilla	Nombre completo del responsable de la revisión de la plantilla		Nombre Completo del responsable de la aprobación de la plantilla		
FECHA							
FIRMA							

Proceso GR02: Monitorear el comportamiento de la gestión de activos.

El proceso evalúa la importancia de cada riesgo en términos de su impacto potencial en los procesos y servicios críticos y a su vez determinar el nivel de riesgo que los institutos están conscientes a aceptar. Lo que conlleva a realizar la siguiente actividad.

Ubicación del riesgo: en esta actividad se utiliza la fase 01, proceso definición de alcance y criterios de riesgo específicamente la figura 18, que servirá para posicionar el riesgo que se identificó en el proceso anterior según su probabilidad e impacto, la cual les permite a los institutos, poder reconocer cuáles son los riesgos de mayor prioridad que se debe de controlar, para evitar que se materialice y a su vez evitar un impacto en sus procesos.

Figura 26: Ubicación de riesgos



Proceso GR03: Medición de la gestión de activos

El proceso consiste en monitorear la efectividad de la gestión de activos y revisar periódicamente las prácticas de gestión de riesgos para garantizar que permanezcan alineados con los objetivos y el contexto cambiante de los institutos. Para este proceso se utilizará la figura 17 criterio de aceptabilidad donde los resultados obtenidos en el proceso anterior se comparan con el apetito y tolerancia que tiene los institutos.

Para tal medición se usará la siguiente tabla donde:

- P: Es la probabilidad
- I: Es el impacto
- A: Es el apetito de riesgo
- T: Es la tolerancia

Tabla 16: Medición de activos

CONDICIÓN	VALORACIÓN
P*I < A	Aceptable
P*I <= A	Aceptable
P*I > A y P*I <= T	No aceptable
P*I >A y P*I >= T	No aceptable
P*I > T	No aceptable

Figura 27: Medición de la gestión de activos

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO							
	FASE 03:	Gestión de riesgos		FECHA DE ELABORACIÓN			__/__/____	
	PROCESO GR03:	Medición de la gestión de activos		FECHA DE APLICACIÓN			__/__/____	
OBJETIVO	Valorar los riesgos identificados a través del impacto y la probabilidad para ver si el instituto aceptan o no el riesgo							
ACTIVO	**ESCENARIO**			**ANÁLISIS**				
	AMENAZA	**VULNERABILIDAD**		**IMPACTO (1-5)**	**PROBABILIDAD (1-5)**	**I*P**	**RIESGO**	**VALOR**
GR01_01: Toma de decisiones no planificadas en inversiones de TI	Acceso no autorizado	Seguridad de la red		**3**	**5**	**15**	**R001**	No Aceptable
	…	…		.	.	.	.	.
GR01_02 . .	…	…		.	.	.		.
	…	…		.	.	.	.	.
	…	…		.	.	.	.	.
. .	…	…		.	.	.	.	.
	…	…		.	.	.	.	.
		…		.	.	.	.	.
RESPONSABLE	**ELABORADO**		**REVISADO**		**APROBADO**			
NOMBRE	Nombre completo del responsable de la creación de la plantilla		Nombre completo del responsable de la revisión de la plantilla		Nombre Completo del responsable de la aprobación de la plantilla			
FECHA								
FIRMA								

Proceso GR04: Plan de gestión de riesgos

Este proceso se enfoca en la elaboración de un plan de gestión de riesgos para determinar una estrategia de respuesta, de acuerdo a los resultados de los riesgos obtenidos en el proceso anterior.

Actividad 01 Tratamiento de riesgos: busca medir el impacto del tratamiento del riesgo, donde se tiene que seleccionar una respuesta para un determinado riesgo, y decidir si está listo para ser aceptado por los institutos o de lo contrario si se debe de aplicar una nueva respuesta o un cambio en la estrategia. Para ello nos basaremos en algunas estrategias de COBIT para riesgos:

- **Evitar:** esto implica eliminar el riesgo al no participar en la actividad que crea el riesgo.
- **Mitigar:** esto implica tomar medidas para reducir la probabilidad o el impacto de un riesgo.
- **Compartir o transferir:** esto implica trasferir el riesgo a agentes externos de acuerdo a la naturaleza del objeto de estudio.
- **Aceptar:** implica aceptar el riesgo sin emprender ninguna acción para mitigarlo, esto puede ser apropiado para riesgos que tienen un impacto relativamente bajo o el costo de mitigar el riesgo es mayor que el impacto potencial.

Para el cumplimiento de esta actividad se propone la siguiente tabla:

Figura 28: Tratamiento de riesgo:

LOGO DE INSTITUTO	**NOMBRE DE INSTITUTO**							
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN	__/__/____				
	PROCESO GR04:	Plan de gestión de riesgos.	FECHA DE APLICACIÓN	__/__/____				
OBJETIVO	Tratar los riesgos identificados para que las organizaciones tomen la decisión de aceptar o no el riesgo							
ACTIVO	**ESCENARIO**		**ANÁLISIS**					
	Amenaza	**Vulnerabilidad**	**IMPACTO**	**PROBABILIDAD**	**I*P**	**RIESGO**	**Valor**	**Tratamiento**
GR01_01 Toma de decisiones no planificadas en inversiones de TI	Acceso no autorizado	Seguridad de la red	**3**	**5**	**15**	**R001**	No Aceptable	Mitigar
	…	…	**3**	**5**	**15**	**R002**	No Aceptable	Mitigar
GR01_02	…	…	.	.	.	.	…	…
.	…	…	.	.	.	.	…	…
	…	…	.	.	.	.	…	…
.	…	…	.	.	.	.	…	…
.	…	…	.	.	.	.	…	…
.	…	…	.	.	.	.	…	…
.	…	…	.	.	.	.	…	…
RESPONSABLE	**ELABORADO**		**REVISADO**			**APROBADO**		
NOMBRE	Nombre completo del responsable de la creación de la plantilla		Nombre completo del responsable de la revisión de la plantilla			Nombre Completo del responsable de la aprobación de la plantilla		
FECHA								
FIRMA								

Actividad 02: Establecer plan de gestión de riesgos: Se debe de implantar un procedimiento de acción una vez identificado los tratamientos de riesgos que se aplicarán para disminuir el impacto de los riesgos. El cual consiste en controlar el cumplimiento de las actividades propuestas anteriormente para poder dar continuidad a los procesos.

Figura 29: Establecer plan de gestión de riesgos

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO				
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN	___/___/___	
	PROCESO GR04:	Establecer plan de gestión de riesgos	FECHA DE APLICACIÓN	___/___/___	
OBJETIVO	Contiene el listado de las actividades del plan de acción a realizar				
CÓDIGO	**NOMBRE DEL PROYECTO**	**RESPONSABLE**	**TIEMPO**	**OBSERVACIONES**	**ESTADO**
Código del plan	Nombre del plan	Nombre de responsable	Tiempo de ejecución	Listado de observaciones	Estado del plan
…	…	…	…	…	…
…	…	…	…	…	…
…	…	…	…	…	…
RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**		
NOMBRE	Nombre completo del responsable de la creación de plantilla	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla		
FECHA					
FIRMA					

Proceso GR05: Documentación de la fase

Consiste en una actividad permanente que tiene como finalidad registrar la información asociada con el desarrollo de los procesos anteriores. El objetivo es que los institutos cuenten con información de sus procesos realizados y que sirva como base de conocimiento sobre la gestión de riesgos de TI que se realiza, generando un procedimiento más adecuado que pueda ser recordado y repetido por los colaboradores.

Figura 30: documentación de la fase 03

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GR05:	Documentación de la fase 03	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Contiene el listado de las actividades de los procesos con sus respectivos responsables de la fase 03 y su estado de la fase			
FASE	**ROL Y RESPONSABILIDAD**		**RESPONSABLE**	**ESTADO DE FASE**
FA3_PR01				
FA3_PR02				

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA			
FIRMA			

Fase 04: Gestión de revisión y mejora continua

En esta fase se gestiona y mejora el reconocimiento y ejecución de mejoras en los sistemas y procesos de TI de las organizaciones para optimizar su eficacia, eficiencia y alineación de sus procesos organizacionales. Es decir, esta fase se encarga de revisar y perfeccionar periódicamente las actividades de administración de riesgos de una organización para garantizar que sigan siendo eficaces para abordar los riesgos actuales y emergentes.

Proceso GM01: Revisión de gestión de riesgos

Consiste en realizar un seguimiento del proceso de gestión de riesgos para garantizar de que siga siendo efectivo; es decir que los institutos tienen que realizar un monitoreo continuo de los diferentes procesos. Para esta actividad se puede utilizar la tabla 14 en donde se puede especificar el estado de cada fase.

Figura 31: Revisión de gestión de riesgos

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO					
	FASE 04:	Gestión de Revisión y mejora continua	FECHA DE ELABORACIÓN	___/___/___		
	PROCESO GM01:	Revisión de Gestión de Riesgos	FECHA DE APLICACIÓN	___/___/___		
OBJETIVO	Contiene el listado de los procesos de gestión de riesgo con sus respectivos responsables de la fase 01,sus fecha de inicio y fin y su estado					
CÓDIGO	**PROCESO**		**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**ESTADO**
…	Estrategia para mitigar los riesgos		Encargado de aplicar la estrategia	Fecha de inicio de estrategia	Fecha fin donde temrina la estrategia	Culminado
…	…		….	….	….	….
RESPONSABLE	**ELABORADO**			**REVISADO**		**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla			Nombre Completo del responsable de la revisión de la plantilla		Nombre completo del responsable de la aprobación de la plantilla
FECHA						
FIRMA						

Proceso GM02: Comunicación de Resultados

Proceso de comunicar de forma segura información sobre riesgos y actividades de gestión de riesgos a los segmentos interesados relevantes dentro de los institutos. El objetivo de la comunicación de resultados es asegurar que las partes interesadas de los institutos estén informadas sobre las tareas de administración de riesgos y a su vez proporcionarles la información que necesitan para tomar decisiones.

En conclusión, la comunicación eficaz de los resultados es esencial para una gestión de riesgos exitosa.

Para el desarrollo de este proceso se propone la siguiente tabla:

Figura 32: Comunicación de resultados

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 04:	Gestión de revisión y mejora continua	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GM02:	Comunicación de resultados	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Comunicar información sobre riesgos y actividades a partes interesadas dentro de los institutos			
CÓDIGO	**PROCESO**	**ACTIVIDAD**	**RESPONSABLE**	**RESULTADOS Y OBSERVACIONES**
…	Procesos realizados	Actividades que se realizaron	Nombre de la persona a cargo del proceso	Se describe los resultados obtenidos después de la ejecución del proceso
…				
RESPONSABLE	**ELABORADO**		**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla		Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA				
FIRMA				

Proceso GM03: Incorporación de nuevas sugerencias

Este proceso se basa en considerar e integrar nuevas ideas y sugerencias técnicas sobre la tecnología en actividades de gestión de riesgos de los institutos. Esto implica buscar activamente comentarios o sugerencias de los segmentos interesados y evaluarlas para establecer si se pueden incorporar a las actividades de gestión, para mejorar los procesos organizacionales.

Para el desarrollo de este proceso se propone la siguiente tabla:

Figura 33: Incorporación de nuevas sugerencias

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 04:	Gestión de revisión y mejora continua	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GM03:	Incorporación de nuevas sugerencias	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Obtener nuevas ideas o sugerencias para la mejora de gestión de riesgos en los institutos			
CÓDIGO	**NUEVAS SUGERENCIAS**	**ACTIVIDAD**	**RESPONSABLE**	**DESCRIPCIÓN**
…	Procesos realizados	Actividades que se realizaron	Nombre de la persona a cargo del proceso	Se describe los resultados obtenidos después de la ejecución del proceso
…	…	…	…	…
RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**	
NOMBRE	Nombre completo del responsable de la creación de plantilla	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla	
FECHA				
FIRMA				

Proceso GM04: Documentación de la fase

El proceso de documentación de cada fase es esencial para garantizar que el proceso sea integral, coherente y eficaz. Para facilitar la mejora y el refinamiento continuo del enfoque de gestión de riesgos.

Se documenta toda la información relacionada con los riesgos y las medidas que se generan en cada actividad de la gestión de riesgos asi como su estado.

Figura 34: Documentación de fase 04

LOGO DE INSTITUTO	NOMBRE DEL INSTITUTO			
	FASE 04:	Gestión de revisión y mejora continua	FECHA DE ELABORACIÓN	___/___/___
	PROCESO GM04:	Documentación de la fase 04	FECHA DE APLICACIÓN	___/___/___
OBJETIVO	Contiene el listado de las actividades de los procesos con sus respectivos responsables de la fase 04 y su estado de la fase			
FASE	**ROL Y RESPONSABILIDAD**		**RESPONSABLE**	**ESTADO DE FASE**
FA4_PR01				
FA4_PR02				

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Nombre completo del responsable de la creación de plantilla	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA			
FIRMA			

3.5. Validez del modelo a través de juicio de expertos

El modelo propuesto se sometió a una evaluación por juicios de expertos para demostrar su validez y aplicabilidad, teniendo como jurado a 03 profesionales con una amplia experiencia en la gestión de riesgos.

Tabla 17: Listado de expertos que validaron el modelo

N°	APELLIDOS Y NOMBRES	EXPERIENCIA
1	MBA.MG. Lomparte Alvarado Rómulo	30 años
2	MBA.MG. Dávila Ramírez Juan	28 años
3	MG. Rodríguez Castro Jorge Martín	20 años

Se presentó un formato para la validación de expertos del modelo propuesto (Ver anexo 6) con la finalidad de obtener la opinión y retroalimentación de cada jurado especialista respecto a la suficiencia, claridad, coherencia y relevancia de cada uno de las fases y sus respectivos procesos contempladas en el modelo.

Por parte de algunos expertos se recibió algunas observaciones, las cuales se tomaron en cuenta y se levantaron dichas observaciones para que el modelo alcance la validez necesaria para su aprobación y aplicación.

Para la validación del modelo se aplicó el coeficiente V de Aiken, donde se debe de obtener un valor entre 0.8 y 1

Aplicando la herramienta Excel para la evaluación de cada uno de los criterios considerados en el juicio de expertos, se obtuvieron los siguientes resultados:

Figura 35: Resultado de V de Aiken

MGR-TI		Experto 01				Experto 02				Experto 03				TOTAL			
Fase	Proceso	SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE
I	DC01	1	1	1	1	0.3	1	1	1	1	1	1	1	0.78	0.89	0.89	0.89
	DC02	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
	DC03	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
	DC04	1	1	1	1	0.3	0.3	0.3	0.3	1	1	1	1	0.78	0.78	0.78	0.78
	DC05	1	1	1	1	1	1	1	1	1	1	1	1	0.78	0.78	0.89	0.89
II	GV01	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
	GV02	1	1	1	1	0.3	0.3	0.3	0.3	1	1	1	1	0.78	0.78	0.78	0.78
	GV03	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
III	GR01	1	1	1	1	0.3	0.3	0.3	0.3	1	1	1	1	0.78	0.78	0.78	0.78
	GR02	1	1	1	1	0.3	0.3	0.3	0.3	1	1	1	1	0.78	0.78	0.78	0.78
	GR03	1	1	1	1	0.3	0.3	0.3	0.3	1	1	1	1	0.78	0.67	0.67	0.78
	GR04	1	1	1	1	0.3	0.3	0.3	0.3	1	1	1	1	0.78	0.78	0.78	0.78
	GR05	1	1	1	1	1	1	1	1	1	1	1	1	0.78	0.78	0.89	0.89
IV	GM01	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
	GM02	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
	GM03	1	1	1	1	1	1	1	1	1	1	1	1	0.89	0.89	0.89	0.89
	GM04	1	1	1	1	1	1	1	1	1	1	1	1	0.78	0.78	0.89	0.89
V de Aiken por cada criterio														0.824	0.8235	0.843	0.85
V de Aiken de MGR-TI														0.83			

De acuerdo a los resultados obtenidos, mostro que todos los criterios presentaron valores superiores al 0.8, lo que concluye la concordancia entre jueces, validando el modelo y su aplicabilidad.

3.6. Implementación del modelo de gestión de riesgos de TI para garantizar la continuidad del servicio en los procesos organizacionales

Se planteó la implementación del modelo propuesto en el Instituto De Educación Superior Tecnológico Público Chognoyape a fin de aplicar cada uno de las fases con sus respectivos procesos, demostrando que el modelo se puede aplicar en el entorno real.

Fase 01 Descripción del contexto

Proceso DC01: Contexto Interno

Se establece el contexto interno del instituto para identificar y mejorar las estrategias de la institución, en donde se evalúo las metas institucionales con las que el instituto cuenta, las cuales se describen en el PEI institucional, los incidentes involucrados con el área de TI como pérdida de datos, errores en los procesos, manejo indebido de la tecnología,

equipamiento de cómputo inferior a lo requerido e historial de incidentes no registrados, tal como se muestra en la figura 36.

Figura 36: Resultados de contexto interno

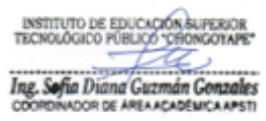
	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 01:	**Descripción del contexto**	FECHA DE ELABORACIÓN	20/11/2023
	Proceso DC01 :	**Contexto Interno**	FECHA DE APLICACIÓN	20/11/2023
OBJETIVO:	Descripción del contexto interno de la institución para poder mejorar las estrategias institucionales.			
ESTRUCTURA INSTITUCIONAL				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
EI_01	Organigrama Institucional		Es necesario tener definido el organigrama de la institución	
METAS INSTITUCIONALES				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
MI_01	Proyecto educativo institucional (PEI)		-Plan Anual de Trabajo (PAT) -Proyecto Curricular (PCI) -Reglamento Interno (RI)	
INCIDENTES RELACIONADOS CON TI				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
IR_01	Incidentes vinculados con TI		-Pérdida de datos (Notas de exámenes de recuperación, actas de validación de notas) -Error en los procesos. (Ya que al no tener un plan se desarrolla de manera empírica) -Manejo indebido de la tecnología -Equipamiento de cómputo indebido -Historial de incidentes no documentada	
RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**	
NOMBRE	Jefferson James Milián Saavedra	Coordinadora de APSTI.	Directora del instituto.	
FECHA	20/11/2023	20/11/2023	20/11/2023	
FIRMA				

De acuerdo a lo analizado en esta lista de cotejo, los hallazgos nos permiten recomendar:

- Actualizar el PEI con estrategias innovadoras que permitan el desarrollo de la organización.
- Planes con base en una metodología acorde a la naturaleza de la institución para definir los procesos y lineamientos requeridos.

Proceso DC02:Contexto Externo Se establece el contexto externo para poder identificar y prevenir las amenazas a las que se encuentra expuesta el instituto, para este proceso se analizan datos obtenidos del INEI como son las características socioeconómicas de los apoderados o padres de familia (C, D y E), tambien se identifican los marcos normativos que rigen a los institutos los cuales son brindados por el MINEDU y GRE, a su vez se analiza las nuevas tecnologías que están disponibles para la mejora de sus procesos, como por ejemplo herramientas de google, fibra óptica, herramientas de protección por ataques cibernéticos, entre otros. Ver más detalles en la figura 37.

Figura 37: Resultados del contexto externo

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 01:	**Descripción del contexto**	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO DC02:	**Contexto Externo**	FECHA DE APLICACIÓN	21/11/2023
OBJETIVO:	Descripción del contexto externo de la institución para poder prevenir las amenazas a la que están expuestas			
CULTURA				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
CU_01	Datos de INEI		Personas que se encuentran socioeconómicamente en las características promedio del jefe de hogar en: C, D y E (Considera a las personas que tienen solo secundaria completa y que no tienen un trabajo estable)	
POLÍTICA				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
PO_01	MINEDU Y GRE		Marco normativo que deben de cumplir las instituciones La institución no cumple con la documentación adecuada	
TECNOLÓGICO				
CODIGO	**ESTRUCTURA**		**DESCRIPCIÓN**	
TE_01	Publicaciones de nuevas tecnologías		Herramientas de Google Cableado tradicional Continuas incidencias de ataques por falta de protección contra ataques cibernéticos. Soporte Tecnológico de forma local	
RESPONSABLE	**ELABORADO**		**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra		Coordinadora de APSTI	Directora del instituto
FECHA	20/11/2023		21/11/2023	21/11/2023
FIRMA					

Proceso DC03: Definición de alcance y criterios de riesgo

En esta fase se necesita los criterios de disponibilidad, confidencialidad e integridad para poder identificar, evaluar las amenazas y los requerimientos de seguridad, las cuales fueron definidas en la propuesta del presente modelo (ver tabla 11,12 y13); se debe de tener en cuenta que 1 es el valor más bajo y 5 el valor más crítico.

Criterios de riesgo:

Los criterios de riesgos que se utilizan se encuentran definidos en el presente modelo:

Paso 1: Criterio de Probabilidad, En este paso se define los criterios y se les asigna una numeración de acuerdo a la ocurrencia que se distribuye por 5 escenarios (ver figura 14)

Paso 2: Criterio de Impacto, Se definen los criterios de impacto, los mismos que se encuentran en la documentación del modelo (Ver figura 15), donde encontramos los escenarios de impacto que se clasifican de a acuerdo a, si son significativos o no para los logros de los objetivos del instituto.

Paso 3: Análisis de Riesgos, Para el análisis de riesgos se estableció en el modelo (Ver figura 16) la forma de cómo se debe valorar el riesgo a través de la probabilidad por el impacto que pueda ocasionar y de acuerdo a la gravedad se diferencia por un determinado color.

Paso 4: criterio de aceptabilidad, el equipo de TI del instituto de educación superior tecnológico público Chongoyape estableció sus indicadores de riesgo, tales como su apetito (muy bajo) y su tolerancia (Bajo).

El siguiente paso es realizar el análisis de la probabilidad por el impacto para poder determinar su nivel de aceptabilidad (ver figura 17)

Una vez que ya se tiene el punto anterior se procede a elaborar el mapa de calor que está definido en el modelo (Ver figura 18)

Proceso DC04: Definición de roles y responsabilidades, Se implementa la definición de roles y responsabilidad dentro del instituto, donde se identifican las siguientes: dirección general con el rol de Director teniendo como responsable a la directora del

instituto, unidad académica teniendo como rol de Responsable y como agente responsable a jefa de unidad académica, secretario académico con el rol de Ejecutor teniendo como responsable al secretario académico y coordinador de arquitectura de plataformas y servicios de tecnologías de información (APSTI) con el rol de Supervisor teniendo como responsable al coordinador de APSTI. (Ver figura 38)

Figura 38: Resultado de la definición de roles y responsabilidades

<table>
<tr><td rowspan="2"></td><td colspan="4">INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE</td></tr>
<tr><td>FASE 01:</td><td>Descripción del contexto</td><td>FECHA DE ELABORACIÓN</td><td>20/11/2023</td></tr>
<tr><td>PROCESO DC04:</td><td>Definición de Roles y responsabilidades</td><td>FECHA DE APLICACIÓN</td><td>22/11/2023</td></tr>
<tr><td>OBJETIVO</td><td colspan="4">Contiene la matriz de roles y responsabilidades del personal involucrado en los diferentes procesos de los institutos: Director (D), Responsable (R), Supervisor (S), Ejecutor (E), Informado (I)</td></tr>
<tr><td>CÓDIGO</td><td colspan="2">ROL Y RESPONSABILIDAD</td><td colspan="2">RESPONSABLE</td></tr>
<tr><td>01</td><td>D</td><td>Dirección general</td><td colspan="2">Directora del instituto</td></tr>
<tr><td>02</td><td>R</td><td>Unidad Académica</td><td colspan="2">Jefa de unidad academia</td></tr>
<tr><td>03</td><td>E</td><td>Secretario Académico</td><td colspan="2">Secretario del instituto</td></tr>
<tr><td>04</td><td>S</td><td>Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información</td><td colspan="2">Coordinadora de APSTI</td></tr>
<tr><td>RESPONSABLE</td><td colspan="2">ELABORADO</td><td>REVISADO</td><td>APROBADO</td></tr>
<tr><td>NOMBRE</td><td colspan="2">Jefferson James Milián Saavedra</td><td>Coordinadora de APSTI</td><td>Directora del instituto</td></tr>
<tr><td>FECHA</td><td colspan="2">20/11/2023</td><td>22/11/2023</td><td>22/11/2023</td></tr>
<tr><td>FIRMA</td><td colspan="2"></td><td>INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO "CHONGOYAPE"
Ing. Sofia Diana Guzmán Gonzales
COORDINADOR DE AREA ACADÉMICA APSTI</td><td>INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO "CHONGOYAPE"
Lic. Maria Jhenny Mendoza Copia
DIRECTORA GENERAL (e)</td></tr>
</table>

Proceso DC05: Documentación de la fase: Es importante documentar la fase al terminar de aplicarla con la finalidad de poder llevar el control y a la vez tener un registro de aplicación de los procesos. En este proceso queda registrado la aplicación de cada fase con su responsable y el estado de la fase: para la fase DC01 se definió como

responsable a la directora del instituto y como estado de la fase culminado, teniendo como recomendación actualizar la documentación.

Para la fase DC02 y DC03 se definió como responsable al coordinador de APSTI y como estado culminado. Para la fase DC04 se estableció como responsable a la directora del instituto y como estado culminada. (Ver figura 39)

Figura 39: Resultado de la documentación de la fase descripción del contexto

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 01:	**Descripción del contexto**	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO DC05:	**Documentación de la fase 01**	FECHA DE APLICACIÓN	22/11/2023
OBJETIVO	Contiene la matriz de roles y responsabilidades de los procesos con sus respectivos responsables de la fase 01			
FASE	**ROL Y RESPONSABILIDAD**		**RESPONSABLE**	**ESTADO DE FASE**
DC01	Director		Directora del instituto	Culminada, pero con recomendaciones de actualización de documentación
DC02	Responsable		Coordinador de APSTI	Culminada
DC03	Responsable		Coordinador de APSTI	Culminada
DC04	Director		Directora del instituto	Culminada
RESPONSABLE	**ELABORADO**	**REVISADO**		**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinadora de APSTI		Directora del instituto
FECHA	20/11/2023	22/11/2023		22/11/2023
FIRMA				

Fase 02: Gestión de valoración

En esta fase se especifican los procesos necesarios que el instituto debe cumplir según la CBC de licenciamiento, tambien se identifican activos del área de TI con el que cuenta el instituto.

Proceso GV01 Identificación de activos: Para este proceso se inicia con la identificación de los procesos que el instituto debe de cumplir, los cuales se encuentran normados en la CBC de licenciamiento en donde se encontró que para la CBC-I gestión institucional cuentan con todos los procesos; sin embargo, para el proceso de gestión estratégica, registro de información académica, bienestar estudiantil y seguimiento al egresado se les recomienda actualizar y mejorar los procesos.

Para la CBC-II gestión académica y programa de estudios pertinentes, cumple con los procesos de gestión académica y pertinencia de los programas de estudios, pero para el proceso de gestión de investigación se registró que no cumple dicho proceso, por tal motivo se le recomienda al instituto que implemente la gestión de investigación.

Para la CBC-III infraestructura física, cumple con el proceso de disponibilidad de infraestructura y equipamiento, asi como el proceso de disponibilidad de servicios básicos como son telefonía e internet, pero se le recomienda mejorar ambos procesos porque presentan algunas dificultades como bajo rendimiento, escasa disponibilidad, etc. Por otra parte, no cumple con el proceso de disponibilidad de recursos o material bibliográfico, por lo que se le recomienda implementar este proceso para una mejor calidad de servicio.

Para la CBC-IV previsión económica y financiera compatible con los fines, si cumple el proceso, teniendo en cuenta que el instituto es del estado el cual genera sus recursos propios limitados.

Es necesario aclarar que no todos los procesos de la CBC se tomaron en cuenta para la aplicación del modelo debido que algunos procesos no concordaban con el caso de estudio. Ver Figura 40.

Figura 40: Resultado de verificación de procesos según la CBC

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 02:	**Gestión de valoración**	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GV01:	**Identificación de procesos**	FECHA DE APLICACIÓN	22/11/2023
OBJETIVO	Identificar con cuáles de los procesos de CBC del licenciamiento, cuentan los institutos			

Área		Responsable		
Código	**Proceso**	**Respuesta**		**Observación**
		Si	**No**	
CBC-I	**Gestión institucional**			
	Gestión estratégica	X		Se le recomienda Actualizar
	Estructura organizativa	X		
	Régimen académico	X		
	Registro de información académica	X		Se le recomienda mejorar este proceso
	Bienestar estudiantil	X		Se le recomienda mejorar este proceso
	Seguimiento al egresado	X		Se le recomienda implementar mejoras
CBC-II	**Gestión académica y programas de estudios pertinentes**			
	Gestión académica	X		
	Pertinencia de los programas de estudios	X		
	Gestión de investigación		X	Se le recomienda implementar la investigación
CBC-III	**Infraestructura Física**			
	Disponibilidad de infraestructura y equipamiento	X		Se le recomienda mejorar este proceso
	Disponibilidad de recurso o materiales bibliográficos		X	Se le recomienda implementar material bibliográfico
	Disponibilidad de servicios básicos, telefonía e internet	X		Se le recomienda mejorar estos servicios básicos
CBC-IV	**Previsión económica y financiera compatible con los fines**			
	Provisión económica y financiera	X		Se debe de tener en cuenta que por ser una institución del estado, genera sus propios recursos limitados.

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinadora de APSTI	Directora del instituto
FECHA	20/11/2023	22/11/2023	22/11/2023
FIRMA			

Una vez identificados los procesos en el paso anterior ahora se procede a identificar los activos de IESTP Chongoyape en donde se encontró activos software los cuales no tienen licencias tanto los sistemas operativos como los aplicativos.

Los activos hardware se encontraron en buen estado operativos, pero aun no cumplen con los requerimientos exactos de la CBC como son algunos de ellos procesador i7, 16 de memora RAM, etc.

Para los activos de servicios se encontraron con mantenimiento preventivo, servicio de internet, portal web, correo electrónico, los cuales funcionan con normalidad, teniendo la única dificultad el rendimiento del internet debido a la ubicación geográfica. (Ver Figura 41)

Figura 41: Resultado de la identificación de activos

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE				
	FASE 02:	**Gestión de valoración**	FECHA DE ELABORACIÓN	20/11/2023	
	PROCESO GV01:	**Identificación de Activos**	FECHA DE APLICACIÓN	23/11/2023	
OBJETIVO	Identificar los activos con los que cuenta el instituto				
ACTIVO	**SOFTWARE**				
CÓDIGO	**NOMBRE**	**DESCRIPCIÓN**	**ESTADO**	**UBICACIÓN**	**RESPONSABLE**
SO_01	Sistema operativo	Windows 8.1 Pro	Operativo sin licencia	Lab_01	Coordinador académico
SO_02	Sistema operativo	Windows 10 Education	Operativo sin licencia	Lab_01	Coordinador académico
SO_03	Sistema Operativo	Windows 10 Pro	Operativo sin licencia	Lab_01	Coordinador académico
SO_04	Sistema Operativo	Windows 10 Education	Operativo sin licencia	Lab_02	Coordinador académico
SO_05	Sistema Operativo	Windows 10 Pro	Operativo sin licencia	Lab_02	Coordinador académico
SO_06	Sistema Operativo	Windows 11 Pro	Operativo sin licencia	Lab_02	Coordinador académico

ACTIVO	HARDWARE				
CODIGO	**NOMBRE**	**DESCRIPCIÓN**	**ESTADO**	**UBICACIÓN**	**RESPONSABLE**
HW_01	Case	Cybertel: Disco duro de 500 GB, RAM 4 GB, Procesador Intel core i3	Operativo	Lab_01	Coordinador académico
HW_02	Monitor	AOC	Operativo	Lab_01	Coordinador académico
HW_03	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_04	Case	Cybertel: Disco duro 500 GB, Ram de 4 GB, Procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_05	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_06	Teclado y mouse	Enkore Access y genius	Operativo	Lab_01	Coordinador académico
HW_07	Case	Cybertel: Disco duro 500 GB, RAM 4 GB, procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_08	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_09	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_10	Case	Cybertel: Disco duro 500 GB, RAM 4 GB, procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_11	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_12	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_13	Case	Halion: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i7	Operativo	Lab_01	Coordinador académico
HW_14	Monitor	Samsung	Operativo	Lab_01	Coordinador académico

HW_133	Teclado y mouse	Halion	Operativo	Lab_03	Coordinador académico
HW_134	Switch	Satra 16-port 10/100 MBps Fast Ethernet switch	Operativo	Lab_03	Coordinador académico
HW_135	Switch	D-Link Des-1016D 10/100 MBps Fast Ethernet switch	Operativo	Lab_03	Coordinador académico
HW_136	Switch	TP-Link TL-SF1016D 16 port 10/100 MBps desktop switch	Operativo	Lab_03	Coordinador académico
ACTIVO	**SERVICIO**				
CODIGO	**NOMBRE**	**DESCRIPCIÓN**	**ESTADO**	**UBICACIÓN**	**RESPONSABLE**
SE_01	Mantenimiento preventivo	Para evitar pérdidas de información y de procesos	Operativo	Diferentes ambiente	Coordinador académico
SE_02	Servicio de internet	El servicio de internet que se adquiere a un proveedor	Operativo	Jefatura	Coordinador académico
SE_03	Portal Web	Página institucional al servicio de la comunidad estudiantil	Operativo	Jefatura	Coordinador académico
SE_03	Correo Electrónico	Correo institucional para los estudiantes, administrativos y docentes	Operativo	Jefatura	Coordinador académico

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	23/11/2023	23/11/2023
FIRMA			

La siguiente figura es un resumen de todo el proceso, para observar la información con más detalles ver Anexo 06.

Proceso GV02: Gestión de valoración de activos de TI: Se procede a la valoración de los activos del instituto de acuerdo a lo establecido en el proceso de definición de alcance y criterios de riesgo, disponibilidad, confidencialidad e integridad (Ver tabla 11, 12 y 13), en donde cada activo se le asignó un valor entre 1 y 5 obteniendo una suma total de los tres criterios (Ver figura 42)

Figura 42: Resultado de la gestión de valoración de los activos de TI

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 02:	**Gestión de valoración**	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GV02:	**Gestión de valoración de activos**	FECHA DE APLICACIÓN	23/11/2023
OBJETIVO	Identificar la valoración de los activos del instituto			

CÓDIGO	**ACTIVOS**	**USO**	**CRITERIO**				**OBSERVACIÓN**
			D	**C**	**I**	**TOTAL**	
VA_SO1	Sistemas operativo Windows 8.1 Pro	X	3	1	2	6	No cuenta con licencias
VA_SO2	Sistema operativo Windows 10 Education	X	4	2	3	9	No cuenta con licencias
VA_SO3	Sistema Operativo Windows 10 Pro	X	4	2	3	9	No cuenta con licencias
VA_SO4	Sistema Operativo Windows 11Pro	X	4	2	3	9	No cuenta con licencias
VA_SO5	Paquete Office 2016	X	4	2	3	9	No cuenta con licencias
VA_SO6	Paquete Office 2019	X	4	2	3	9	No cuenta con licencias
VA_SO7	Paquete Office 2021	X	4	2	3	9	No cuenta con licencias
VA_SO8	Página Web Institucional	X	5	5	5	15	
VA_SO9	Aplicativo Correo Institucional	X	5	5	5	15	
VA_SO10	Sistema Registra	X	5	5	5	15	
VA_HD1	Case- Cybertel: Disco duro de 500 GB, RAM 4 GB, Procesador Intel core i3	X	3	3	3	9	Tiende a reiniciarse solo, debido a la antigüedad
VA_HD2	Monitor AOC	X	4	3	3	10	

VA_HD3	Teclado y mouse Enkore Access	X	4	4	4	12	
VA_HD4	Monitor Samsung	X	4	4	4	12	
VA_HD5	Monitor LG	X	4	4	4	12	
VA_HD6	Case Halion: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i7	X	3	3	3	9	Se le recomienda Actualizar su SO
VA_HD7	Teclado y mouse Genius	X	5	4	4	13	
VA_HD8	Case HP: Disco duro 250 GB, RAM 4 GB, procesador Intel Core 2 duo	X	3	3	3	9	Tiende a reiniciarse solo, debido a la antigüedad
VA_HD9	Monitor HP	X	3	4	4	11	
VA_HD10	Monitor Dell	X	2	4	4	10	
VA_HD11	Teclado y mouse Halion	X	5	4	4	13	
VA_HD12	Teclado y mouse Enkore Access	X	5	4	4	13	
VA_HD13	Case Halion: Disco duro 1 TB, RAM 4 GB, procesador AMD R5	X	4	4	4	12	Se le recomienda aumentar memora RAM
VA_HD14	Case Ecotrend: Disco duro 500 GB, RAM 4 GB, procesador AMD	X	3	3	3	9	Se le recomienda aumentar memora RAM
VA_HD15	Case Micronics: Disco duro 500 GB, RAM 4 GB, RAM 4 GB	X	3	3	3	9	Tiende a reiniciarse solo, debido a la antigüedad
VA_HD16	Tecla do y mouse Logitech	X	4	4	4	12	
VA_HD17	Switch Encore ENH916-NWY-16 port nway switch	X	4	4	4	12	Se le recomienda actualizar, con la finalidad de aumentar más puertos
VA_HD18	Case HP: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i5	X	4	4	4	12	
VA_HD19	Case Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	X	5	4	4	13	

VA_HD20	Case Teros: Disco duro 500 GB, RAM 8GB, procesador Intel Core i5	X	5	4	4	13	
VA_HD21	Case Teros: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i5	X	5	4	4	13	
VA_HD22	Switch Satra 16-port 10/100 MBps Fast Ethernet switch	X	4	4	4	12	Se le recomienda actualizar, con la finalidad de aumentar más puertos
VA_HD23	Switch D-Link Des-1016D 10/100 MBps Fast Ethernet switch	X	4	4	4	12	Se le recomienda actualizar, con la finalidad de aumentar más puertos
VA_HD24	Switch TP-Link TL-SF1016D 16 port 10/100 MBps desktop switch	X	4	4	4	12	Se le recomienda actualizar, con la finalidad de aumentar más puertos
VA_SE1	Mantenimiento preventivo	X	4	5	4	13	
VA_SE2	Servicio de internet	X	2	3	2	7	
VA_SE3	Portal Web	X	3	4	5	12	
VA_SE4	Correo Electrónico	X	5	4	5	14	

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de ASPTI	Directora del instituto
FECHA	20/11/2023	23/11/2023	23/11/2023
FIRMA			

Proceso GV03: Documentación de la fase: Se procede a documentar la fase para llevar un control de cumplimento de todos los procesos en donde se especifican el rol y la responsabilidad de cada proceso, el cual le corresponde al coordinador de ASPTI, asi tambien el estado (ver tabla 14) de cada proceso que se encuentra en culminada. (Ver figura 43)

Figura 43: Resultado de documentación de la fase de gestión de valoración

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 02:	**Gestión de valoración**	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GV03:	**Documentación de la fase 02**	FECHA DE APLICACIÓN	23/11/2023
OBJETIVO	Contiene el listado de las actividades de los procesos con sus respectivos responsables de la fase 02 y su nivel			

FASE	**ROL Y RESPONSABILIDAD**	**RESPONSABLE**	**ESTADO DE FASE**
FA2_GV01	Responsable	Coordinador de APSTI	Culminada
FA2_GV02	Responsable	Coordinador de APSTI	Culminada

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	23/11/2023	23/11/2023
FIRMA			

Fase 03: Gestión de riesgos

Proceso 1: Gestionar los activos en riesgos: En este proceso se inicia con el reconocimiento de los escenarios de riesgos a los que pueden estar expuestos el instituto, para ello se tomó los escenarios establecidos en el modelo, dando como resultado que cinco de los escenarios propuestos tienen riesgos con un impacto y una probabilidad muy alta y solo tres de ellos tienen riesgos con un impacto intermedio. (Ver figura 44)

Figura 44: Resultados de gestionar los activos de riesgos

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE						
	FASE 03:	**Gestión de riesgos**		FECHA DE ELABORACIÓN			20/11/2023
	PROCESO GR01:	**Gestionar los activos en riesgos**		FECHA DE APLICACIÓN			23/11/2023
OBJETIVO:	Identificar, evaluar y reducir periódicamente los riesgos relacionados con TI de los institutos						
CÓDIGO	**ACTIVO**	**ESCENARIO**		**ANÁLISIS**			
		AMENAZA	**VULNERABILIDAD**	**IMPACTO (1-5)**	**PROBABILIDAD (1-5)**	**I*P**	**RIESGO**
GR01_01: Toma de decisiones no planificadas en inversiones de TI	**VA_HD17, VA_HD22, VA_HD23, VA_HD24, VA_SE3, VA_SE4**	Acceso no autorizado, por la carencia de inversión en protección de hardware y software de la organización.	Seguridad de la red	**3**	**5**	**15**	**R001**
	VA_HD1, VA_HD3, VA_HD6, VA_HD8, VA_HD13, VA_HD14, VA_HD5, VA_HD16, VA_HD17, VA_HD18, VA_HD19, VA_HD20, VA_HD22, VA_HD23, VA_HD24, VA_SE1	Fallo de hardware	Tiempo de inactividad del sistema	**3**	**5**	**15**	**R002**
GR01_02: Incidencias	**VA_HD17, VA_HD22, VA_HD23, VA_HD24, VA_SE1**	Interrupción de conectividad	Respaldo de red no diseñada	**5**	**5**	**25**	**R003**
	VA_SO1, VA_SO5, VA_HD17, VA_HD22, VA_HD23, VA_HD24,	Errores humanos	Capacitación del personal insuficiente	**3**	**3**	**9**	**R004**

Operativas en la infraestructura de TI	**VA_SE1, VA_SE3. VA_SE4**						
	VA_SO1, VA_SO5,	Software desfasado	Actualizaciones de software no periódicas.	**5**	**5**	**25**	**R005**
	VA_SO1, VA_SO5, VA_HD17, VA_HD22, VA_HD23, VA_HD24, VA_SE1, VA_SE3. VA_SE4	Interrupciones prolongadas	Inexistente plan de continuidad del negocio	**5**	**5**	**25**	**R006**
GR01_03: Problemas en la adopción y uso de software	**VA_SO1, VA_SO2, VA_SO05**	Fallos del sistema por corrupción de datos	Problemas de compatibilidad	**5**	**5**	**25**	**R007**
	VA_SO1, VA_SO2, VA_SO05, VA_SE1	Retardos en la asistencia para problemas técnicos.	Soporte de usuario insuficiente	**3**	**3**	**9**	**R008**
	VA_SO1, VA_SO2, VA_SO05, VA_SE3, VA_SE4	Dificultad para solucionar problemas por la carencia en la actualización de conocimiento.	Documentación inadecuada	**3**	**5**	**15**	**R009**
GR01_04: Incidentes de hardware	**VA_HD1, VA_HD3, VA_HD8, VA_HD9, VA_HD10, VA_HD13, VA_HD14, VA_HD15, VA_HD17, VA_HD18, VA_HD19, VA_HD20, VA_HD21, VA_HD22, VA_HD23, VA_HD24, VA_SE1**	Equipo obsoleto o sin soporte	Hardware obsoleto	**5**	**5**	**25**	**R010**
	VA_HD1, VA_HD3, VA_HD8, VA_HD9, VA_HD10, VA_HD13, VA_HD14, VA_HD15, VA_HD17, VA_HD18, VA_HD19, VA_HD20, VA_HD21, VA_HD22, VA_HD23, VA_HD24, VA_SE1	Mal funcionamiento del equipamiento de TI	Fallo de hardware	**5**	**5**	**25**	**R011**
GR01_05:	**VA_SO1, VA_SO2, VA_SO5, VA_SO8, VA_SO9, VA_SO10**	Conflictos de compatibilidad, inestabilidad del sistema.	Problemas de incompatibilidad	**3**	**3**	**9**	**R012**

Fallas en el Software	**VA_SO1, VA_SO2, VA_SO5, VA_SO8, VA_SO9, VA_SO10**	Dificultad en la resolución de problemas, respuesta retrasada a incidentes del sistema	Registro y auditoría inadecuados	**3**	**5**	**15**	**R013**
	VA_SO1, VA_SO2, VA_SO5, VA_SO8, VA_SO9, VA_SO10	Ataques de inyección que generan la corrupción de datos.	Falta de validación de entrada	**5**	**5**	**25**	**R014**
GR01_06: Ataques lógicos	**VA_SO1, VA_SO8, VA_SO9, VA_SO10**	Cracking de contraseñas, robo de credenciales	Contraseñas débiles o reutilizadas	**5**	**5**	**25**	**R015**
	VA_SO1, VA_SO8, VA_SO9, VA_SO10	Seguridad de cuenta débiles	No se aplica la autenticación multifactor	**5**	**5**	**25**	**R016**
GR01_07: Innovación basada en tecnología	**VA_HD1, VA_HD3, VA_HD4, VA_HD5, VA_HD6, VA_HD8, VA_HD9, VA_HD10, VA_HD13, VA_HD14, VA_HD15, VA_HD17, VS_HD18, VA_HD19, VA_HD20, VA_HD21, VA_HD22, VA_HD23, VA_HD24**	Actualizaciones en periodos cortos de la tecnología en el sector que deja obsoleta la actualización.	Obsolescencia tecnológica	**5**	**3**	**15**	**R017**
	VA_HD1, VA_HD3, VA_HD4, VA_HD5, VA_HD6, VA_HD8, VA_HD9, VA_HD10, VA_HD13, VA_HD14, VA_HD15, VA_HD17, VS_HD18, VA_HD19, VA_HD20, VA_HD21, VA_HD22, VA_HD23, VA_HD24, VA_SE1	Incompatibilidad o dificultades para integrar la innovación con los sistemas existentes.	Desafíos de integración	**5**	**3**	**15**	**R018**
	VA_HD1, VA_HD3, VA_HD4, VA_HD5, VA_HD6, VA_HD8, VA_HD9, VA_HD10, VA_HD13, VA_HD14, VA_HD15, VA_HD17, VS_HD18, VA_HD19, VA_HD20, VA_HD21,	Incumplimiento de las regulaciones y estándares de la industria.	Cumplimiento normativo	**5**	**5**	**25**	**R019**

	VA_HD22, VA_HD23, VA_HD24, VA_SE1						
	VA_HD1, VA_HD3, VA_HD4, VA_HD5, VA_HD6, VA_HD8, VA_HD9, VA_HD10, VA_HD13, VA_HD14, VA_HD15, VA_HD17, VS_HD18, VA_HD19, VA_HD20, VA_HD21, VA_HD22, VA_HD23, VA_HD24, VA_SE1	Falta de aceptación o adopción por las partes interesadas	Resistencia al cambio	4	5	20	R020
GR01_08: Administración de datos e información	VA_SO1, VA_SO8, VA_SO9, VA_SO10, VA_HD17, VA_HD22, VA_HD23, VA_HD24	Pérdida de datos por tiempo de inactividad prolongada	Copia de seguridad y recuperación insuficientes	5	5	25	R021
	VA_SO8, VA_SO9, VA_SO10	Mal uso o mal manejo de datos sensibles	Falta de clasificación y etiquetado de datos.	4	5	20	R022
	VA_SO8, VA_SO9, VA_SO10, VA_SE2	Datos inexactos o incompletos	Mala gestión de la calidad de los datos	3	5	15	R023
	VA_SO1, VA_SO8, VA_SO9, VA_SO10, VA_HD17, VA_HD22, VA_HD23, VA_HD24, VA_SE2, VA_SE3, VA_SE4	Intercepción de datos por manipulación	Transmisión de datos insegura	5	5	25	R024

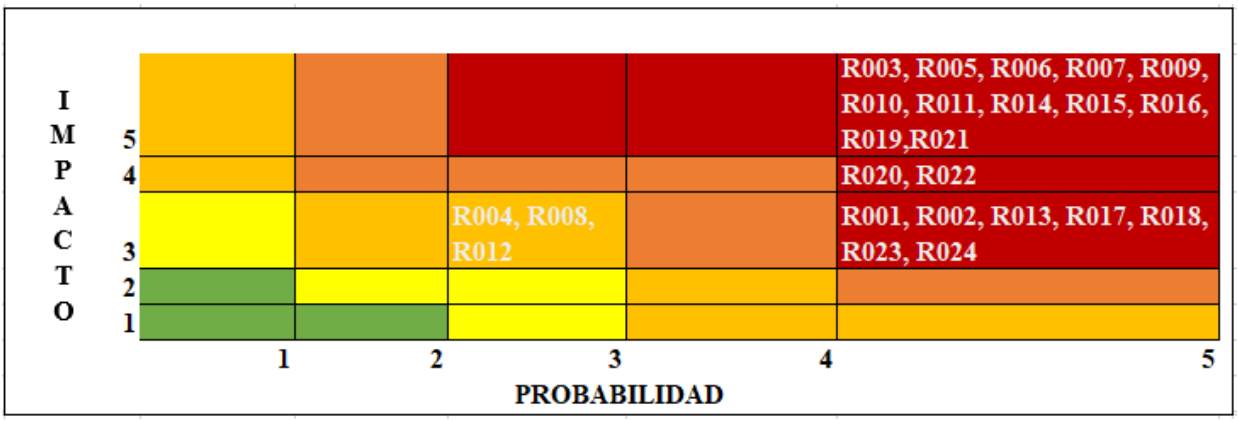
RESPONSABLE	ELABORADO	REVISADO	APROBADO
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	23/11/2023	23/11/2023
FIRMA			

Proceso 02: Monitorear el comportamiento de la gestión de activos

En este proceso se monitorea los riesgos del instituto por su impacto potencial en sus procesos y servicios, tambien se determina los niveles de riesgo que puede asumir la institución.

Ubicación del riesgo: Esta actividad consiste en la ubicación de cada riesgo en el mapa de calor, lo que permitió al instituto identificar los riesgos prioritarios a los que debe de tratar para que no se materialice los riesgos mencionados en la figura 44, resultando solo tres riesgos con una prioridad intermedia de atención (Ver figura 45)

Figura 45: Resultado de ubicación de riesgo



Proceso GR03: Medición de la gestión de activos

En este proceso es donde el instituto toma la decisión del que hacer con respecto a los riesgos de acuerdo a su ubicación en el mapa de calor, en donde se tomó la decisión de no aceptar ningún riesgo para los escenarios propuestos, debido a que los riesgos están ubicados en una posición elevada, lo que indica que el riesgo puede materializarse. (Ver figura 46)

Figura 46: Resultado de medición de gestión de activos

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE						
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN	20/11/2023			
	PROCESO GR03:	Medición de la gestión de activos	FECHA DE APLICACIÓN	05/12/2023			
OBJETIVO	Valorar los riesgos identificados a través del impacto y la probabilidad para ver si el instituto aceptan o no el riesgo						
ACTIVO	**ESCENARIO**		**ANÁLISIS**				
	AMENAZA	**VULNERABILIDAD**	**IMPACTO (1-5)**	**PROBABILIDAD (1-5)**	**I*P**	**RIESGO**	**VALOR**
GR01_01: Toma de decisiones no planificadas en inversiones de TI	Acceso no autorizado	Seguridad de la red	**3**	**5**	**15**	**R001**	No Aceptable
	Fallo de hardware	Tiempo de inactividad del sistema	**3**	**5**	**15**	**R002**	No Aceptable
GR01_02 Incidencias Operativas en la infraestructura de TI	Interrupción de conectividad	Falta de respaldo de red	**5**	**5**	**25**	**R003**	No Aceptable
	Errores humanos	Falta de capacitación del personal	**3**	**3**	**9**	**R004**	No Aceptable
	Software desfasado	Falta de actualizaciones de software	**5**	**5**	**25**	**R005**	No Aceptable
	Interrupciones prolongadas	Falta de plan de continuidad del negocio	**5**	**5**	**25**	**R006**	No Aceptable
GR01_03	Fallos del sistema, corrupción de datos	Problemas de compatibilidad	**5**	**5**	**25**	**R007**	No Aceptable
	Falta de asistencia para problemas técnicos.	Soporte de usuario insuficiente	**3**	**3**	**9**	**R008**	No Aceptable

Problemas en la adopción y uso de software	Dificultad para solucionar problemas, falta de conocimiento.	Documentación inadecuada	**3**	**5**	**15**	**R009**	No Aceptable
GR01_04 Incidentes de hardware	Equipo obsoleto o sin soporte	Hardware envejecido	**5**	**5**	**25**	**R010**	No Aceptable
	Mal funcionamiento del componente	Fallo de hardware	**5**	**5**	**25**	**R011**	No Aceptable
GR01_05 Fallas en el Software	Conflictos de compatibilidad, inestabilidad del sistema.	Problemas de incompatibilidad	**3**	**3**	**9**	**R012**	No Aceptable
	Dificultad en la resolución de problemas, respuesta retrasada a incidentes	Registro y auditoría inadecuados	**3**	**5**	**15**	**R013**	No Aceptable
	Ataques de inyección, corrupción de datos.	Falta de validación de entrada	**5**	**5**	**25**	**R014**	No Aceptable
GR01_06 Ataques lógicos	Cracking de contraseñas, robo de credenciales	Contraseñas débiles o reutilizadas	**5**	**5**	**25**	**R015**	No Aceptable
	Seguridad de cuenta débiles	Falta de autenticación multifactor	**5**	**5**	**25**	**R016**	No Aceptable
GR01_07 Innovación basada en tecnología	Avances rápidos que hacen que la innovación quede obsoleta	Obsolescencia tecnológica	**5**	**3**	**15**	**R017**	No Aceptable
	Incompatibilidad o dificultades para integrar la innovación con los sistemas existentes.	Desafíos de integración	**5**	**3**	**15**	**R018**	No Aceptable
	Incumplimiento de las regulaciones y estándares de la industria.	Cumplimiento normativo	**5**	**5**	**25**	**R019**	No Aceptable
	Falta de aceptación o adopción por parte de las partes interesadas	Resistencia al cambio	**4**	**5**	**20**	**R020**	No Aceptable

GR01_08 Administración de datos e información	Pérdida de datos, tiempo de inactividad prolongado	Copia de seguridad y recuperación insuficientes	**5**	**5**	**25**	**R021**	No Aceptable
	Mal uso o mal manejo de datos sensibles	Falta de clasificación y etiquetado de datos.	**4**	**5**	**20**	**R022**	No Aceptable
	Datos inexactos o incompletos	Mala gestión de la calidad de los datos	**3**	**5**	**15**	**R023**	No Aceptable
	Intercepción de datos, manipulación	Transmisión de datos insegura	**5**	**5**	**25**	**R024**	No Aceptable

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del isntituto
FECHA	20/11/2023	05/12/2023	05/12/2023
FIRMA			

Proceso GR04: Plan de gestión de riesgos

Actividad 01 Tratamiento de riesgos: En este punto es donde el instituto toma la decisión de mitigar todos los riesgos de acuerdo a los resultados obtenidos y según la aplicación de las estrategias de COBIT (Ver figura 47)

Figura 47: Resultados de tratamiento de riesgos

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE							
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN				20/11/2023	
	PROCESO GR04:	Plan de gestión de riesgos.	FECHA DE APLICACIÓN				05/12/2023	
OBJETIVO	Tratar los riesgos identificados para que las organizaciones tomen la decisión de aceptar o no el riesgo							
ACTIVO	**ESCENARIO**		**ANÁLISIS**					
	Amenaza	**Vulnerabilidad**	**IMPACTO**	**PROBABILIDAD**	**I*P**	**RIESGO**	**Valor**	**Tratamiento**
GR01_01 Toma de decisiones no planificadas en inversiones de TI	Acceso no autorizado	Seguridad de la red	**3**	**5**	**15**	**R001**	No Aceptable	Mitigar
	Fallo de hardware	Tiempo de inactividad del sistema	**3**	**5**	**15**	**R002**	No Aceptable	Mitigar
GR01_02 Incidencias Operativas en la infraestructura de TI	Interrupción de conectividad	Falta de respaldo de red	**5**	**5**	**25**	**R003**	No Aceptable	Mitigar
	Errores humanos	Falta de capacitación del personal	**3**	**3**	**9**	**R004**	No Aceptable	Mitigar
	Software desfasado	Falta de actualizaciones de software	**5**	**5**	**25**	**R005**	No Aceptable	Mitigar
	Interrupciones prolongadas	Falta de plan de continuidad del negocio	**5**	**5**	**25**	**R006**	No Aceptable	Mitigar

GR01_03 Problemas en la adopción y uso de software	Fallos del sistema, corrupción de datos	Problemas de compatibilidad	**5**	**5**	**25**	**R007**	No Aceptable	Mitigar
	Falta de asistencia para problemas técnicos.	Soporte de usuario insuficiente	**3**	**3**	**9**	**R008**	No Aceptable	Mitigar
	Dificultad para solucionar problemas, falta de conocimiento.	Documentación inadecuada	**3**	**5**	**15**	**R009**	No Aceptable	Mitigar
GR01_04 Incidentes de hardware	Equipo obsoleto o sin soporte	Hardware envejecido	**5**	**5**	**25**	**R010**	No Aceptable	Mitigar
	Mal funcionamiento del componente	Fallo de hardware	**5**	**5**	**25**	**R011**	No Aceptable	Mitigar
GR01_05 Fallas en el Software	Conflictos de compatibilidad, inestabilidad del sistema.	Problemas de incompatibilidad	**3**	**3**	**9**	**R012**	No Aceptable	Mitigar
	Dificultad en la resolución de problemas, respuesta retrasada a incidentes	Registro y auditoría inadecuados	**3**	**5**	**15**	**R013**	No Aceptable	Mitigar
	Ataques de inyección, corrupción de datos.	Falta de validación de entrada	**5**	**5**	**25**	**R014**	No Aceptable	Mitigar
GR01_06 Ataques lógicos	Cracking de contraseñas, robo de credenciales	Contraseñas débiles o reutilizadas	**5**	**5**	**25**	**R015**	No Aceptable	Mitigar
	Seguridad de cuenta débiles	Falta de autenticación multifactor	**5**	**5**	**25**	**R016**	No Aceptable	Mitigar
GR01_07	Avances rápidos que hacen que la innovación quede obsoleta	Obsolescencia tecnológica	**5**	**3**	**15**	**R017**	No Aceptable	Mitigar
	Incompatibilidad o dificultades para integrar la innovación con los sistemas existentes.	Desafíos de integración	**5**	**3**	**15**	**R018**	No Aceptable	Mitigar

Innovación basada en tecnología	Incumplimiento de las regulaciones y estándares de la industria.	Cumplimiento normativo	**5**	**5**	**25**	**R019**	No Aceptable	Mitigar
	Falta de aceptación o adopción por parte de las partes interesadas	Resistencia al cambio	**4**	**5**	**20**	**R020**	No Aceptable	Mitigar
GR01_08 Administración de datos e información	Pérdida de datos, tiempo de inactividad prolongado	Copia de seguridad y recuperación insuficientes	**5**	**5**	**25**	**R021**	No Aceptable	Mitigar
	Mal uso o mal manejo de datos sensibles	Falta de clasificación y etiquetado de datos.	**4**	**5**	**20**	**R022**	No Aceptable	Mitigar
	Datos inexactos o incompletos	Mala gestión de la calidad de los datos	**3**	**5**	**15**	**R023**	No Aceptable	Mitigar
	Intercepción de datos, manipulación	Transmisión de datos insegura	**5**	**5**	**25**	**R024**	No Aceptable	Mitigar

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	05/12/2023	05/12/2023
FIRMA			

Actividad 02: Establecer plan de gestión de riesgos: En esta actividad se elabora un plan de acción en donde se establece responsables, actividad y tiempo de duración de actividad para cada escenario de riesgo con la finalidad de disminuir el impacto de los riesgos.

Se establecieron ocho planes de gestión de riesgo uno para cada escenario de riesgo, capacitación en mejora de la toma de dicciones sobre inversiones de TI, realizar un registro de incidentes de infraestructura operativa de TI, capacitación en la adopción y uso de software, registro de incidentes de hardware, registro de fallas en el software, actualización sobre seguridad de ataques lógicos, plan de innovación basada en tecnología e implementación de mejoras en la administración de datos e información de los cuales todos se encuentran en la fase de iniciados. (Ver figura 48)

Figura 48: Resultado de establecimiento de plan de gestión de riesgos

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE					
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN	20/11/2023		
	PROCESO GR04:	Establecer plan de gestión de riesgos	FECHA DE APLICACIÓN	05/12/2023		
OBJETIVO	Contiene el listado de las actividades del plan de acción a realizar					
CÓDIGO	**NOMBRE DEL PROYECTO**	**RESPONSABLE**	**TIEMPO**	**OBSERVACIONES**	**ESTADO**	
GR04_01	Capacitación en mejora de la toma de decisiones sobre inversiones de TI	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	5 Días	Las capacitaciones sobre toma de decisiones siempre deben de estar presentes en los institutos	Iniciado	
GR04_02	Realizar un registro de incidentes de infraestructura operativa de TI	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	10 Días	Esta parte es importante para tener en cuenta los incidentes de infraestructura que ocurrieron en TI	Iniciado	

GR04_03	Capacitación en la adopción y uso de software	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	5 Días	Se tiene que capacitar tanto al responsable, como a todo el equipo de TI	Iniciado
GR04_04	Registro de Incidentes de hardware	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	5 Días	Es importante tener el registro de los incidentes de hardware	Iniciado
GR04_05	Registro de Fallas en el software	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	5 Días	Es importante tener el registro de fallas de software	Iniciado
GR04_06	Actualización sobre seguridad de Ataques lógicos	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	5 Días	Es importante estar actualizado en los nuevos ataques lógicos para poder tomar medidas de precaución	Iniciado
GR04_07	Plan de Innovación basada en tecnologia	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	20 Días	Es muy importante tener un plan de innovación tecnológica	Iniciado
GR04_08	Implementación de mejoras en la administración de datos e información	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	30 Días	La implementación de mejores de administración de datos e información siempre debe de estar presente en los institutos	Iniciado

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Nombre Completo del responsable de la revisión de la plantilla	Nombre completo del responsable de la aprobación de la plantilla
FECHA	20/11/2023	05/12/2023	05/12/2023
FIRMA			

Proceso GR05: Documentación de la fase

En esta fase de registra las actividades desarrolladas en las anteriores faces, indicando el estado de las fases para poder guardar un registro de aplicación. Indicando que 3 fases ya se culminaron y solo queda pendiente la última fase (Ver figura 49)

Figura 49: Resultado de la documentación de la fase 03

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 03:	Gestión de riesgos	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GR05:	Documentación de la fase 03	FECHA DE APLICACIÓN	05/12/2023
OBJETIVO	Contiene el listado de las actividades de los procesos con sus respectivos responsables de la fase 03 y su estado de la fase			

FASE	ROL Y RESPONSABILIDAD	RESPONSABLE	ESTADO DE FASE
FA3_GR01	Responsable	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	Culminado
FA3_GR02	Responsable	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	Culminado
FA3_GR03	Responsable	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	Culminado
FA3_GR04	Responsable	Coordinador del área de Arquitectura de plataformas y servicios de tecnologías de la información	Iniciado

RESPONSABLE	ELABORADO	REVISADO	APROBADO
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	05/12/2023	05/12/2023
FIRMA			

Fase 04: Gestión de revisión y mejora continua

Esta fase se realiza la mejora continua de los procesos de administración de riesgos, detectados en el instituto.

Proceso GM01: Revisión de gestión de riesgos

Se realiza el seguimiento al proceso de gestión de riesgos detectados en el instituto, este proceso se tiene que realizar de manera continua, en donde se obtiene como resultado que los primeros seis procesos del plan de gestión de riesgos ya fueron ejecutados teniendo como estado culminado; mientras los dos últimos planes que son plan de innovación basada en tecnología e implementación de mejora en la administración de datos informáticos tienen su estado en progreso, lo que quiere decir que aún se están ejecutando dichos planes debido al periodo de receso de la institución. (Ver figura 50)

Figura 50: Resultado de revisión de gestión de riesgos

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE				
	FASE 04:	Gestión de Revisión y mejora continua	FECHA DE ELABORACIÓN	20/11/2023	
	PROCESO GM01:	Revisión de Gestión de Riesgos	FECHA DE APLICACIÓN	11/12/2023	
OBJETIVO	Contiene el listado de los procesos de gestión de riesgo con sus respectivos responsables de la fase, sus fecha de inicio y fin y su estado				
CÓDIGO	**PROCESO**	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**ESTADO**
GM01_01	Capacitación en mejora de la toma de decisiones sobre inversiones de TI	Coordinador de APSTI	05/12/2023	10/12/223	Culminado
GM01_02	Realizar un registro de incidentes de infraestructura operativa de TI	Coordinador de ASPTI	05/12/2023	15/12/2023	Culminado
GM01_03	Capacitación en la adopción y uso de software	Coordinador de APSTI	05/12/2023	10/12/2023	Culminado
GM01_04	Registro de Incidentes de hardware	Coordinadora de APSTI	05/12/2023	10/12/2023	Culminado
GM01_05	Registro de Fallas en el software	Coordinador de ASPSTI	05/12/2023	10/12/2023	Culminado
GM01_06	Actualización sobre seguridad de Ataques lógicos	Coordinador de APSTI	05/12/2023	10/12/2023	Culminado
GM01_07	Plan de Innovación basada en tecnología	Coordinador de APSTI	05/12/2023	10/12/2023	En proceso
GM01_08	Implementación de mejoras en la administración de datos e información	Coordinador de ASPTI	05/12/2023	05/01/2024	En proceso
RESPONSABLE	**ELABORADO**	**REVISADO**		**APROBADO**	
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI		Directora del instituto	
FECHA	20/11/2023	11/12/2023		11/12/2023	
FIRMA					

Proceso GM02: Comunicación de Resultados

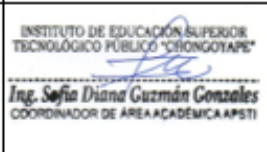
En este proceso se comunica la información de los riesgos y actividades de gestión de riesgos a las autoridades interesadas dentro del instituto, para asegurar que estén informados sobre las tareas de administración de riesgos.

Donde se informó que los 6 primeros procesos se realizaron con éxito, mitigando los riesgos identificados en los procesos anteriores; por otro lado, se informó que los dos últimos procesos aún están en implementación. (Ver figura 51)

Figura 51: Resultados de la fase de comunicación

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 04:	Gestión de revisión y mejora continua	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GM02:	Comunicación de resultados	FECHA DE APLICACIÓN	12/12/2023
OBJETIVO	Comunicar información sobre riesgos y actividades a partes interesadas dentro de los institutos			
CÓDIGO	**PROCESO**	**ACTIVIDAD**	**RESPONSABLE**	**RESULTADOS Y OBSERVACIONES**
GM02_01	Toma de decisiones no planificadas en inversiones de TI	Capacitación en mejora de la toma de decisiones sobre inversiones de TI	Coordinador de APSTI	Se realizó con éxito la capacitación, dando como resultado una mejora en la toma de decisiones sobre inversiones de TI
GM02_02	Incidencias Operativas en la infraestructura de TI	Realizar un registro de incidentes de infraestructura operativa de TI	Coordinador de APSTI	Se realizó el registro de incidentes para un tratamiento adecuado
GM02_03	Problemas en la adopción y uso de software	Capacitación en la adopción y uso de software	Coordinador de APSTI	Se realizó la capacitación de adopción, mejorando aceptación y uso de software
GM02_04	Incidentes de hardware	Registro de Incidentes de hardware	Coordinador de APSTI	Se realizó el registro de incidentes, para un mejor control y tratamiento
GM02_05	Fallas en el software	Registro de Fallas en el software	Coordinador de APSTI	Se realizó el registro de fallas, para tener un historial y poder

				realizar comparaciones futuras.
GM02_06	Ataques lógicos.	Actualización sobre seguridad de Ataques lógicos.	Coordinador de ASPTI	Se realizó la actualización, con la finalidad de mitigar los posibles ataques a los que está expuesto el instituto.
GM02_07	Innovación basada en tecnología.	Plan de Innovación basada en tecnología.	Coordinador de APSTI	Se sigue implementando el plan.
GM02_08	Administración de datos e información.	Implementación de mejoras en la administración de datos e información.	Coordinador de APSTI	Se continua con la implementación de mejoras en la administración de datos.

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de ASPTI	Directora del instituto
FECHA	20/11/2023	12/12/2023	12/12/2023
FIRMA			

Proceso GM03: Incorporación de nuevas sugerencias

Este proceso se encarga de incorporar nuevas sugerencias sobre la gestión de riesgos de parte de los interesados en las actividades del instituto. Como nueva sugerencia se tomó al proceso de transformación digital, el cual está establecido por el ministerio de educación. Se le asignó una actividad y un responsable. (Ver figura 52)

Figura 52: Resultado de incorporación de nuevas sugerencias

	INSTITUTO DE EDUCACION SUPERIOR TECNOLOGICO PUBLICO CHONGOYAPE			
	FASE 04:	Gestión de revisión y mejora continua	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GM03:	Incorporación de nuevas sugerencias	FECHA DE APLICACIÓN	13/12/2023
OBJETIVO	Obtener nuevas ideas o sugerencias para la mejora de gestión de riesgos en el instituto			
CODIGO	**NUEVAS SUGERENCIAS**	**ACTIVIDAD**	**RESPONSABLE**	**DESCRIPCION**
GM03_01	Actualizar el PEI con estrategias innovadoras que permitan el desarrollo de la organización.	Elaboración de plan de actualización del PEI institucional.	Coordinador de APSTI	Se le plantea la actualización del plan del PEI con el fin de mejorar los procesos organizacionales.
GM03_02	Nuevos planes con base en una metodología acorde a la naturaleza de la institución para definir los procesos y lineamientos requeridos.	Estudio y elaboración de planes metodológicos para definición de procesos y lineamientos requeridos.	Coordinador de APSTI	Con los estudios y la elaboración de planes metodológicos se busca mejorar los procesos y lineamientos que requiere la institución.
GM03_03	Mejorar la gestión estratégica.	Elaboración de plan de mejora de gestión estratégica e implementar el proceso de bienestar estudiantil y seguimiento al egresado	Coordinador de APSTI	La mejora estratégica ayudara a mejorar los procesos institucionales.
GM03_04	Mejorar el registro de información académica.	Establecer un plan de registro de información académica.	Coordinador de APSTI	El plan de registro busca tener la información disponible y evitar pérdidas de datos.
GM03_05	Mejorar la estructura y equipamiento.	Establecer un plan de mejora	Coordinador de APSTI	El plan de equipamiento tiene que estar

		de equipamiento.		alineado con las CBC para poder cumplir con los requerimientos como son procesador de pc i7, RAM de 16, etc.
GM03_06	Mejorar la disponibilidad de servicios básicos, telefonía e internet.	Realizar un plan de mejora de conectividad.	Coordinador de APSTI	Se le recomienda la Fibra óptica y la computación en la nube.
GM03_07	Transformación digital para el periodo 2023-2025 del ministerio de educación.	Elaboración Plan de Transformación digital.	Coordinador de APSTI	Se plantea iniciar el proceso de transformación digital a través de la elaboración de un plan.

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	13/12/2023	13/12/2013
FIRMA			

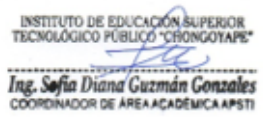
Proceso GM04: Documentación de la fase

Se documenta la información relacionada con las actividades de revisión de gestión de riesgos, comunicación de resultados e incorporación de nuevas sugerencias, verificando el estado de las fases y su responsable, que está representado por el coordinador de APSTI. (Ver Figura 53)

Figura 53: Resultado de documentación de la fase de gestión de revisión y mejora continua

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE			
	FASE 04:	Gestión de revisión y mejora continua	FECHA DE ELABORACIÓN	20/11/2023
	PROCESO GM04:	Documentación de la fase 04	FECHA DE APLICACIÓN	14/12/2023
OBJETIVO	Contiene el listado de las actividades de los procesos con sus respectivos responsables de la fase 04 y su estado de la fase			

FASE	**ROL Y RESPONSABILIDAD**	**RESPONSABLE**	**ESTADO DE FASE**
FA4_GM01	Revisión de Gestión de Riesgos	Coordinador de APSTI	En proceso
FA4_GM02	Comunicación de resultados	Coordinador de APSTI	En proceso
FA4_GM03	Incorporación de nuevas sugerencias	Coordinador de APSTI	En proceso

RESPONSABLE	**ELABORADO**	**REVISADO**	**APROBADO**
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	14/12/2023	14/12/2023
FIRMA			

Luego de haber culminado con la aplicación del modelo, se realizó nuevamente la aplicación del instrumento en forma de POST-TEST, para identificar las mejoras de la gestión de riesgos de TI. Para ello se evaluará las dimensiones gestión de incidentes y gestión de riesgos de TI, con sus respectivos indicadores establecidos en el caso de estudio.

Dimensión 01

- **Indicador 01 número de incidentes**: este indicador muestra información sobre el registro del historial de números de incidentes

Tabla 18: Resultados de indicador 01

COMPARACIÓN DE INDICADOR 01			
INDICADOR	**PRE TEST**	**POST TEST**	**MEJORA**
Número de incidentes	38%	60%	22%

El resultado del pre test para este indicador es de un 38% (ver anexo 05, pregunta 13), evidenciando que no siempre se documentan los incidentes que ocurren durante el desarrollo de sus procesos, lo que afecta en la continuidad del servicio. Por otra parte, el resultado de post test para este indicador es de un 60% (ver anexo 10, pregunta 13), evidenciando una mejora del 22% lo que demuestra que la aplicación del modelo mejora el porcentaje de este indicador, debido a la aplicación de las capacitaciones de las ventajas de realizar registro de incidentes.

- **Indicador 02 tiempo en que se recupera el servicio por incidencias:** este indicador muestra información sobre las mediciones para el monitoreo del servicio.

Tabla: 19: Resultados de indicador 02

COMPARACIÓN DE INDICADOR 02			
INDICADOR	**PRE TEST**	**POST TEST**	**MEJORA**
Tiempo en que se recupera el servicio por incidencia	0%	60%	60%

El resultado del pre test para este indicador es de un 0% (ver anexo 05, pregunta 10), evidenciando que no se ha definido y tampoco implementado medidas para el monitoreo de los servicios, lo que genera un mal funcionamiento del servicio al no tener un seguimiento de verificación de funcionamiento. Por otra parte, el resultado del post test para este indicador es de un 60 % (ver anexo 10, pregunta 11), evidenciando una mejora del 60%, lo que demuestra que la aplicación del modelo mejora el porcentaje de este indicador, debido a la aplicación de las capacitaciones se logró concientizar a los responsables de los procesos sobre el monitorea de los servicios de TI.

- **Indicador 03 Tiempo de respuesta por incidente:** este indicador muestra información sobre la ejecución de control en todos los niveles para implantar las respuestas a los riesgos de TI.

Tabla 20: Resultado de indicador 03

COMPARACIÓN DE INDICADOR 03			
INDICADOR	**PRE TEST**	**POST TEST**	**MEJORA**
Tiempo de respuesta por incidente	38%	60%	22%

El resultado del pre test para este indicador es de un 38% (ver anexo 5, pregunta 12), evidenciando que tiene un índice bajo en el tiempo de respuesta para los incidentes en TI, es decir que ante la presencia de un incidente no se tiene definido el tiempo en que el servicio estará disponible nuevamente, generando deficiencia en sus procesos. Por otra parte, el resultado del post test para este indicador es de 60 % (ver anexo 10, pregunta 12), evidenciando una mejora de 22%, demostrando que la aplicación del modelo mejora el porcentaje de este indicador, luego de las capacitaciones realizadas, los responsables iniciaron las actividades para mejorar el tiempo de respuesta por incidentes, teniendo en cuenta de la importancia de tener a tiempo los servicios disponibles.

Dimensión 02

- **Indicador 01 Identificación de riesgos internos y externos:** este indicador muestra información sobre la determinación de amenazas o vulnerabilidades con impacto potencial sobre las metas o las operaciones de la institución.

Tabla 21: Resultado de indicador 01

COMPARACIÓN DE INDICADOR 03			
INDICADOR	**PRE TEST**	**POST TEST**	**MEJORA**
Identificación de riesgos internos y externos	13%	60%	47%

El resultado del pre test para este indicador es de un 13% (ver anexo 05, pregunta 23), evidenciando que tiene un índice bajo para este indicador, es decir la institución no ha identificado aquellas amenazas y vulnerabilidades que puedan afectar a sus procesos, lo que genera que no se puedan reducir los riesgos ya que no son identificados. Por otra parte, el resultado del post test para este indicador es de 60% (ver anexo 10, pregunta 23), evidenciando una mejora de 47%, demostrando que la aplicación del modelo mejora el porcentaje para este indicador, debido a que luego de las capacitaciones de registros de incidentes, los responsables tomaron conciencia en la importancia de tener el registro de riesgos para poder tener un plan de contingencia.

- **Indicador 02 número de registro de riesgos:** este indicador muestra información sobre la documentación de los registros de incidentes.

Tabla 22: Resultado de indicador 02

COMPARACIÓN DE INDICADOR 02			
INDICADOR	**PRE TEST**	**POST TEST**	**MEJORA**
Número de registro de riesgos	38%	60%	22%

El resultado del pre test para este indicador es de un 38% (ver anexo 5, pregunta 13), evidenciando que no se tiene un registro de los riesgos que ocurren durante el desarrollo de sus procesos, afectando la continuidad del servicio. Por otro parte el resultado del post test para este indicador es de 60% (ver anexo 10, pregunta 13), evidenciando una mejora de 22%, demostrando que la aplicación del modelo mejora el porcentaje para este indicador, debido a que luego de las capacitaciones de ventajas de realizar registros de incidentes, los responsables se dieron cuenta de la importancia de tener un registro de riesgos.

- **Indicador 03 prioridad de riesgos:** este indicador muestra información sobre la asignación de prioridades para poder implantar respuestas a los riesgos de TI

Tabla 23: Resultado de indicador 03

COMPARACIÓN DE INDICADOR 03			
INDICADOR	**PRE TEST**	**POST TEST**	**MEJORA**
Prioridad de riesgos	38%	60%	22%

El resultado del pre test para este indicador es de un 38% (ver anexo 5, pregunta 12), evidenciando que no se le da importancia a la priorización de riesgos, pues no cuentan con actividades de respuesta a riesgos. Por otra parte, el resultado del post test para este indicador es de 60% (ver anexo 10, pregunta 12), evidenciando una mejora de 22%, demostrando que la aplicación del modelo mejora el porcentaje para este indicador, debido a que luego de las capacitaciones los responsables tomaron conciencia e iniciaron la priorización de riesgos con sus respectivas actividades en respuestas a los riesgos.

Después del análisis de los resultados anteriormente mencionados, se concluye que la aplicación del presente modelo mejora los indicadores evaluados, lo que genera que el instituto garantice la continuidad de sus servicios en los procesos organizacionales a través de la gestión de riesgos.

IV. Discusión de resultados

Se analizarán los resultados adquiridos en esta investigación, los cuales tiene relación con antecedentes descritos anteriormente.

La presente investigación concuerda con Paucar [8] y con Oviedo [9] en lograr la mejora continua de sus procesos a través de la gestión de riesgos. En la cual el primer autor mencionado, se basó en el cumplimento de los requisitos de la norma ISO 9001:2015, el segundo autor se basó en ISACA y NIST. A diferencia de la presente investigación que se desarrolló con los marcos de trabajo, MAGERIT 3.0, COBIT FOR RISK 5 e ISO31000-2018, las cuales ayudaron a la construcción del modelo y a lograr el cumplimiento de los requerimientos mínimos de la CBC de licenciamiento garantizando la continuidad del servicio en el instituto.

En la investigación de Benites y B. Frank [6], en relación a determinar la incidencia de un modelo de gestión de TI en una organización del estado. Basado en la NTP/IEC 27005:2018 y MAGERIT V.3(2014). concluye que es de suma importancia seguir linimentos de un modelo de gestión de TI para poder contrarrestar cualquier incidente o riesgo. Concordando con la presente investigación, a pesar de diferir en algunos marcos de trabajo. Donde gracias al modelo de la presente investigación se logró reducir el impacto de los riesgos que afectan la continuidad del servicio del instituto.

Delgado [11], en su investigación sobre un modelo de gestión de servicios de TI basado en COBIT5 e ITIL3, concluye que la aplicación de su modelo permitió establecer controles que garanticen la continuidad de los servicios. Concordando con el resultado del presente modelo que tiene por objetivo garantizar la continuidad del servicio, el cual se logró gracias a la aplicación y cumplimiento de las fases del modelo mejorando los procesos organizacionales del instituto, dando soporte a la toma de decisiones para adoptar mejoras de TI y uso de software, administración de datos e información, etc., difiriendo solo en los marcos de trabajos.

En general el marco de trabajo MAGERIT se emplea en las organizaciones públicas con el propósito de resolver o garantizar la gestión de riesgos, como el caso de la investigación propuesta por B. Y. H. Villanueva [7] que planteó la aplicación de un modelo de gestión de riesgos, basado en las estándares o marcos de trabajo MAGERIT, OCTAVE, y NIS, coincidiendo con la presente investigación solo en la utilización de MAGERIT y se acompañó de otros marcos de trabajo para la gestión de riesgos en instintos de educación superior tecnológicos. Logrando resolver riesgos significativos (Fallas en software, incidentes en hardware, ataques lógicos, etc.) para la continuidad del servicio educativo.

La presente investigación concuerda con Raico [14] y Torres[15] en mejorar el servicio de TI para garantizar la continuidad de servicios de educación, aunque difieren en algunos marcos o metodologías de trabajo. la presente investigación se

desarrolló en el ámbito educativo superior tecnológico donde se logró garantizar la continuidad del servicio educativo a través de la mejora de los servicios de TI, reduciendo las incidencias de infraestructura operativa de TI, problemas en la adopción y uso de hardware, etc.

A su vez el presente modelo de gestión de riesgos permitió fortalecer la continuidad del servicio en los procesos organizacionales y salvaguardar los activos de información en el sector de educación tecnológico pública, para ello se planteó como estrategias las capacitaciones en la mejora de la toma de decisiones sobre inversiones de TI, capacitación en la adopción y uso de software, debido a que es una de las dificultades, que deben de reforzarse y uno de los eslabones débiles en la continuidad del servicio en los procesos organizacionales.

V. Conclusiones

Para poder alcanzar el primer objetivo se logró armonizar los estándares y marcos de trabajos de gestión de servicios de TI. Los marcos que se utilizaron fueron AS/NZ 4360:204, ITIL 4, ISO 27000 – 2016, COBIT FOR RISK 5, MAGERIT 3.0. e ISO 31000 – 2018. De los cuales fueron seleccionados los 3 últimos basado en las dimensiones de: estructura del marco, procesos de gestión de riesgos, terminología de gestión de riesgos y sus fortalezas, las que fueron analizadas para determinar la afectación en la gestión de riesgos de TI para poder garantizar la continuidad de los servicios en los institutos.

Se realizó el análisis organizacional identificándose los procesos específicos (gestión institucional, gestión académica y programa de estudios pertinentes, infraestructura física, etc.) para beneficio de los estudiantes en donde se obtuvo que dichos procesos no son eficientes, no cumplen con los lineamientos que demanda la CBC y tampoco cuentan con un plan para actuar frente a algún riesgo. Ayudando asi a la elaboración de los componentes del modelo de gestión de riesgos.

Como contribución se propuso el modelo de gestión de riesgos de TI que tiene bases teóricas de tres marcos de trabajo los cuales permitieron dar soporte a la creación del modelo de la presente investigación, el cual consta de 4 fases principales (Descripción del contexto, gestión de valoración, gestión de riesgos y gestión de revisión y mejora continua), teniendo cada fase procesos internos, tambien cuentan con un conjunto de tablas, formularios y gráficos que dan soporte a su aplicación, con la única finalidad de garantizar la continuidad del servicio en los procesos organizacionales.

Se validó el modelo a través del método del juico de expertos. Los cuales fueron 3 los que validaron el presente modelo a través de los criterios de suficiencia, claridad, coherencia y relevancia, con una calificación del 1 al 4 siendo 1 el valor que no cumple y 4 el rango alto en cumplimiento por cada fase. Tras la prueba estadística de la V de AIKEN se obtuvo como resultado un 0.83 de validez, con ello se concluye que el modelo cumple con los criterios de validez del contenido.

La implementación del modelo en el IESTP Chongoyape, realizada por el autor de esta investigación, ha permitido mejorar la gestión de riesgos de TI y garantizar la continuidad del servicio en los procesos organizacionales en dicha entidad, a través del cumplimento de los requisitos de la CBC de licenciamientos para institutos, los cuáles fueron implementados con 8 proyectos.

A sí mismo esta investigación puede contribuir a futuras investigaciones para continuar con la gestión de riesgos de TI, dando soporte a los institutos de educación superior en la mejora de sus procesos y garantizar el cumplimiento de las normas o leyes que son dadas por MINEDU, para que de esa forma los institutos continúen brindando el servicio educativo de buena calidad.

En la presente investigación se presentaron las siguientes limitaciones, falta de disponibilidad por parte de los responsables de los procesos, resistencia al cambio debido a la comodidad de prácticas cotidianas, falta de comprensión u apoyo para las medidas de mitigación de riesgos por la percepción de que las nuevas medidas de gestión pueden afectar negativamente los procesos organizacionales.

VI. Recomendaciones

Se recomienda a futuras investigaciones enfatizar en las metodologías de armonización de los marcos de trabajo, con la finalidad que puedan adaptar la gestión de riesgos al contexto en donde se aplicará la investigación, de esta manera obtener mejores resultados en la gestión de riesgos, garantizando la continuidad del servicio.

Se recomienda a futuras investigaciones realizar el análisis de los procesos organizacionales, para poder obtener los servicios que les permitan formular los componentes del modelo, tal y como se realizó en la presente investigación en donde se obtuvo que no cumplían con los lineamentos de las CBC y que no contaban con un plan para actuar frente a algún riesgo.

En futuras investigaciones de gestión de riesgos de TI, se recomienda aplicar la validación de juicio de expertos y la prueba estadística de la V de AIKEN, con la finalidad de obtener el nivel de cumplimiento de los criterios de validez del contenido, que se encuentra en el rango de 0.80 – 1 para asegurar su validez.

Se recomienda implementar la gestión de riesgos enfatizando en la seguridad de la información en cualquier otro sector empresarial o institucional con la finalidad de facilitar la reducción de riesgos que puedan tener las entidades, de acuerdo al rubro de desempeño y asi garantizar la continuidad de los servicios que ofrecen, aplicando los diferentes estándares o marcos de trabajo referentes a la gestión de riesgos.

Se recomienda al instituto de educación superior tecnológico público continuar con la implementación del modelo propuesto con la finalidad de poder garantizar la continuidad del servicio en los procesos organizacionales, a través del tratamiento de las vulnerabilidades o amenazas a las que podrían estar expuestos. Y a su vez seguir adoptando nuevos modelos de gestión de riesgo, para ayudar a la mejora de sus procesos.

VII. Referencias

[1] «Aceleración digital: más del 94% de las pymes peruanas invirtió en tecnología en el último año», News Center Latinoamérica. Accedido: 9 de enero de 2023. [En línea]. Disponible en: https://news.microsoft.com/es-xl/aceleracion-digital-mas-del-94-de-las-pymes-peruanas-invirtio-en-tecnologia-en-el-ultimo-ano/

[2] «Riesgos TI Servicios Financieros (ok).pdf». Accedido: 11 de noviembre de 2022. [En línea]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf

[3] A. J. M. Mosquera, «Estado actual de la auditoria de seguridad en los sistemas de información de educación superior.□», p. 16.

[4] «Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio». Accedido: 11 de noviembre de 2022. [En línea]. Disponible en: https://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio

[5] M. M. S. Barrantes, «Dr. Víctor Ángel Ancajima Miñan presidente», p. 174.

[6] D. A. Benites y M. Frank, «Línea de Investigación»:, p. 79.

[7] B. Y. H. Villanueva, «Tesis para optar el grado académico de maestro en ingeniería de sistemas y computación con mención en dirección estratégica de tecnologías de información», p. 197.

[8] E. A. G. Paucar, «Diseño del modelo de gestión de la calidad basado en la norma iso 9001:2015, para la carrera de tecnología superior en confección textil del instituto superior tecnológico “Cotacachi”», p. 520.

[9] A. M. Oviedo, «Modelo de gobierno y gestión de riesgos ti para las Universidades Públicas de Colombia: caso de estudio universidad popular del cesar», p. 115.

[10] C. A. T. Jiménez, «Modelo de Gobierno y Gestión para la Arquitectura Empresarial, en instituciones de educación superior públicas del nivel técnico profesional. Caso IES INFOTEP de Ciénaga, Magdalena», p. 157.

[11] L. S. L. Delgado, «Modelo de gestión de servicios de ti, para mejorar la estrategia de fidelización de estudiantes en los Institutos de Educación Superior Pedagógicos Públicos en la Región Cajamarca», p. 192.

[12] J. A. G. Flores, «Modelo de gestión basado en el ciclo de vida del servicio de ti para mejorar los procesos de ti en las Instituciones Educativas Particulares de la Región Lambayeque», p. 215.

[13] L. R. T. Cornetero, «Modelo de seguridad de la información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque», p. 137.

[14] M. M. Z. Raico y M. Y. A. Garcia, «Tesis para optar el grado académico de maestro en ingeniería de sistemas y computación con mención en dirección estratégica de tecnologías de información», p. 245.

[15] M. E. F. Torres, «Modelo de gestión de servicios de ti para dar soporte a la continuidad del servicio educativo en Instituciones Públicas de Educación Básica Regular Nivel Secundaria de la Región Lambayeque».

[16] M. De E. Del Perú, «Ley de Institutos | Minedu». Accedido: 9 de enero de 2023. [En línea]. Disponible en: http://www.minedu.gob.pe/ley-de-institutos/

[17] P. M. De Educación, «Condiciones básicas de calidad para el procedimiento de licenciamiento de los Institutos de Educación Superior y las Escuelas de Educación Superior

Tecnológica», *Minist. Educ.*, feb. 2019, Accedido: 27 de julio de 2023. [En línea]. Disponible en: https://repositorio.minedu.gob.pe/handle/20.500.12799/6667

[18] «Aprueban Reglamento de la Ley N° 30512, Ley de Institutos y Escuelas de Educación Superior y de la Carrera Pública de sus Docentes-DECRETO SUPREMO-N° 010-2017-MINEDU». Accedido: 23 de enero de 2023. [En línea]. Disponible en: http://busquedas.elperuano.pe/normaslegales/aprueban-reglamento-de-la-ley-n-30512-ley-de-institutos-y-decreto-supremo-n-010-2017-minedu-1558487-1/

[19] «RVM 178 - Lineamientos-Academicos-Generales-2018 PDF | PDF | Educación más alta | Aprendizaje», Scribd. Accedido: 24 de enero de 2023. [En línea]. Disponible en: https://es.scribd.com/document/396764715/Curso-Auxiliar-Administrativo

[20] M. M. Arteaga-Martínez, «Gestión de riesgos de TI», 2017, Accedido: 3 de diciembre de 2022. [En línea]. Disponible en: https://www.academia.edu/69362708/Gesti%C3%b3n_de_riesgos_de_TI

[21] «Glosario». Accedido: 3 de diciembre de 2022. [En línea]. Disponible en: https://www.iso27000.es/glosario.html

[22] V. Mendez, «COBIT 5 for Risk», Accedido: 3 de diciembre de 2022. [En línea]. Disponible en: https://www.academia.edu/31530752/COBIT_5_for_Risk

[23] «COBIT 5 - Riesgo - pdf Docer.com.ar», Docer.com.ar. Accedido: 3 de diciembre de 2022. [En línea]. Disponible en: https://docer.com.ar/doc/sn0evcc

[24] «Gestion Riesgo Ti Unidad 3 PDF | PDF | Cobit | Toma de decisiones», Scribd. Accedido: 12 de enero de 2023. [En línea]. Disponible en: https://es.scribd.com/document/329436187/gestion-riesgo-ti-unidad-3-pdf

[25] Standards Australia, Ed., Risk management: AS NZS 4360:2004: Australian, New Zealand Standard, 3. Ed. Sydney, 2004.

[26] «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método».

[27] «ISO 31000 2009 gestion de riesgos - NORMA INTERNACIONAL ISO 31000 Primera edición - Noviembre 15 de - Studocu». Accedido: 10 de enero de 2023. [En línea]. Disponible en: https://www.studocu.com/pe/document/universidad-cesar-vallejo/gestion-de-proyectos/iso-31000-2009-gestion-de-riesgos/30180045

[28] «Serie 27k». Accedido: 9 de diciembre de 2022. [En línea]. Disponible en: https://www.iso27000.es/iso27000.html

[29] A. LIMITED, ITIL® Foundation, edición ITIL4. London: The Stationery Office Ltd, 2019.

VIII. Anexos

Anexo 01: Carta de aceptación para la elaboración de proyecto de tesis

MINISTERIODE EDUCACION
GERENCIA REGIONAL DE
EDUCACION LAMBAYEQUE

INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLOGICO PUBLICO
"CHONGOYAPE"
R.M. No. 0568-94-ED.//Revalidado con R.M. Nº 068-2005-ED
Dirección: Calle Miguel Iglesia N° 380 Teléfono: 433125
Email: institutochongoyape@gmail.com www.institutochongoyape.com

CARTA DE AUTORIZACIÓN DE ACEPTACIÓN PARA LA ELABORACIÓN DE PROYECTO DE TESIS PARA MAESTRÍA

INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PUBLICO CHONGOYAPE con RUC. N° **20313274234,** ubicado en CAL. MIGUEL IGLESIAS NRO. 380 LAMBAYEQUE - CHICLAYO – CHONGOYAPE, bajo el cargo de **DIRECTORA LIC. ZULEMA MENDOZA COPIA**

AUTORIZA:

Al **ING. JEFFERSON JAMES MILIÁN SAAVEDRA** con DNI: **46924324** estudiante de **POSGRADO** de ESCUELA PROFESIONAL DE MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN de la **UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO**, llevar a cabo **LA ELABORACIÓN DE TESIS DE MAESTRÍA**, bajo los consentimientos, políticas y lineamientos de nuestra representada, además la información que se le brindará es de confidencialidad, real y actualizada acorde con el desarrollo de proyectos y actividades dentro de nuestra organización

la presente se extiende a petición del interesado para los fines académicos que estime conveniente.

Chongoyape, 28 de diciembre 2022

INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PUBLICO "CHONGOYAPE"
Lic. Zulema Mendoza Copia
DIRECTORA GENERAL (e)

MINISTERIO DE EDUCACIÓN · I.E.S.T. - CHONGOYAPE · DIRECCIÓN

Directora
Lic. Zulema Mendoza Copia

Anexo 02: Descripción de estado actual de los institutos

DESCRIPCIÓN DE INSTITUTOS TECNOLÓGICO PÚBLICOS

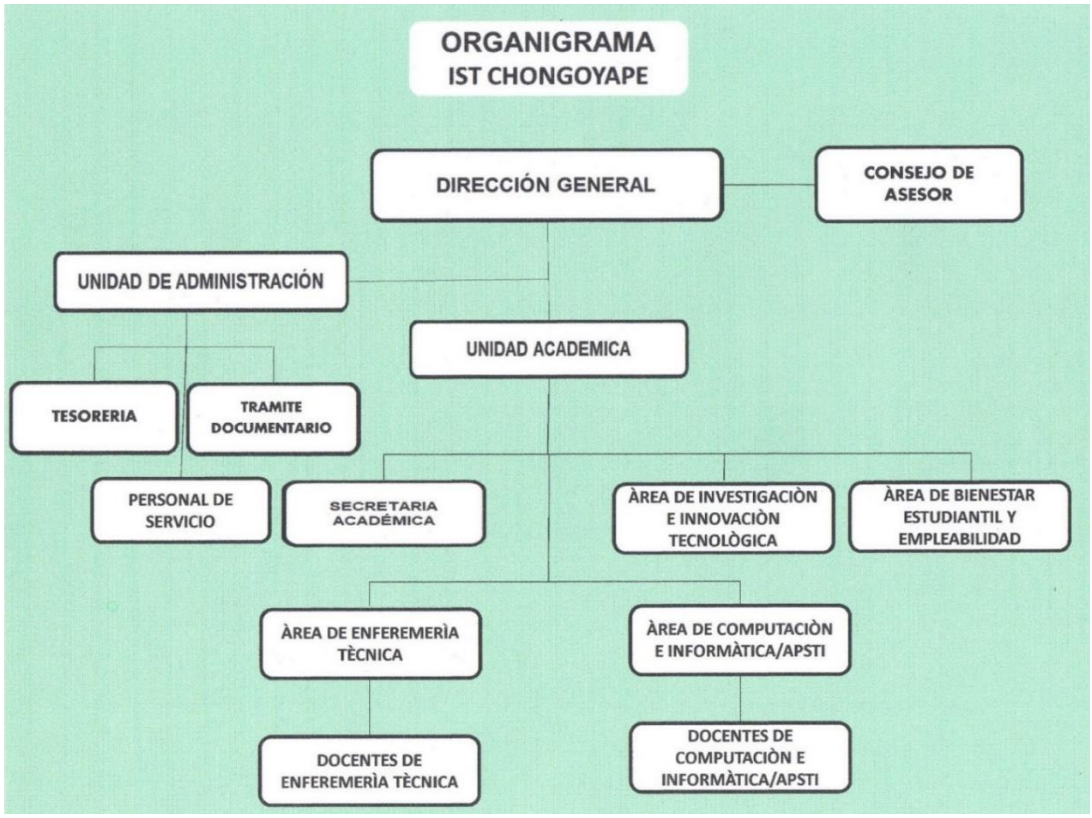
Se establece el contexto de las instituciones educativas, del sector público del nivel superior tecnológico de la región Lambayeque, siendo 3 institutos los que fueron elegidos para efectuar el análisis del contexto con el fin de optimizar la planificación para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos.

IESTP-CHONGOYAPE

La institución cuenta con 31 años a la prestación pedagógica de nivel superior tecnológico de la región Lambayeque. Quein actualmente cuenta como directora a la Lic. Zulema Mendoza Copia.

Está ubicado en el departamento de Lambayeque, provincia Chiclayo, distrito de Chongoyape, en la calle Miguel Iglesias N° 380 con teléfono 433072.

Seguidamente, se especifica el organigrama de la institución en donde se describe las diferentes áreas, de las cuales nos enfocaremos en aquellas que comprendan a las áreas académicas en los procesos organizacionales.



Misión:

Formar Profesionales Técnicos competitivos en Enfermería Técnica y Arquitectura de Plataformas y Servicios de Tecnologías de la Información; comprometidos con la innovación tecnológica para el desarrollo socioeconómico, práctica de valores, protección de la salud y el medio ambiente.

Visión:

Ser una institución líder en la región con carreras profesionales acreditadas que brindan una educación basada en la investigación, formando profesionales creativos, innovadores y emprendedores en el campo productivo, empresarial y de servicio; con principios éticos, comprometidos con la sociedad y la sostenibilidad del medio ambiente.

Valores:

La educación en el I.E.S.T.P. CHONGOYAPE se llama persona rescatando la esencia de la educación la cual esta fortalecida por la cultura desarrollada de valores, los docentes profesores son maestros que forman de manera integral a los estudiantes como ciudadanos con el objetivo ser agentes de transformación social. La comunidad educativa está comprometida en la práctica una filosofía basada en valores y esta se materializa en actos que de algún modo conllevan al logro y realización del proyecto de vida en la cual existe una dimensión ética donde se reflejan los valores que forman hábitos cultivos conllevan a la esencia humana de una virtud en su máxima expresión modelan el comportamiento de quienes constituimos un segmento de esta Institución.

En ese argumento toda la corporación, establecemos como valores primordiales los siguientes:

Valores Profesionales:

- Responsabilidad
- Compromiso
- Trabajo en equipo
- Aptitud

Valores Humanos:

- Solidaridad
- Prudencia
- Igualdad
- Sinceridad

Principios institucionales:

- Excelencia
- Pluralismo
- Innovación
- Respeto

Objetivos estratégicos:

En el ámbito pedagógico:

- Monitorear el cumplimiento de lo planificado en el periodo académico para así obtener una excelente capacidad operativa para el seguimiento y monitoreo pedagógico e institucional
- Definir y llevar a la práctica nuestra propuesta pedagógica para lograr en los estudiantes que desarrollen de forma integral sus potencialidades y capacidades y el ejercicio de actitudes y valores, que les permita su realización personal y los haga capaces de integrarse positivamente a su familia, su comunidad y la sociedad.
- Atraer al talento humano con docentes identificados, comprometidos y actualizados tecnológica y pedagógicamente, para lograr aprendizajes significativos en los estudiantes sabiendo que el pilar de la fuerza laboral lo conforman la plana docente en su mayoría que siendo actualmente los docentes de especialidad contratados.

En el ámbito institucional:

- Fortalecimiento de la imagen de nuestra institución dándose a conocer ante los grupos de interés buscando una identificación armoniosa con espacios de desarrollo para todos los colaboradores, estudiantes y comunidad en general dando lugar a alianzas estratégicas de apoyo para beneficio de la institución.
- Ampliar el trabajo integrado y trabajo en equipo promoviendo actividades de integración entre las diferentes áreas y estamentos de la institución, para disponer de un clima institucional positivo que sirva de marco adecuado e indispensable para el desarrollo del proceso de enseñanza - aprendizaje.
- Propiciar la participación activa de estudiantes en actividades programadas por el instituto, como soporte del mejoramiento de su desempeño.

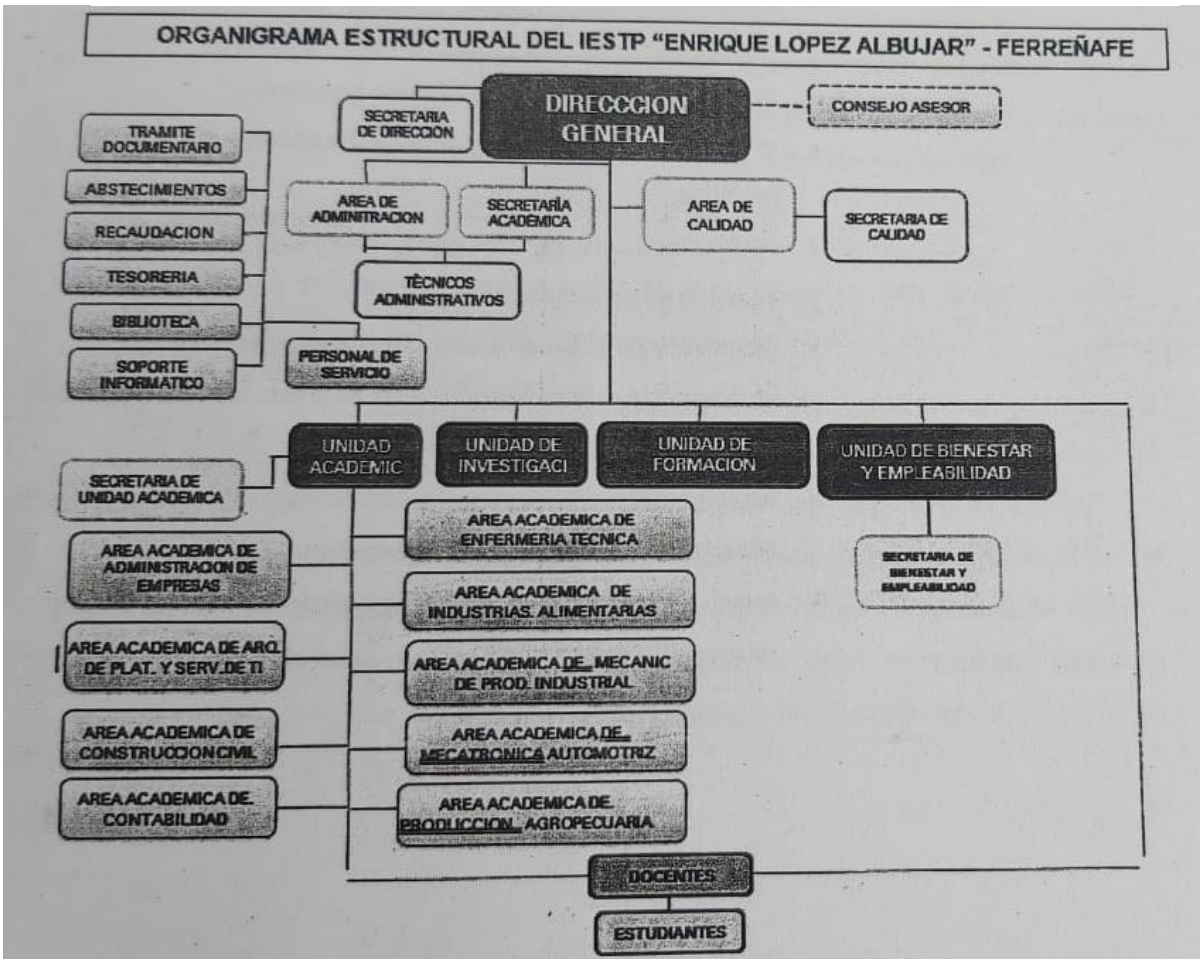
En el ámbito administrativo:

- Ordenamiento Administrativo y de Gestión de los procesos que brindan soporte a las actividades cotidianas dando énfasis al uso de plataformas tecnológicas que permitan tener información adecuada y oportuna para tomar decisiones.
- Maximización y correcta asignación del personal y economía con la finalidad de optimizar los ratios de gestión.

IESTP-ENRIQUE LOPEZ ALBUJAR:

La institución cuenta con 43 años a la prestación pedagógica de nivel superior tecnológico de la región Lambayeque. Quein actualmente cuenta como directora al Mg. Víctor Manuel Vásquez Mendoza.

Está ubicado en el departamento de Lambayeque, provincia Chiclayo, distrito de Ferreñafe, en la calle Víctor Raúl Haya de la Torre N° 214. Pueblo Nuevo. Seguidamente, se especifica el organigrama de la institución en donde se describe las diferentes áreas, de las cuales nos enfocaremos en aquellas que comprendan a las áreas académicas en los procesos organizacionales.



Misión:

Somos una Institución educativa de nivel superior que formamos profesionales técnicos, íntegros, competitivos, comprometidos con la investigación e innovación tecnológica que responde a las exigencias del mercado laboral para el cambio que la sociedad requiere.

Visión:

Al 2027 ser una institución licenciada, acreditada, líder en la educación superior tecnológica, comprometidos esencialmente con la investigación, innovación y el desarrollo humano sostenible de la región y del país.

Objetivos estratégicos:

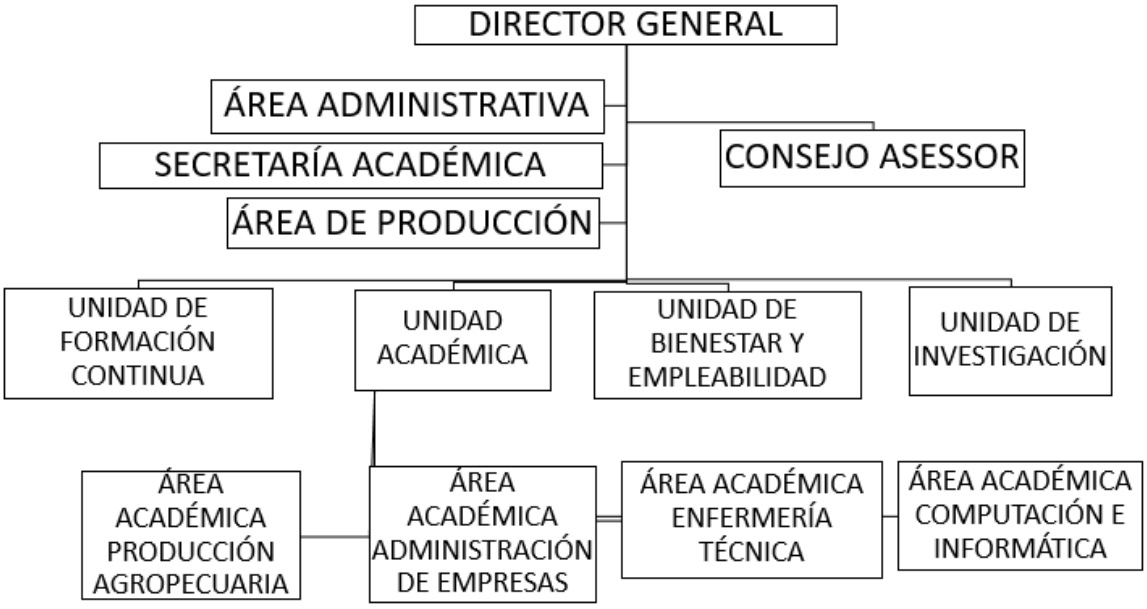
- Gestionar la ejecución del proyecto de mejoramiento de la Infraestructura educativa y su equipamiento en 02 años.
- Implementar los programas de estudios, a través de la formulación y ejecución de proyectos sostenibles, de producción de bienes, servicios y de proyección social, que permitan captar recursos económicos en un periodo de 04 años.
- Fortalecer el desarrollo profesional docente y administrativo, implementando eventos de capacitación permanentemente con una infraestructura moderna.
- Consolidar las EFSRT y contribuir la inserción laboral del egresado estableciendo convenios y alianzas estratégicas con empresas públicas y privadas en el ámbito regional y nacional
- Fortalecer las capacidades de investigación e innovación tecnológica de docentes y estudiantes para el desarrollo de proyectos, en 2 años.
- Lograr el Licenciamiento institucional, en un periodo de 04 años que garantice la calidad educativa y el liderazgo en la región.

IESTP-MOTUPE

La institución cuenta con 39 años a la prestación pedagógica de nivel superior tecnológico de la región Lambayeque. Quein actualmente cuenta como directora al Mg. Jose Elías Vasquez Carranza

Está ubicado en el departamento de Lambayeque, provincia Chiclayo, distrito de Motupe con teléfono 910920997

Seguidamente, se especifica el organigrama de la institución en donde se describe las diferentes áreas, de las cuales nos enfocaremos en aquellas que comprendan a las áreas académicas en los procesos organizacionales.



Misión:

Somos una Institución de Educación Superior Tecnológica Publica que forma profesionales técnicos altamente competitivos, creativos, emprendedores e innovadores, con calidad humana que responden a las necesidades de la actividad productiva y de servicio, respetando el medio natural.

Visión:

Al 2025 seremos una institución líder de educación superior tecnológica acreditada, con alianzas estratégicas con instituciones públicas y privadas con permanente practica de valores y principios institucionales acorde con los avances tecnológicos constantes.

Anexo 03: Instrumento de evaluación de variable dependiente

Cuestionario Instrumento de evaluación

Título de la tesis:

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN PARA GARANTIZAR LA CONTINUIDAD DEL SERVICIO EN LOS PROCESOS ORGANIZACIONALES EN LOS INSTITUTOS DE EDUCACIÓN SUPERIOR TECNOLÓGICOS PÚBLICOS

Dirigida: Personal Directivo

Objetivo:

La presente encuesta tiene como objetivo analizar la gestión de riesgos de tecnología de información en los procesos organizacionales del instituto superior tecnológico público Chongoyape dentro del marco de referencia de COBIT 2019

Las siguientes preguntas se responderán con las siguientes alternativas:

(1) Nunca; (2) la mayoría de las veces; (3) Unas veces sí, otras veces no; (4) La mayoría de las veces y (5) siempre

N°	Pregunta	1	2	3	4	5
1	¿La administración tiene claramente definido un plan estratégico de tecnología de información?					
2	¿En el plan estratégico de TI se encuentra definida la distribución de los recursos financieros?					
3	¿El plan estratégico ha definido metas e indicadores de evaluación de los proyectos de TI?					
4	¿Se han efectuado evaluaciones a los planes estratégicos de TI?					
5	¿Existe un plan para la adquisición o restructuración de TI?					
6	¿Se han definido procesos para informar al personal relevante sobre la adquisición e implementación de las TI?					
7	¿Al momento de adquirir TI o desarrollarlas, se aplican estándares para su aprobación?					
8	¿Los proyectos de TI están vinculados al portafolio de proyectos de la organización?					
9	¿Existe un marco de trabajo para los procesos relacionados con TI?					
10	¿Se realiza un seguimiento a los cronogramas de actividades de los proyectos de TI?					
11	¿Se han definido, planeado e implantado mediciones para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con las TI?					
12	¿Se han asignado prioridades y planeado las actividades identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución de control en todos los niveles para implantar las respuestas a los riesgos asociados a las TI?					

13	¿Se documentan los inconvenientes evidenciados en la ejecución de cada uno de los proyectos de TI?					
14	¿La organización ha establecido un comité encargado del direccionamiento y asesoramiento de la incorporación de las TI a los procesos de negocio?					
15	¿Se han definido roles y responsabilidades de los actores relacionados con las TI?					
16	¿Se han definido e implementado políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI?					
17	¿Se administran y controlan los riesgos relacionados con TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento?					
18	¿Se han realizado sesiones de capacitaciones de forma regular respecto a los procesos, los roles y las responsabilidades de los actores de las TI en caso de riesgo?					
19	¿La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear planes de seguridad de TI?					
20	¿Se realiza una adecuada transferencia de conocimiento a la gerencia?					
21	¿Se toman medidas cuando el desempeño y la capacidad de las TI no están en el nivel requerido?					
22	¿Se han definido y administrado una estrategia de distribución para asegurar que los planes de contingencia ante riesgos se distribuyan de manera apropiada y segura?					
23	¿Se han determinado todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa?					
24	En caso de actualizaciones a sistemas existentes, ¿se realiza un análisis de impacto, justificación costo/beneficio y administración de requerimientos?					

Anexo 04: Instrumento de evaluación Entrevista

Entrevista:

Dirigida: Alta dirección

Objetivo:

La presente entrevista tiene como objetivo analizar la gestión de riesgos de tecnología de información en los procesos organizacionales del instituto superior tecnológico publico Chongoyape

1. ¿De qué manera La administración tiene claramente definido un plan estratégico de tecnología de información?

2. ¿De qué manera los proyectos de TI están vinculados al portafolio de proyectos de la organización?

3. ¿La administración cuenta con la existencia de un marco de trabajo para los procesos relacionados con TI?

4. ¿De alguna manera se ha establecido un control de seguimiento a los cronogramas de actividades de los proyectos de TI?

5. ¿De qué forma la administración han definido, planeado e implantado mediciones para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con las TI?

6. ¿La administración han asignado prioridades y planeado las actividades identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución de control en todos los niveles para implantar las respuestas a los riesgos asociados a las TI?

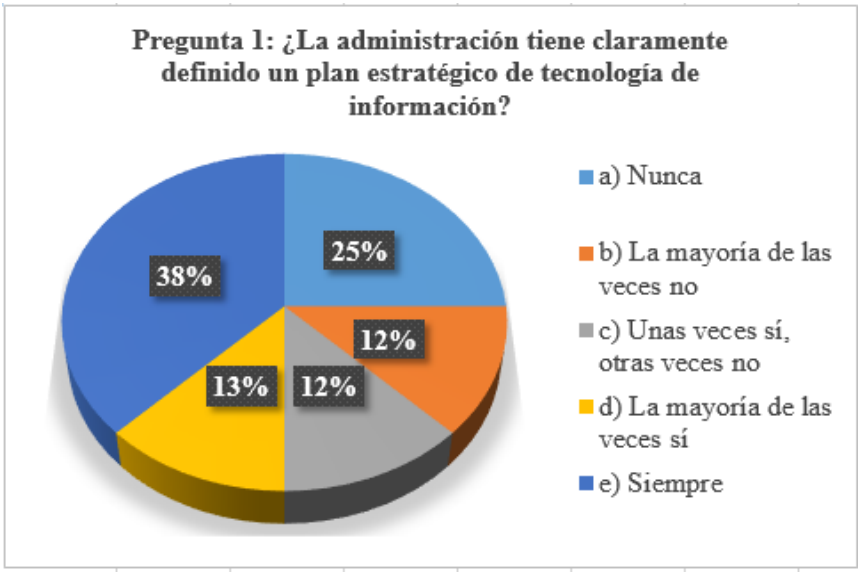
7. ¿De qué manera la alta dirección ha considerado establecer algún tipo de direccionamiento para la incorporación de las TI a los procesos organizacionales?

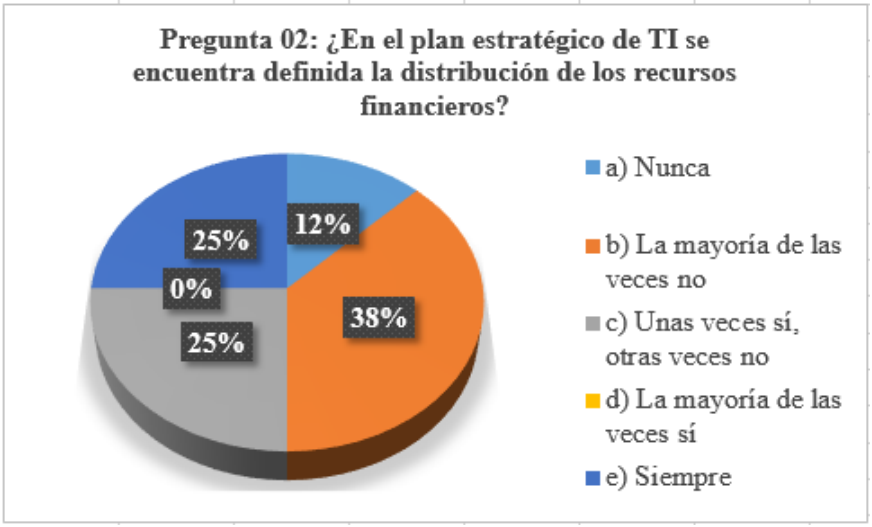
8. ¿La alta dirección ha definido roles y responsabilidades de los actores relacionados con las TI?

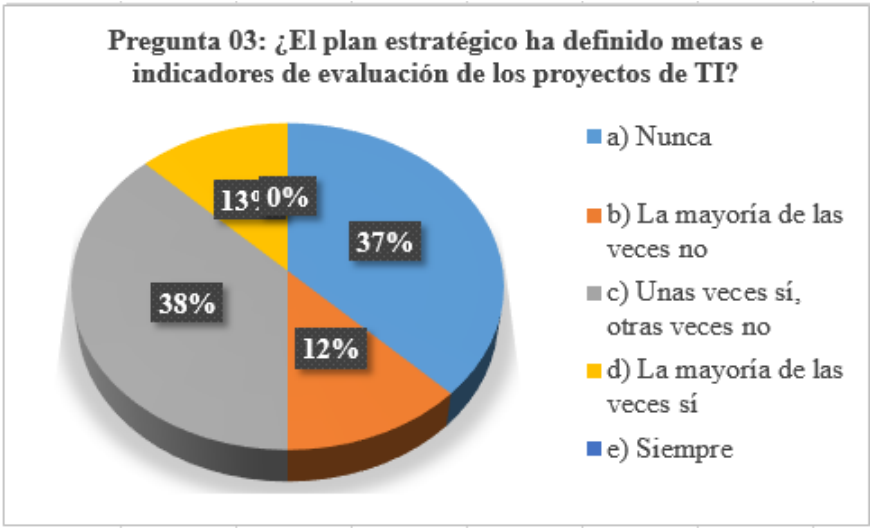
9. ¿De qué manera la alta dirección ha realizado sesiones de capacitaciones de forma regular respecto a los procesos, los roles y las responsabilidades de los actores de las TI en caso de riesgo?

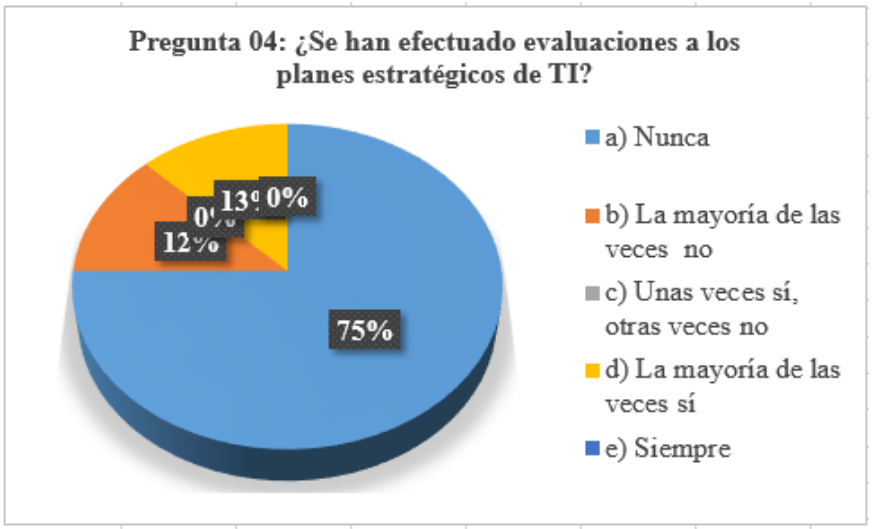
10. ¿De qué manera se le informa a la alta dirección los procesos y actividades de TI?

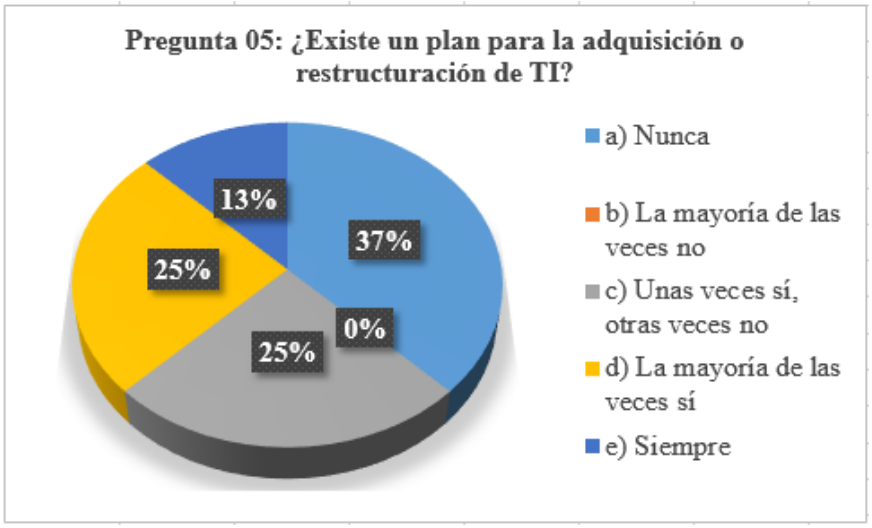
Anexo 05: Resultados de cuestionario Pre test

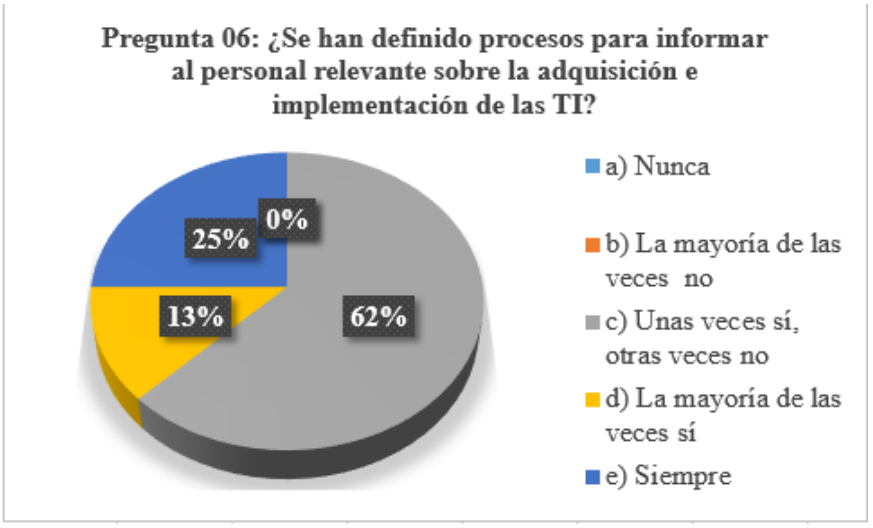




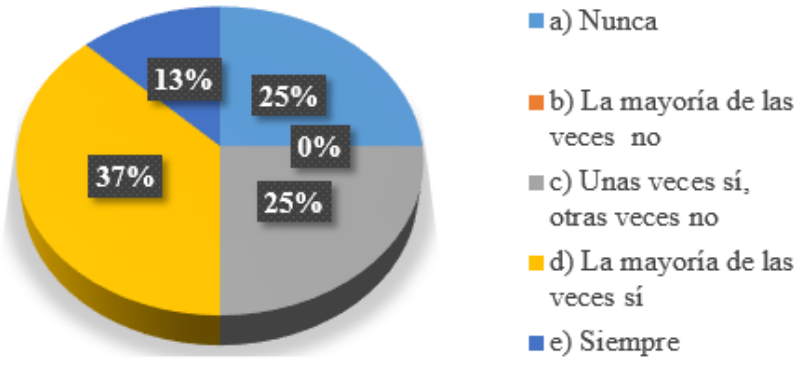



Pregunta 04: ¿Se han efectuado evaluaciones a los planes estratégicos de TI?
0%
12%
75%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre

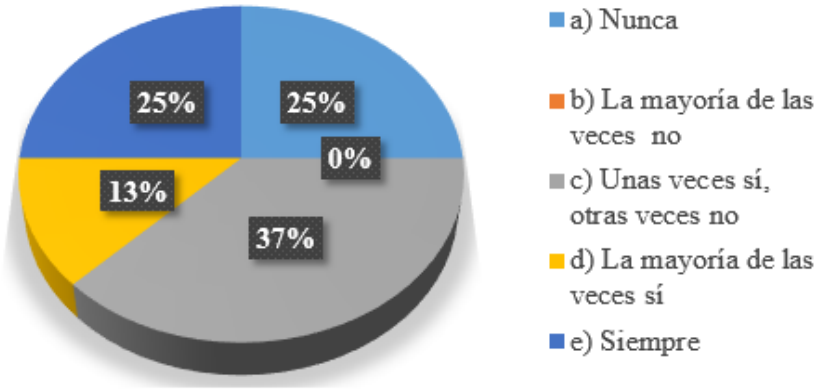

Pregunta 05: ¿Existe un plan para la adquisición o restructuración de TI?
13%
37%
25%
0%
25%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 06: ¿Se han definido procesos para informar al personal relevante sobre la adquisición e implementación de las TI?
0%
25%
13%
62%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre

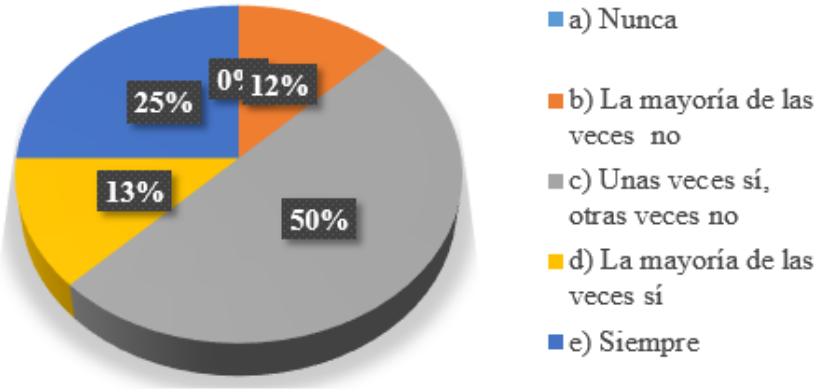
Pregunta 07: ¿Al momento de adquirir TI o desarrollarlas, se aplican estándares para su aprobación?



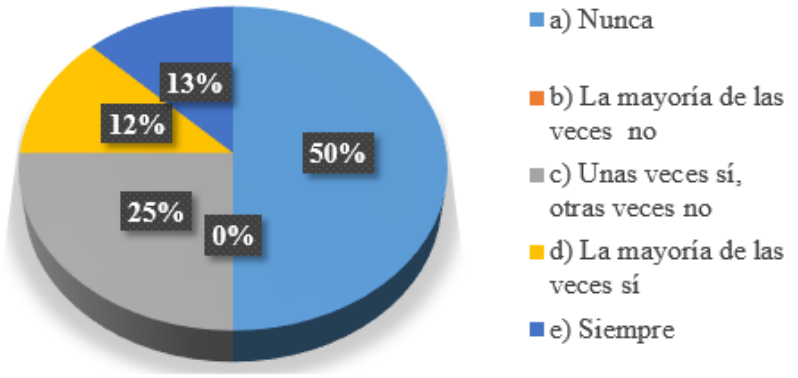
Pregunta 08: ¿Los proyectos de TI están vinculados al portafolio de proyectos de la organización?



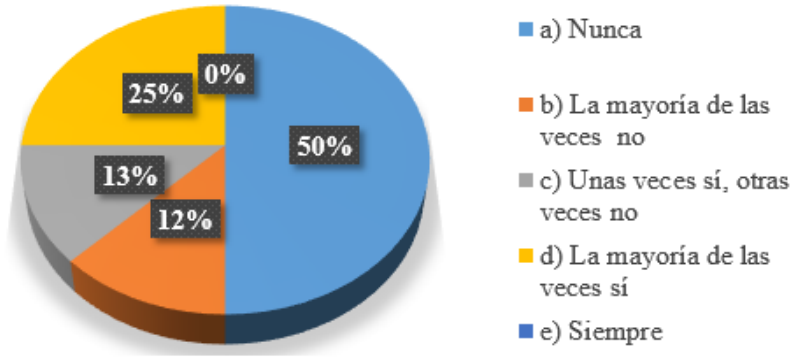
Pregunta 09: ¿Existe un marco de trabajo para los procesos relacionados con TI?



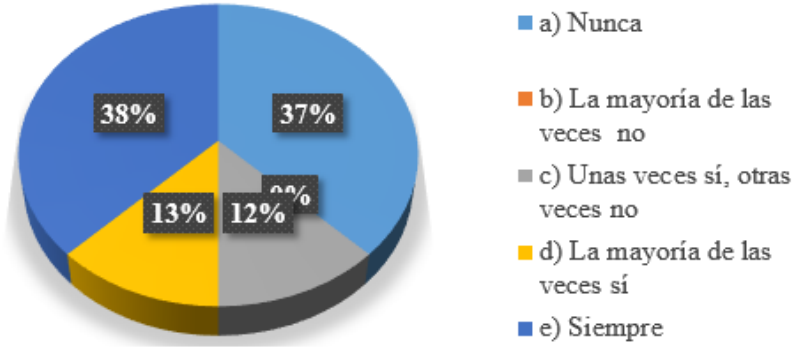
Pregunta 10: ¿Se realiza un seguimiento a los cronogramas de actividades de los proyectos de TI?



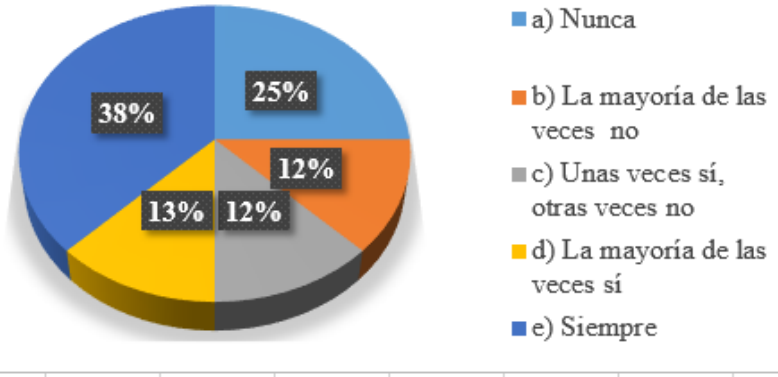
Pregunta 11: ¿Se han definido, planeado e implantado mediciones para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con las TI?



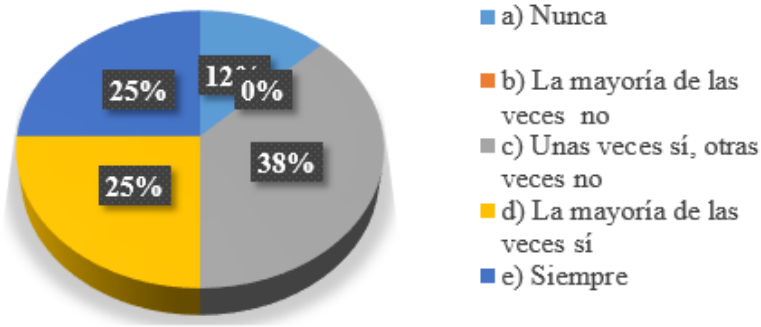
Pregunta 12: ¿Se han asignado prioridades y planeado las actividades identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución de control en todos los niveles para implantar las respuestas a los



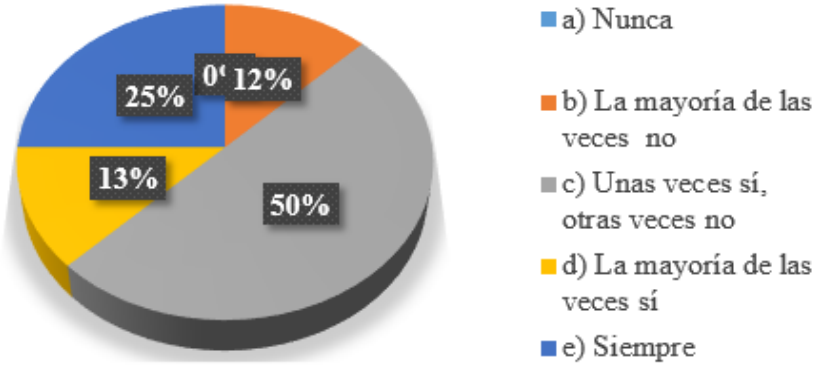
Pregunta 13: ¿Se documentan los inconvenientes evidenciados en la ejecución de cada uno de los proyectos de TI?



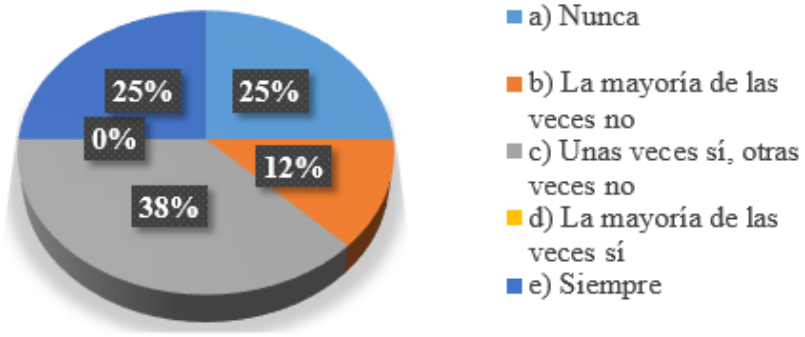
Pregunta 14: ¿La organización ha establecido un comité encargado del direccionamiento y asesoramiento de la incorporación de las TI a los procesos de negocio?



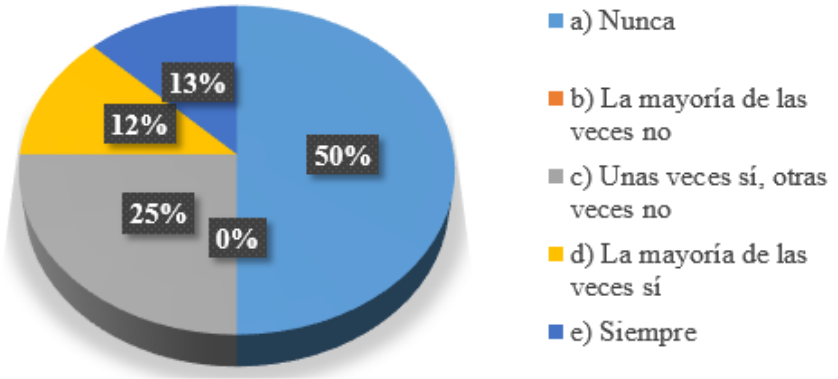
Pregunta 15: ¿Se han definido roles y responsabilidades de los actores relacionados con las TI?



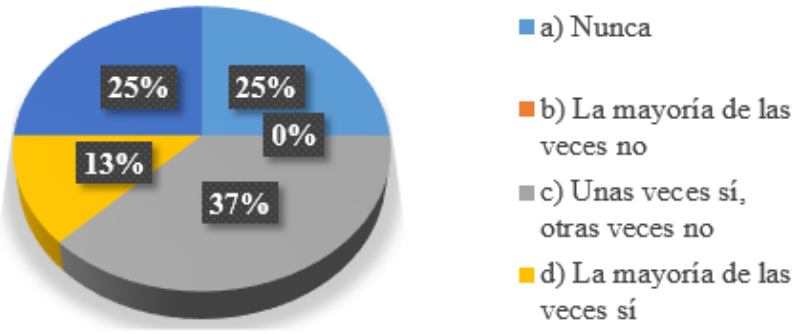
Pregunta 16: ¿Se han definido e implementado políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI?



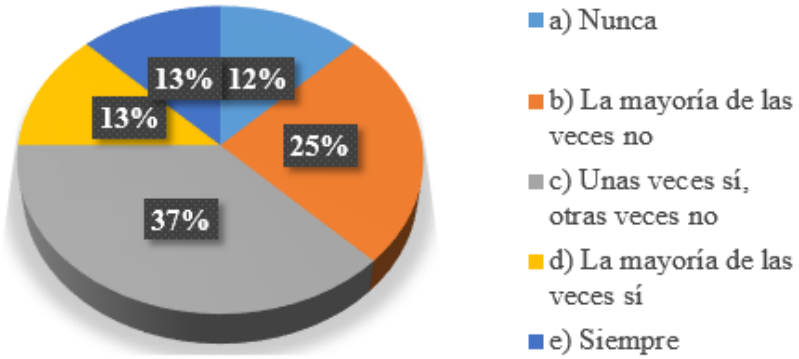
Pregunta 17: ¿Se administran y controlan los riesgos relacionados con TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento?



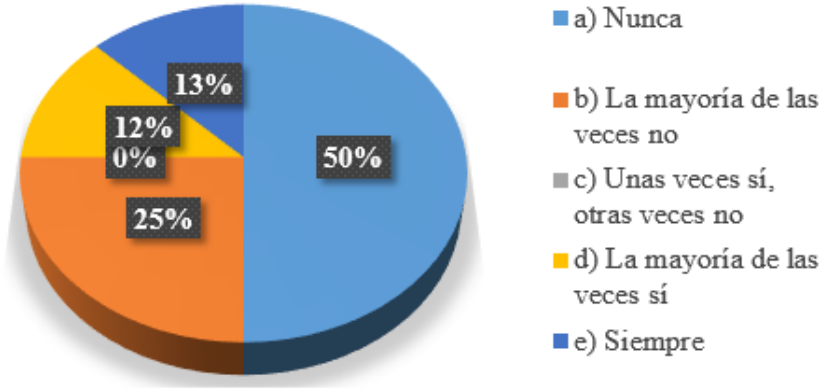
Pregunta 18: ¿Se han realizado sesiones de capacitaciones de forma regular respecto a los procesos, los roles y las responsabilidades de los actores de las TI en caso de riesgo?



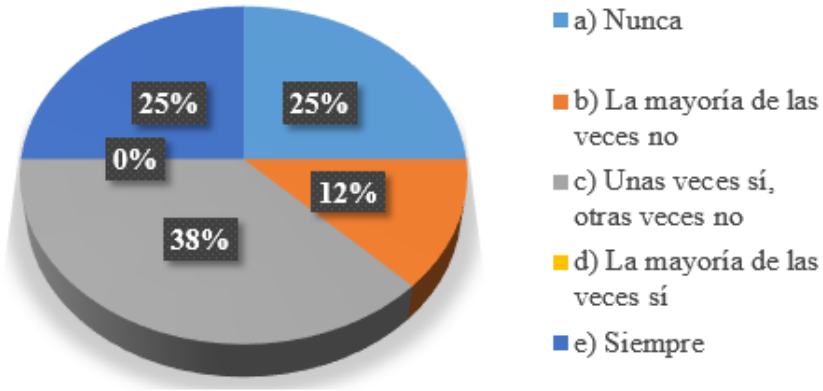
Pregunta 19: ¿La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear planes de seguridad de TI?



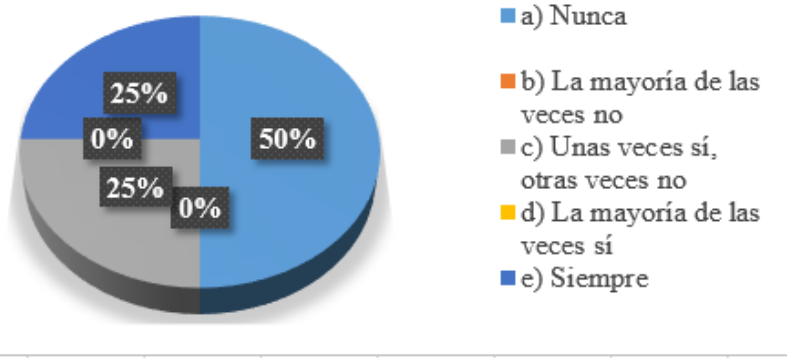
Pregunta 20: ¿Se realiza una adecuada transferencia de conocimiento a la gerencia?



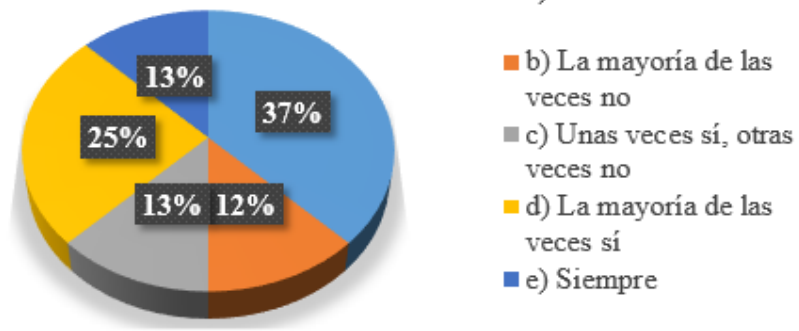
Pregunta 21: ¿Se toman medidas cuando el desempeño y la capacidad de las TI no están en el nivel requerido?



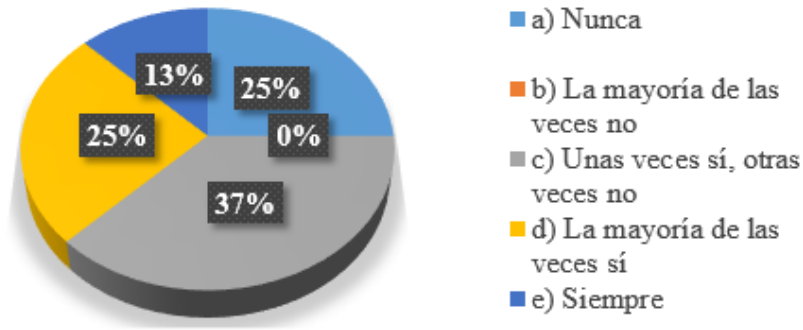
Pregunta 22: ¿Se han definido y administrado una estrategia de distribución para asegurar que los planes de contingencia ante riesgos se distribuyan de manera apropiada y segura?



Pregunta 23: ¿Se han determinado todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa?



Pregunta 24: En caso de actualizaciones a sistemas existentes, ¿se realiza un análisis de impacto, justificación costo/beneficio y administración de requerimientos?



Anexo 06: Validación de juicio de expertos:

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	14/09/2023	**Investigador:**	Jefferson James Milián Saavedra
Datos del Experto			
Nombres y apellidos	Rómulo Lomparte Alvarado		
Formación académica	Licenciado en Computación / MBA		
Áreas de experiencia profesional:	Gobierno de TI, auditoria, seguridad de la información, ciberseguridad y desarrollo de proyectos, calidad, gestión de riesgo, protección de datos, continuidad de negocio, etc.		
Tiempo de experiencia	30 años		
Cargo actual	Líder de Consultoría para Hispanoamérica / Docente de postgrado		
Institución / Empresa	Telefónica Tech / USAT, UNMSM, UTP, UPN, UPAO, UContinental, UPC		
Objetivo de la investigación	Implementar un modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos		
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.		
Objetivo de la prueba	Determinar la utilidad del modelo propuesto para los institutos de educación superior tecnológicos públicos de la región Lambayeque		

Firma del experto

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

USAT
Universidad Católica
Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**PROCESO**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Fase 01: Descripción del contexto:	**DC01:** Contexto interno	4	4	4	4	
	DC02: Contexto Externo	4	4	4	4	
	DC03: Definición de alcance y criterios de riesgos	4	4	4	4	
	DC04: Definición de roles y responsabilidades	4	4	4	4	
	DC05: Documentación de la fase	4	4	4	4	
Fase 02: Gestión de valoración	**GV01:** Identificación de activos	4	4	4	4	
	GV02: Gestión de valoración de activos	4	4	4	4	
	GV03: Documentación de la fase	4	4	4	4	
Fase 03: Gestión de riesgos	**GR01:** Gestionar los activos de riesgos	4	4	4	4	
	GR02: Monitorear los activos	4	4	4	4	
	GR03: Medición de activos	4	4	4	4	
	GR04: Definición del plan de gestión de riesgos	4	4	4	4	
	GR05: Documentación de la fase	4	4	4	4	
Fase 04: Gestión de revisión y mejora continua	**GM01:** Revisión de gestión de riesgos	4	4	4	4	
	GM02: Comunicación de resultados	4	4	4	4	
	GM03: Incorporación de nuevas sugerencias	4	4	4	4	
	GM04: Documentación de la fase	4	4	4	4	
				ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)		**Aceptado**

Firma del experto

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	2-Oct-2023	**Investigador:**	Jefferson James Millán Saavedra
Datos del Experto			
Nombres y apellidos	Juan Dávila Ramírez		
Formación académica	Ingeniero Industrial / MBA		
Áreas de experiencia profesional:	Riesgos tecnológicos / Seguridad de Información / Ciberseguridad / Auditoría de TI /		
Tiempo de experiencia	28 años		
Cargo actual	Director		
Institución / Empresa	PROTIVITI Perú Consulting Firm		
Objetivo de la investigación	Implementar un modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos		
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.		
Objetivo de la prueba	Determinar la utilidad del modelo propuesto para los institutos de educación superior tecnológicos públicos de la región Lambayeque		

Firma del experto

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

USAT
Universidad Católica
Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**PROCESO**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Fase 01: Descripción del contexto:	**DC01**: Contexto interno	2	3	3	3	Confusiones conceptuales sobre el contexto, gobierno e incidentes de TI
	DC02: Contexto Externo	3	3	3	3	
	DC03: Definición de alcance y criterios de riesgos	3	3	3	3	
	DC04: Definición de roles y responsabilidades	2	2	2	2	Demasiado genérico. No indica cómo hacerlo.
	DC05: Documentación de la fase	3	3	3	3	
Fase 02: Gestión de valoración	**GV01**: Identificación de activos	3	3	3	3	
	GV02: Gestión de valoración de activos	2	2	2	2	No queda claro qué tipo de activo se valora
	GV03: Documentación de la fase	3	3	3	3	
Fase 03: Gestión de riesgos	**GR01**: Gestionar los activos de riesgos	2	2	2	2	Confusión conceptual de activos y escenarios
	GR02: Monitorear los activos	2	2	2	2	Esto no es monitorear
	GR03: Medición de activos	2	2	2	2	Esto no es medición de activos
	GR04: Definición del plan de gestión de riesgos	2	2	2	2	Esto es plan de acción
	GR05: Documentación de la fase	3	3	3	3	
Fase 04: Gestión de revisión y mejora continua	**GM01**: Revisión de gestión de riesgos	3	3	3	3	
	GM02: Comunicación de resultados	3	3	3	3	
	GM03: Incorporación de nuevas sugerencias	3	3	3	3	
	GM04: Documentación de la fase	3	3	3	3	
					ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)	**Observado**

Firma del experto

USAT

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha		**Investigador:**	Jefferson James Milián Saavedra
Datos del Experto			
Nombres y apellidos	Jorge Martín Rodríguez Castro		
Formación académica	Ing. Computación e Informática Mtro. Ing. Sistemas y Computación		
Áreas de experiencia profesional:	Gestión de Proyectos / Desarrollo Sw. Docencia Universitaria		
Tiempo de experiencia	20+ años		
Cargo actual	Desarrollador Independiente / Docente		
Institución / Empresa	(Privado) / Univ Tecnológica del Perú		
Objetivo de la investigación	Implementar un modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos		
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende		
Objetivo de la prueba	Determinar la utilidad del modelo propuesto para los institutos de educación superior tecnológicos públicos de la región Lambayeque		

Firma del experto

USAT

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

USAT
Universidad Católica

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	PROCESO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Fase 01: Descripción del contexto:	**DC01:** Contexto interno	4	4	4	4	—
	DC02: Contexto Externo	4	4	4	4	—
	DC03: Definición de alcance y criterios de riesgos	4	4	4	4	—
	DC04: Definición de roles y responsabilidades	4	4	4	4	—
	DC05: Documentación de la fase	3	3	4	4	DEFINIR POSIBLES VALORES PARA ESTADO DE FASE
Fase 02: Gestión de valoración	**GV01:** Identificación de activos	4	4	4	4	—
	GV02: Gestión de valoración de activos	4	4	4	4	—
	GV03: Documentación de la fase	4	4	4	4	—
Fase 03: Gestión de riesgos	**GR01:** Gestionar los activos de riesgos	4	4	4	4	—
	GR02: Monitorear los activos	4	4	4	4	—
	GR03: Medición de activos	4	3	3	4	TABLA 16. CONDICIONES SE SUPERPONEN, RECTIFICAR
	GR04: Definición del plan de gestión de riesgos	4	4	4	4	—
	GR05: Documentación de la fase	3	3	4	4	DEFINIR POSIBLES VALORES PARA ESTADO DE FASE
Fase 04: Gestión de revisión y mejora continua	**GM01:** Revisión de gestión de riesgos	4	4	4	4	—
	GM02: Comunicación de resultados	4	4	4	4	—
	GM03: Incorporación de nuevas sugerencias	4	4	4	4	—
	GM04: Documentación de la fase	3	3	4	4	DEFINIR POSIBLES VALORES PARA ESTADO DE FASE
					ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)	ACEPTADO

DEBE LEVANTAR LAS OBSERVACIONES, QUE SON MENORES.

Firma del experto

Anexo 07: Resultado de gestión de valoración

	INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO CHONGOYAPE				
	FASE 02:	**Gestión de valoración**	FECHA DE ELABORACIÓN	20/11/2023	
	PROCESO GV01:	**Identificación de Activos**	FECHA DE APLICACIÓN	23/11/2023	
OBJETIVO	Identificar los activos con los que cuenta el instituto				
ACTIVO	**SOFTWARE**				
CÓDIGO	**NOMBRE**	**DESCRIPCIÓN**	**ESTADO**	**UBICACIÓN**	**RESPONSABLE**
SO_01	Sistema operativo	Windows 8.1 Pro	Operativo sin licencia	Lab_01	Coordinador académico
SO_02	Sistema operativo	Windows 10 Education	Operativo sin licencia	Lab_01	Coordinador académico
SO_03	Sistema Operativo	Windows 10 Pro	Operativo sin licencia	Lab_01	Coordinador académico
SO_04	Sistema Operativo	Windows 10 Education	Operativo sin licencia	Lab_02	Coordinador académico
SO_05	Sistema Operativo	Windows 10 Pro	Operativo sin licencia	Lab_02	Coordinador académico
SO_06	Sistema Operativo	Windows 11 Pro	Operativo sin licencia	Lab_02	Coordinador académico
SO_07	Sistema Operativo	Windows 10 Education	Operativo sin licencia	Lab_03	Coordinador académico
SO_08	Sistema Operativo	Windows 10 Pro	Operativo sin licencia	Lab_03	Coordinador académico
SO_09	Sistema Operativo	Windows 11 Pro	Operativo sin licencia	Lab_03	Coordinador académico
SO_10	Aplicativo	Paquete Office 2016	Operativo sin licencia	Lab_01	Coordinador académico
SO_11	Aplicativo	Paquete Office 2019	Operativo sin licencia	Lab_01	Coordinador académico

SO_12	Aplicativo	Paquete Office 2019	Operativo sin licencio	Lab_02	Coordinador académico
SO_13	Aplicativo	Paquete Office 2021	Operativo sin licencio	Lab_02	Coordinador académico
SO_14	Aplicativo	Paquete Office 2019	Operativo sin licencio	Lab_03	Coordinador académico
SO_15	Aplicativo	Paquete Office 2021	Operativo sin licencio	Lab_03	Coordinador académico
SO_16	Página Web	https://iestchongoyape.edu.pe/	Operativo	Hosting	Coordinador académico
SO_17	Aplicativo	Correo Corporativo @iestchongoyape.edu.pe	Operativo	Hosting	Coordinador académico
SO_18	Aplicativo	Sistema Registrar	Operativo	MINEDU	Secretario Académico
ACTIVO	**HARDWARE**				
CODIGO	**NOMBRE**	**DESCRIPCIÓN**	**ESTADO**	**UBICACIÓN**	**RESPONSABLE**
HW_01	Case	Cybertel: Disco duro de 500 GB, RAM 4 GB, Procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_02	Monitor	AOC	Operativo	Lab_01	Coordinador académico
HW_03	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_04	Case	Cybertel: Disco duro 500 GB, RAM de 4 GB, Procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_05	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_06	Teclado y mouse	Enkore Access y genius	Operativo	Lab_01	Coordinador académico
HW_07	Case	Cybertel: Disco duro 500 GB, RAM 4 GB, procesador Intel Core i3	Operativo	Lab_01	Coordinador académico

HW_08	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_09	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_10	Case	Cybertel: Disco duro 500 GB, RAM 4 GB, procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_11	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_12	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_13	Case	Halion: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i7	Operativo	Lab_01	Coordinador académico
HW_14	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_15	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_16	Case	Halion: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i7	Operativo	Lab_01	Coordinador académico
HW_17	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_18	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_19	Case	HP: Disco duro 250 GB, RAM 4 GB, procesador Intel Core 2 duo	Operativo	Lab_01	Coordinador académico
HW_20	Monitor	HP	Operativo	Lab_01	Coordinador académico
HW_21	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_22	Case	HP: Disco duro 250 GB, RAM 4 GB, procesador Intel Core 2 duo	Operativo	Lab_01	Coordinador académico
HW_23	Monitor	Dell	Operativo	Lab_01	Coordinador académico
HW_24	Teclado y mouse	Halion	Operativo	Lab_01	Coordinador académico

HW_25	Case	Cybertel: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_26	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_27	Teclado y mouse	Halion	Operativo	Lab_01	Coordinador académico
HW_28	Case	Cybertel: Disco duro 500 GB, RAM 4 GB, procesador Intel Core i3	Operativo	Lab_01	Coordinador académico
HW_29	Monitor	HP	Operativo	Lab_01	Coordinador académico
HW_30	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_31	Case	Halion: Disco duro 1 TB, RAM 8GB, procesador Intel Core i7	Operativo	Lab_01	Coordinador académico
HW_32	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_33	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_34	Case	Halion: Disco duro 1 TB, RAM 4 GB, procesador AMD R5	Operativo	Lab_01	Coordinador académico
HW_35	Monitor	HP	Operativo	Lab_01	Coordinador académico
HW_36	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_37	Case	Ecotrend: Disco duro 500 GB, RAM 4 GB, procesador AMD	Operativo	Lab_01	Coordinador académico
HW_38	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_39	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_40	Case	Halion: Disco duro 1TB, RAM 8 GB, procesador Intel Core i7	Operativo	Lab_01	Coordinador académico

HW_41	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_42	Teclado y mouse	Enkore Access	Operativo	Lab_01	Coordinador académico
HW_43	Case	Micronics: Disco duro 500 GB, RAM 4 GB, RAM 4 GB	Operativo	Lab_01	Coordinador académico
HW_44	Monitor	Samsung	Operativo	Lab_01	Coordinador académico
HW_45	Teclado y mouse	Logitech	Operativo	Lab_01	Coordinador académico
HW_46	Case	Halion: Disco duro 1TB, RAM 8 GB, procesador Intel Core i7	Operativo	Lab_01	Coordinador académico
HW_47	Monitor	LG	Operativo	Lab_01	Coordinador académico
HW_48	Teclado y mouse	Genius	Operativo	Lab_01	Coordinador académico
HW_49	Switch	Encore ENH916-NWY-16 port nway switch	Operativo	Lab_01	Coordinador académico
HW_50	Case	HP: Disco duro 1 TB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_51	Monitor	HP	Operativo	Lab_02	Coordinador académico
HW_52	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_53	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_54	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_55	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_56	Case	Teros: Disco duro 500 GB, RAM 8GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_57	Monitor	LG	Operativo	Lab_02	Coordinador académico

HW_58	Teclado y mouse	Logitech	Operativo	Lab_02	Coordinador académico
HW_59	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_60	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_61	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_62	Case	Halion: disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_63	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_64	Teclado y mouse	HP	Operativo	Lab_02	Coordinador académico
HW_65	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_66	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_67	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_68	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_69	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_70	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_71	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_72	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_73	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico

HW_74	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_75	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_76	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_77	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_78	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_79	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_80	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_81	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_82	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_83	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_84	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_85	Teclado y mouse	Halion	Operativo	Lab_02	Coordinador académico
HW_86	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_87	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_88	Teclado y mouse	Logitech	Operativo	Lab_02	Coordinador académico
HW_89	Case	Teros: Disco duro 1 TB, RAM 8 GB,	Operativo	Lab_02	Coordinador académico

		procesador Intel Core i5			
HW_90	Monitor	Samsung	Operativo	Lab_02	Coordinador académico
HW_91	Teclado y mouse	HP	Operativo	Lab_02	Coordinador académico
HW_92	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_02	Coordinador académico
HW_93	Monitor	LG	Operativo	Lab_02	Coordinador académico
HW_94	Teclado y mouse	Logitech	Operativo	Lab_02	Coordinador académico
HW_95	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_96	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_97	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_98	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_99	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_100	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_101	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_102	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_103	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_104	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_105	Monitor	LG	Operativo	Lab_03	Coordinador académico

HW_106	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_107	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_108	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_109	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_110	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_111	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_112	Teclado y mouse	Halion	Operativo	Lab_03	Coordinador académico
HW_113	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_114	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_115	Teclado y mouse	Enkore Access	Operativo	Lab_03	Coordinador académico
HW_116	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_117	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_118	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_119	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_120	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_121	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico

HW_122	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_123	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_124	Teclado y mouse	Logitech	Operativo	Lab_03	Coordinador académico
HW_125	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_126	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_127	Teclado y mouse	Halion	Operativo	Lab_03	Coordinador académico
HW_128	Case	Halion: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_129	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_130	Teclado y mouse	Halion	Operativo	Lab_03	Coordinador académico
HW_131	Case	Teros: Disco duro 500 GB, RAM 8 GB, procesador Intel Core i5	Operativo	Lab_03	Coordinador académico
HW_132	Monitor	LG	Operativo	Lab_03	Coordinador académico
HW_133	Teclado y mouse	Halion	Operativo	Lab_03	Coordinador académico
HW_134	Switch	Satra 16-port 10/100 MBps Fast Ethernet switch	Operativo	Lab_03	Coordinador académico
HW_135	Switch	D-Link Des-1016D 10/100 MBps Fast Ethernet switch	Operativo	Lab_03	Coordinador académico
HW_136	Switch	TP-Link TL-SF1016D 16 port 10/100 MBps desktop switch	Operativo	Lab_03	Coordinador académico
ACTIVO	**SERVICIO**				

CODIGO	NOMBRE	DESCRIPCIÓN	ESTADO	UBICACIÓN	RESPONSABLE
SE_01	Mantenimiento preventivo	Para evitar pérdidas de información y de procesos	Operativo	Diferentes ambiente	Coordinador académico
SE_02	Servicio de internet	El servicio de internet que se adquiere a un proveedor	Operativo	Jefatura	Coordinador académico
SE_03	Portal Web	Página institucional al servicio de la comunidad estudiantil	Operativo	Jefatura	Coordinador académico
SE_03	Correo Electrónico	Correo institucional para los estudiantes, administrativos y docentes	Operativo	Jefatura	Coordinador académico

RESPONSABLE	ELABORADO	REVISADO	APROBADO
NOMBRE	Jefferson James Milián Saavedra	Coordinador de APSTI	Directora del instituto
FECHA	20/11/2023	23/11/2023	23/11/2023
FIRMA			

Anexo 08: Autorización de capacitación sobre riesgos de TI

MINISTERIO DE EDUCACION
GERENCIA REGIONAL DE
EDUCACION LAMBAYEQUE

INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLOGICO PUBLICO
"CHONGOYAPE"
R.M. No. 0568-94-ED.//Revalidado con R.M. N° 068-2005-ED
Dirección: Calle Miguel Iglesia N° 380 Teléfono: 433125
Email: Institutoohongoyape@gmail.com www.Institutoohongoyape.com

CARTA DE AUTORIZACIÓN PARA CAPACITACIÓN SOBRE RIESGOS DE TI PARA CONTINUAR CON EL DESARROLLO DE TESIS PARA MAESTRÌA

INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO ÚBLICO CHONGOYAPE con RUC. N° **20313274234,** ubicado en CALLE MIGUEL IGLESIAS NRO. 380 LAMBAYEQUE - CHICLAYO – CHONGOYAPE, bajo el cargo de **DIRECTORA LIC. ZULEMA MENDOZA COPIA**

AUTORIZA:

Al **ING. JEFFERSON JAMES MILIÁN SAAVEDRA** con DNI: **46924324** estudiante de **POSGRADO** de ESCUELA PROFESIONAL DE MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN de la **UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO**, llevar a cabo **LA CAPACITACIÓN SOBRE RIESGOS DE TI CON LA FINALIDAD DE CONTINUAR CON EL DESARROLLO DE TESIS DE MAESTRÍA**, bajo los consentimientos, políticas y lineamientos de nuestra representada.

la presente se extiende a petición del interesado para los fines académicos que estime conveniente.

Chongoyape, 04 de diciembre 2023

INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO "CHONGOYAPE"
Lic. María Zulema Mendoza Copia
DIRECTORA GENERAL (e)

Directora
Lic. Zulema Mendoza Copia

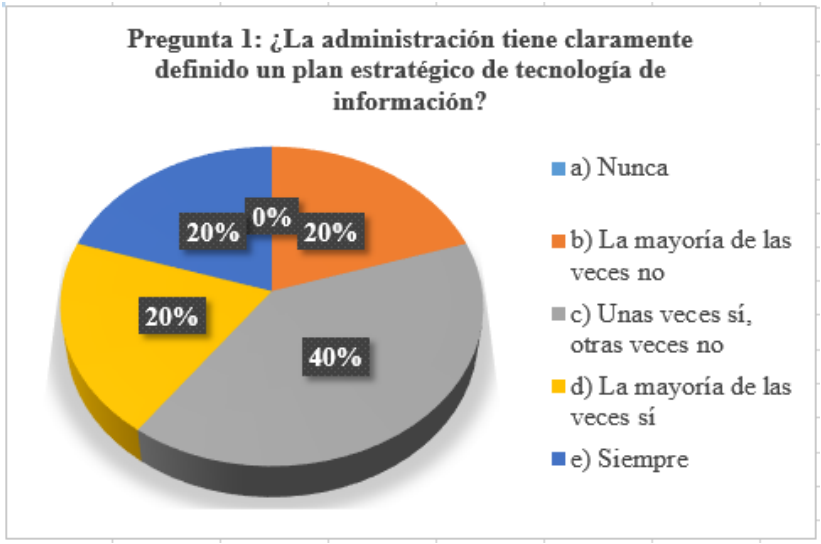
Anexo 09: Evidencias de capacitación

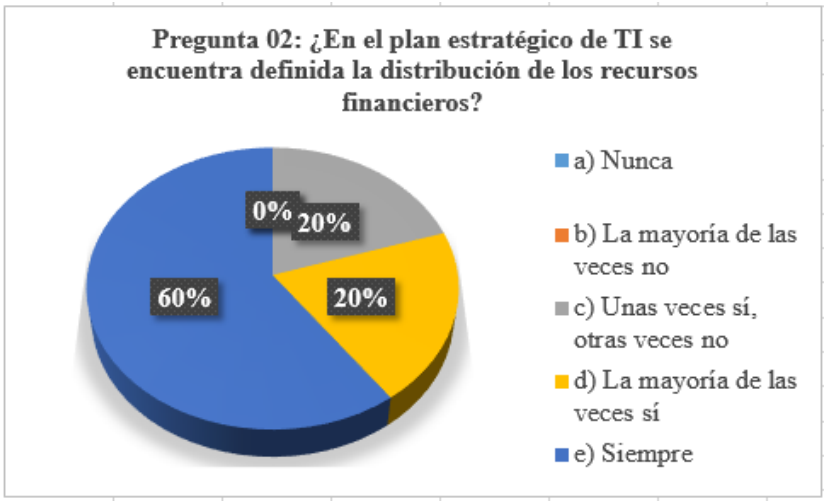


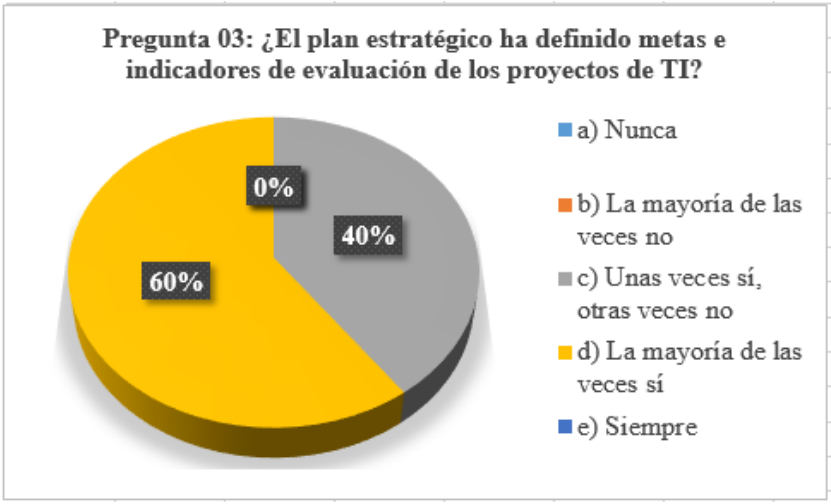


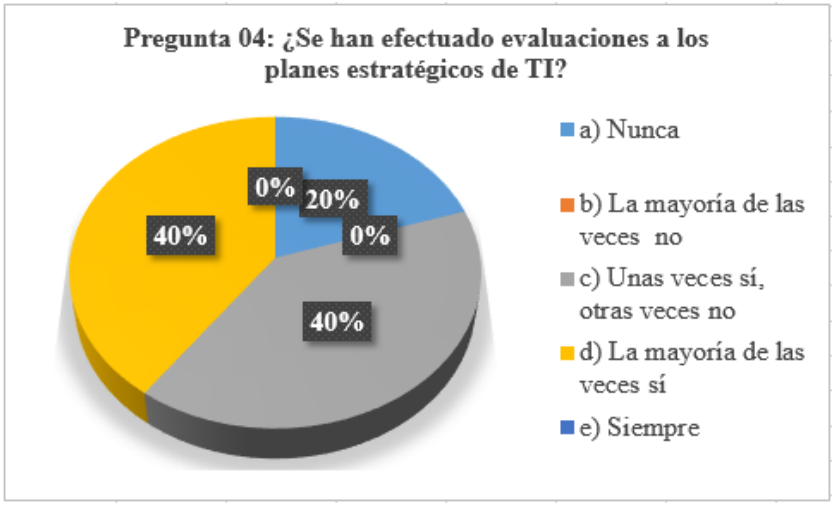


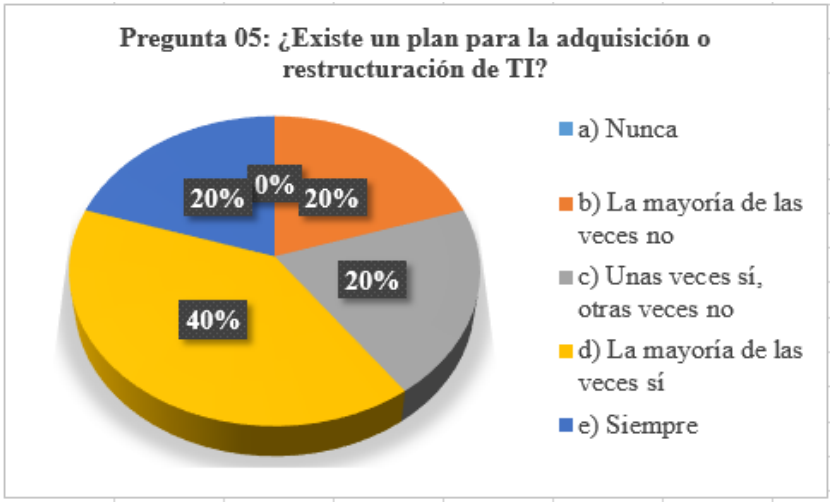

Anexo 10: Resultados de Cuestionario post test

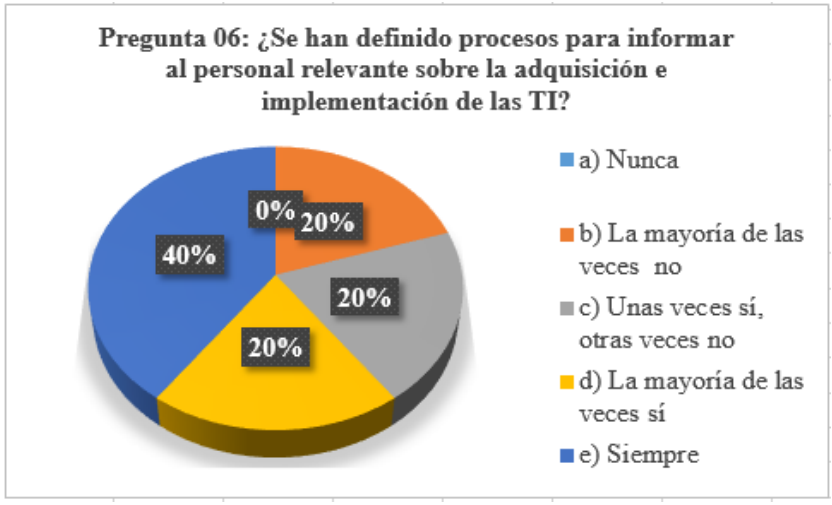


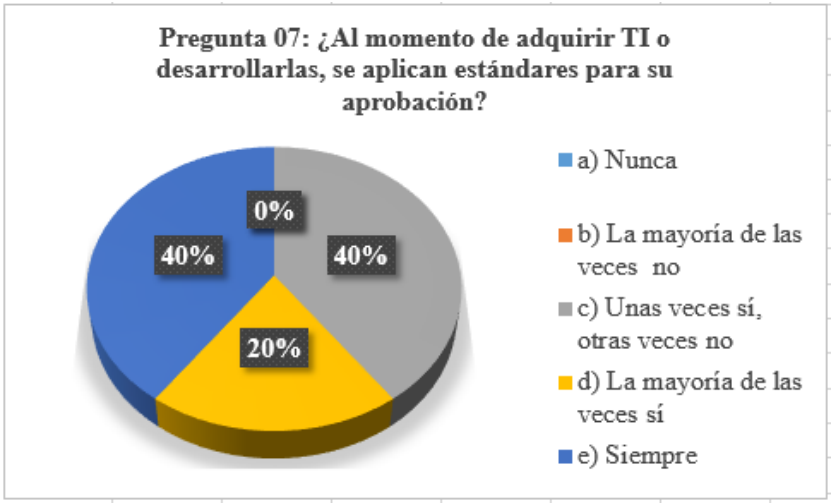


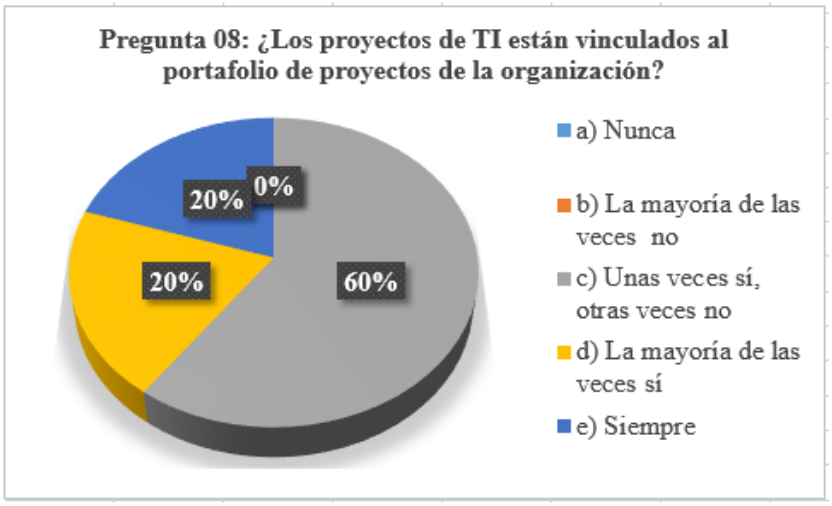


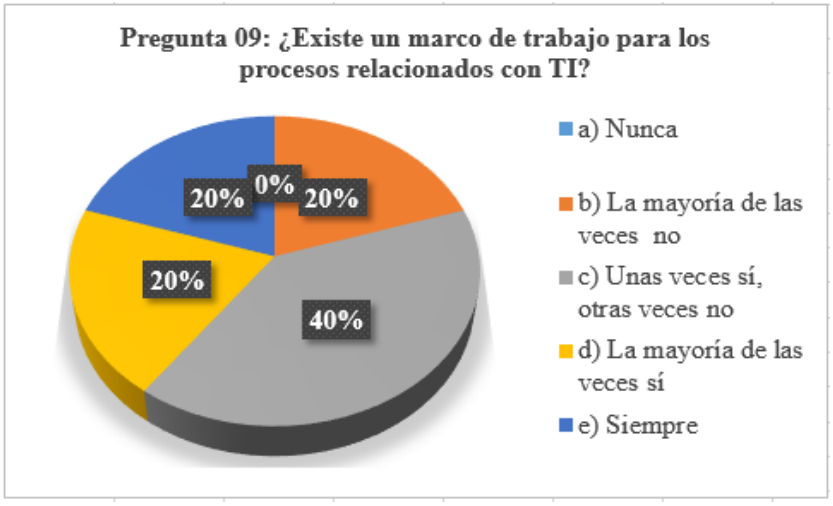

Pregunta 04: ¿Se han efectuado evaluaciones a los planes estratégicos de TI?
0%
20%
0%
40%
40%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 05: ¿Existe un plan para la adquisición o restructuración de TI?
20%
0%
20%
20%
40%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre

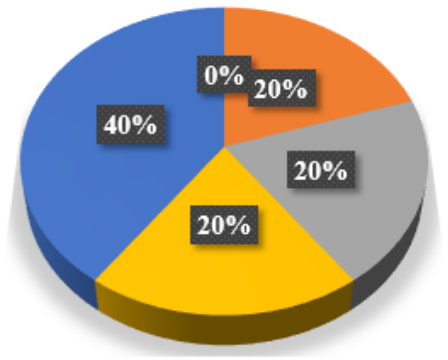

Pregunta 06: ¿Se han definido procesos para informar al personal relevante sobre la adquisición e implementación de las TI?
0%
20%
40%
20%
20%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 07: ¿Al momento de adquirir TI o desarrollarlas, se aplican estándares para su aprobación?
0%
40%
40%
20%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 08: ¿Los proyectos de TI están vinculados al portafolio de proyectos de la organización?
20%
0%
20%
60%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre

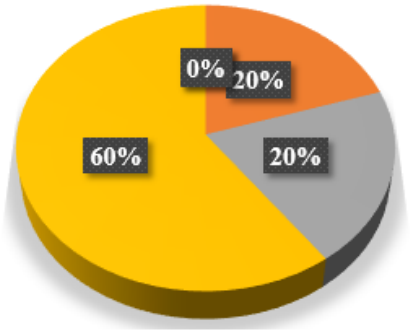

Pregunta 09: ¿Existe un marco de trabajo para los procesos relacionados con TI?
20%
0%
20%
20%
40%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre

Pregunta 10: ¿Se realiza un seguimiento a los cronogramas de actividades de los proyectos de TI?



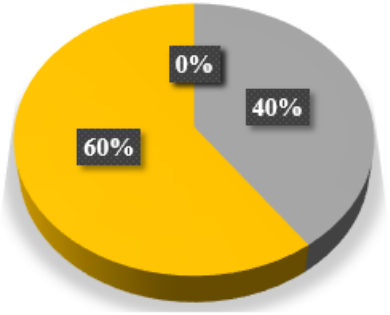
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

Pregunta 11: ¿Se han definido, planeado e implantado mediciones para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con las TI?



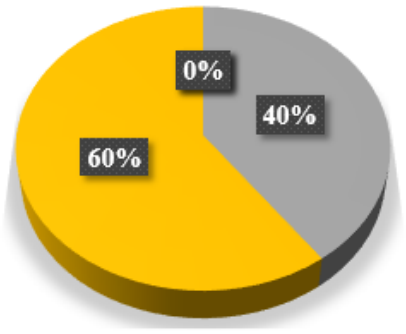
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

Pregunta 12: ¿Se han asignado prioridades y planeado las actividades identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución de control en todos los niveles para implantar las respuestas a los



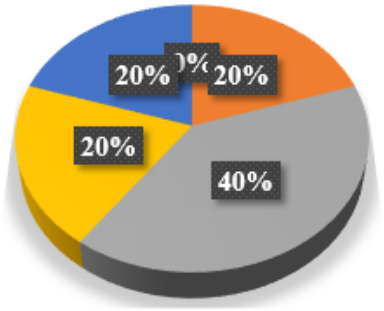
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

Pregunta 13: ¿Se documentan los inconvenientes evidenciados en la ejecución de cada uno de los proyectos de TI?



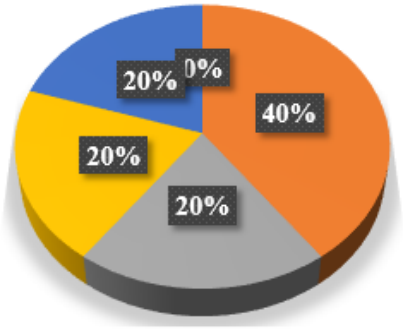
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

Pregunta 14: ¿La organización ha establecido un comité encargado del direccionamiento y asesoramiento de la incorporación de las TI a los procesos de negocio?

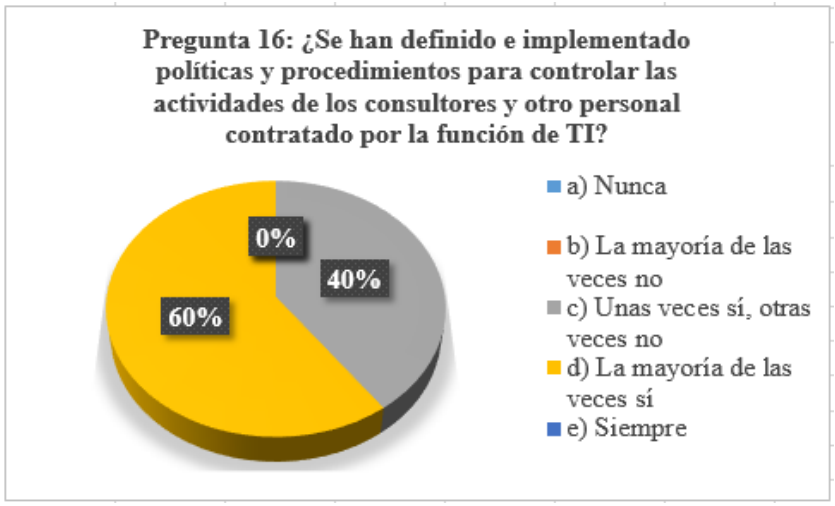


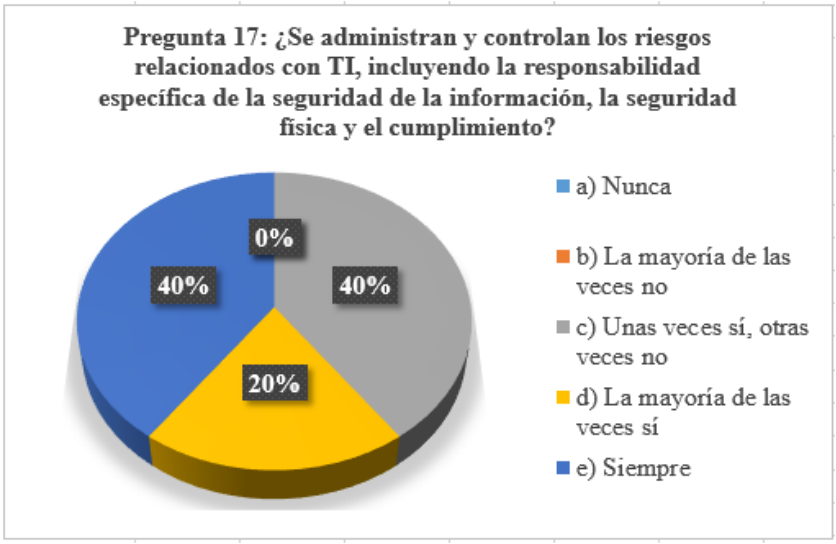
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

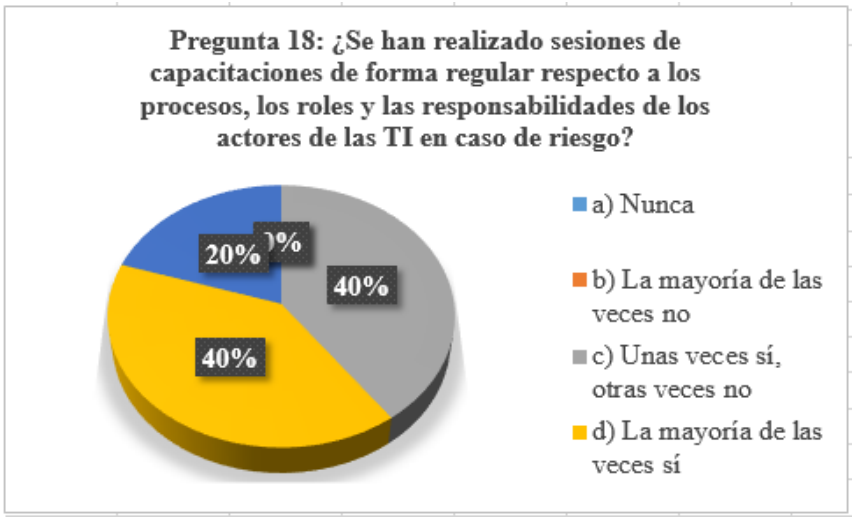
Pregunta 15: ¿Se han definido roles y responsabilidades de los actores relacionados con las TI?



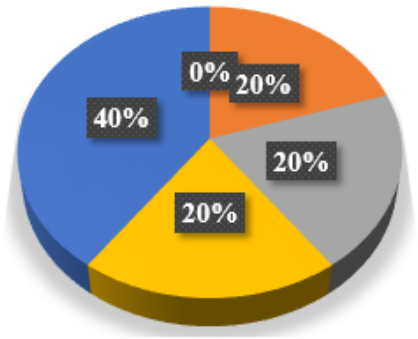
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre


Pregunta 16: ¿Se han definido e implementado políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI?
0%
40%
60%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 17: ¿Se administran y controlan los riesgos relacionados con TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento?
0%
40%
40%
20%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre

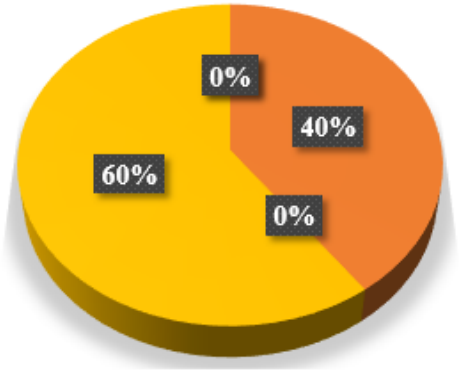

Pregunta 18: ¿Se han realizado sesiones de capacitaciones de forma regular respecto a los procesos, los roles y las responsabilidades de los actores de las TI en caso de riesgo?
20%
40%
40%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí

Pregunta 19: ¿La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear planes de seguridad de TI?



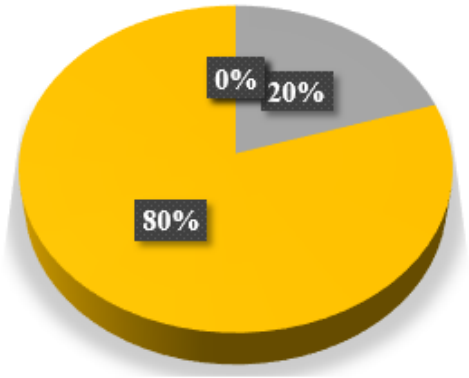
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

Pregunta 20: ¿Se realiza una adecuada transferencia de conocimiento a la gerencia?

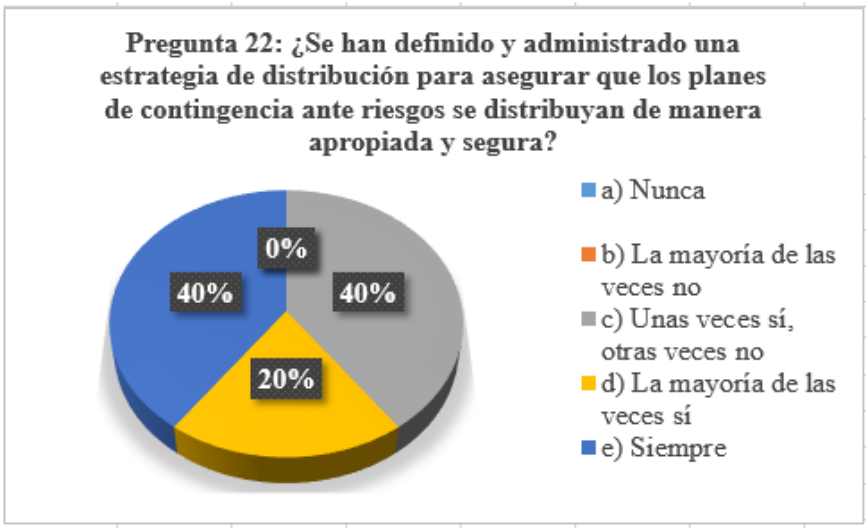


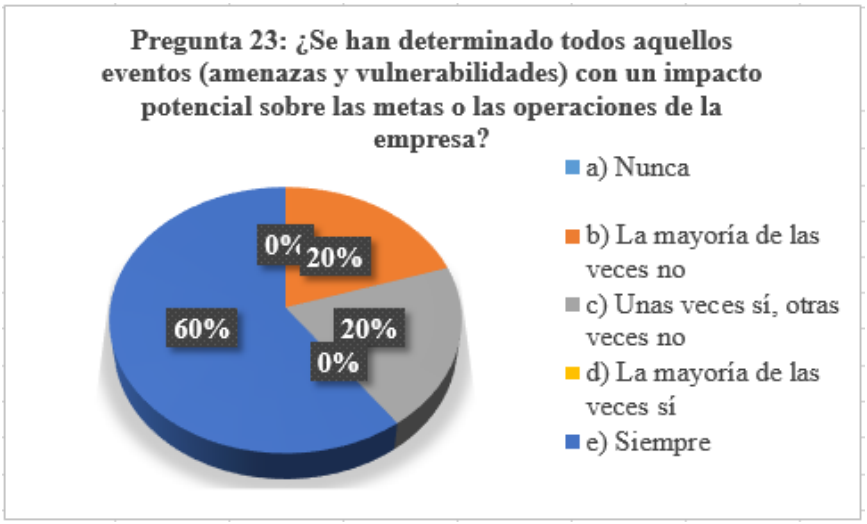
- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre

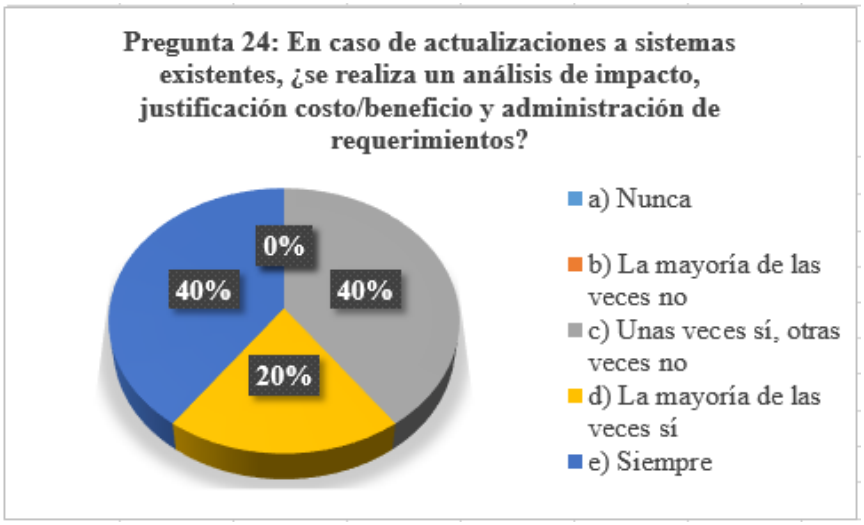
Pregunta 21: ¿Se toman medidas cuando el desempeño y la capacidad de las TI no están en el nivel requerido?



- a) Nunca
- b) La mayoría de las veces no
- c) Unas veces sí, otras veces no
- d) La mayoría de las veces sí
- e) Siempre


Pregunta 22: ¿Se han definido y administrado una estrategia de distribución para asegurar que los planes de contingencia ante riesgos se distribuyan de manera apropiada y segura?
0%
40%
40%
20%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 23: ¿Se han determinado todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa?
0%
20%
60%
20%
0%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre


Pregunta 24: En caso de actualizaciones a sistemas existentes, ¿se realiza un análisis de impacto, justificación costo/beneficio y administración de requerimientos?
0%
40%
40%
20%
a) Nunca
b) La mayoría de las veces no
c) Unas veces sí, otras veces no
d) La mayoría de las veces sí
e) Siempre