UNIVERSIDAD PERUANA UNIÓN
ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE INGENIERIA Y ARQUITECTURA

Modelo de evaluación de capacidad de procesos para el gobierno y gestión de tecnologías de información basado en COBIT 5 para una universidad privada

Tesis presentada para optar el grado académico de maestro en Ingeniería de Sistemas

Por
Lizeth Geanina Huanca López

Lima, Perú
2018

Modelo de evaluación de capacidad de procesos para el gobierno y gestión de tecnologías de información basado en COBIT 5 para una universidad privada

TESIS

Presentada para optar el Grado Académico de Maestra en Ingeniería de Sistemas con mención en Dirección y Gestión de Tecnologías de Información

JURADO DE SUSTENTACIÓN

Dra. Lili Albertina Fernández Molocho
Presidente

Dra. Erika Inés Acuña Salinas
Secretaria

Dr. Guillermo Mamani Apaza
Asesor

Mg. Sergio Omar Valladares Castillo
Vocal

Mg. Immer Elías Cuellar Rodríguez
Vocal

Lima, 23 de noviembre de 2018

ANEXO 07 DECLARACIÓN JURADA DE AUTORIA DEL INFORME DE TESIS

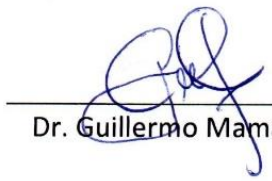
Dr. Guillermo Mamani Apaza, de la Escuela de Posgrado, Unidad de Posgrado de Ingeniería y Arquitectura, de la Universidad Peruana Unión.

DECLARO:

Que el presente informe de investigación titulado: *"Modelo de evaluación de capacidad de procesos para el gobierno y gestión de tecnologías de información basado en COBIT 5 para una universidad privada"* constituye la memoria que presenta la **Bachiller Lizeth Geanina Huanca López** para aspirar al Grado académico de Maestra en Ingeniería de Sistemas ha sido realizada en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente constancia en Lima, a los *23 días* del mes de noviembre del año 2018



Dr. Guillermo Mamani Apaza

DEDICATORIA

La presente investigación fue realizada con el propósito de proveer una herramienta que apoye a las organizaciones en su anhelo de establecer el gobierno y gestión de las tecnologías de información, especialmente en su etapa inicial, cuando se requiere evaluar el nivel en el que se encuentran los procesos de tecnologías de información con los que cuenta la empresa, estén formalizados o no.

En ese sentido, dedico este trabajo de investigación a todos aquellos profesionales de TI que deseen implementar el gobierno y gestión de tecnologías de información en sus organizaciones, esperando que lo expuesto en este documento sirva de orientación y apoyo.

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por crear la investigación y proveer de sabiduría y conocimientos a los que nos atrevemos a hacer este tipo de trabajo, sin la intervención divina sería mucho más complejo de lo que ya es, por eso agradezco a Dios por todo lo que provee para el desarrollo de nuevos conocimientos.

En segundo lugar, agradezco a mis padres, mi hijo, mis hermanas y cuñados, mi linda familia, que por mucho tiempo me alentaron y ayudaron de muchas formas a continuar y culminar esta investigación, pues constituye un logro importante en mi desarrollo profesional y laboral.

Finalmente, agradezco a mi querida Universidad, a sus administradores y colaboradores en todas las áreas y niveles, que promueven la investigación y el desarrollo profesional a través del apoyo en el estudio de programas de posgrado.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El objetivo de la investigación fue diseñar un modelo de evaluación de la capacidad de procesos de TI para el gobierno y gestión de tecnologías de información basado en las buenas prácticas de COBIT 5 para una universidad privada. La metodología utilizada consta de 4 etapas, las primeras 3 etapas tienen un resultado o entregable que forma parte del modelo propuesto, la última etapa consiste en la validación del modelo. El Modelo de Evaluación de la Capacidad de Procesos de TI propuesto consta de 3 Fases: la primera se en el alineamiento de la TI con la estrategia de la universidad, la Fase 2 identifica y describe los procesos de TI que generan valor a la universidad, y en la Fase 3 se evalúa la capacidad de los procesos de TI identificados. El modelo fue validado por juicio de expertos y aplicado al contexto de una universidad privada. Se concluye que el modelo propuesto es aplicable para el inicio del gobierno y gestión de TI adecuados en cualquier organización.

Palabras clave: Gobierno de TI, Gestión de TI, COBIT 5, Modelo de Evaluación de Procesos – PAM.

ABSTRACT

The objective of the research was to design a model for assessing the capacity of IT processes for the governance and management of information technologies based on the good practices of COBIT 5 for a private university. The methodology used consists of 4 stages, the first 3 stages have a result or deliverable that is part of the proposed model, the last stage consists in the validation of the model. The proposed IT Process Capacity Assessment Model consists of 3 Phases: the first is in the alignment of IT with the strategy of the university, Phase 2 identifies and describes the IT processes that generate value to the university, and in Phase 3, the capacity of the identified IT processes is evaluated. The model was validated by expert judgment and applied to the context of a private university. It is concluded that the proposed model is applicable for the initiation of governance and adequate IT management in any organization.

Keywords: IT Governace, IT Management, COBIT 5, Process Assessment Model - PAM

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

1.1.1. Descripción de la situación problemática

Gobernar las tecnologías de información (TI), en la actualidad, es mucho más complejo que gobernar otros activos de la empresa, debido a la presión que ejercen las diferentes áreas de la empresa buscando soluciones basadas en las tecnologías de información y a la incertidumbre que tienen los directivos sobre el valor de las tecnologías de información en contra del costo que supone para la organización. Por otro lado, la percepción de que el personal del área de TI controla el rendimiento de la organización a través de las TI en lugar de generar oportunidades de negocio es cada vez más notoria.[1]

Las organizaciones que explotan de manera exitosa las tecnologías de información son aquellas que alinean las estrategias de las TI con las estrategias del negocio, de tal manera que los objetivos, las estrategias, la táctica y la operación están clarificados entre las unidades de negocio y el área de tecnologías de información. También, cuentan con adecuadas estructuras organizativas que facilitan la implementación del gobierno de las TI construyendo relaciones con una comunicación efectiva entre los que usan las TI en la empresa y los que implementan las TI. Estas organizaciones han implementado o puesto en práctica un marco de gobierno de TI. [2]

No es usual encontrar una empresa que explote de manera exitosa las TI. Frecuentemente, se ve un distanciamiento en la comunicación entre los directivos y el personal de TI, por lo que la imagen de los directivos respecto a las TI es que siempre llegan tarde, son lentos, son caros y no son del todo convenientes.[1]

En el ámbito educativo, las instituciones de educación superior están asumiendo esfuerzos denodados para mejorar la calidad educativa basando sus procesos académicos en la innovación tecnológica, Sin embargo, la complejidad del gobierno de TI en una universidad hace difícil la realización de planes de desarrollo educativo. Zambrano & Molina mencionan que la incorporación del gobierno de TI en las universidades de todo el mundo ya alcanza una madurez del 2,30 sobre 5.[3]. Sin embargo, hace falta más divulgación y conocimiento sobre los modelos de gobierno de TI estandarizados o de buenas prácticas de gobierno aceptadas a nivel mundial. Al no contar con un modelo de Gobierno de TI dentro de la gestión universitaria, las TI han sido reconocidas a nivel técnico más no estratégico. Por tal motivo, es conveniente para toda institución de educación superior, implementar un modelo de Gobierno de TI que permita: el

alineamiento estratégico con la TI, la entrega de valor por medio de la TI, la gestión de riesgos relacionados con la TI, la gestión de los recursos relacionados con la TI y la medición del rendimiento, es decir, conocer el nivel de madurez o capacidad que tiene las tecnologías de información de la universidad.[1]

Actualmente existen modelos de gobierno de TI que pueden ser implementados en las organizaciones. Sin embargo, existe cierto grado de complejidad en la interpretación y adaptación de los modelos existentes a la realidad de las empresas. En ese sentido, es conveniente el análisis de estos modelos de gobierno de TI, para proponer formas de interpretación y adaptación al contexto de la empresa en particular. El resultado sería un modelo de gobierno de TI mejorado como una herramienta útil para la implementación del gobierno de TI y la evaluación del rendimiento en función a la capacidad de los procesos de TI en un contexto universitario.

Esta investigación está orientada a analizar el modelo de gobierno de TI propuesto por ISACA, COBIT 5. El análisis a realizar contempla los siguientes elementos de gobierno: alineación estratégica con la TI, entrega de valor y medición del rendimiento de las TI. El propósito es proveer una herramienta que apoye a las organizaciones en su anhelo de establecer el gobierno y gestión de las tecnologías de información. El resultado de este análisis se plantea como un nuevo modelo de Evaluación de la Capacidad de Procesos para el Gobierno y Gestión de las Tecnologías de Información en una universidad privada.

1.1.2. Formulación del problema

¿El diseño de un modelo de evaluación de la capacidad de procesos de TI basado en las buenas prácticas de COBIT 5 permite el gobierno y gestión de TI en una universidad privada?

1.2. Finalidad e importancia de la investigación

Toda organización, sea cual fuere su tamaño y giro de negocio, requiere de las tecnologías de información (TI) para soportar y desarrollar sus procesos de negocio, en ese sentido se espera que las TI sean verdaderos aliados que aporten con el logro de los objetivos estratégicos de la organización.[4] De acuerdo a lo expresado por ISACA, la forma cómo una organización puede obtener los resultados esperados de sus TI es gobernándolas y gestionándolas. Para esto, propone un marco de referencia que contiene buenas prácticas y promueve un adecuado uso de las TI, denominado COBIT 5. [4]

Este marco de referencia propone el gobierno y gestión de las TI por medio de procesos definidos que toda organización de TI puede implementar. De alguna u otra forma, estos procesos ya están funcionando en las empresas, sin embargo, se desconoce cuál su nivel de capacidad para luego identificar cuáles son los aspectos que se deben mejorar a fin de que las TI realmente aporten al logro de los objetivos estratégicos.

La presente investigación tiene como finalidad el desarrollo de un modelo que permita la evaluación de la capacidad de los procesos de TI que sirva como una herramienta de apoyo en un contexto para iniciar con la implementación del gobierno y gestión de TI, o de monitorear su desarrollo con el propósito de mejorar continuamente.

La importancia de esta investigación radica en el hecho de que las organizaciones necesitan que las tecnologías de información con las que cuentan sean sus aliados estratégicos en el logro de sus objetivos organizacionales y en su desarrollo en un mundo en constante cambio. En ese sentido, es muy importante conocer la manera cómo estas TI aportan a ese desarrollo, por eso se requiere alinearlas a las estrategias de la organización y evaluar su nivel de capacidad actual para identificar las mejoras sustanciales que se deben hacer para que, realmente, sean los aliados que se espera.

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Diseñar un modelo de evaluación de la capacidad de procesos de TI para el gobierno y gestión de tecnologías de información basado en las buenas prácticas de COBIT 5 para una universidad privada.

1.3.2. Objetivos específicos

a) Desarrollar la alineación entre los objetivos estratégicos de la universidad con los procesos de TI (Cascada de metas).
b) Definir un modelo de referencia de procesos de gobierno de TI que soportan los objetivos estratégicos de la universidad. (Modelo de referencia de procesos)
c) Desarrollar la caracterización formal de la evaluación de la capacidad de procesos para la universidad. (Modelo de Evaluación de Procesos – PAM)
d) Aplicar la caracterización en la evaluación de la capacidad del proceso Gestionar los servicios de seguridad en la universidad para validar su funcionamiento.

CAPÍTULO II: FUNDAMENTO TEÓRICO DE LA INVESTIGACIÓN

2.1. Antecedentes de la investigación

a) ***Diagnóstico y plan de acción para la implementación del marco de negocio para el gobierno y gestión de tecnologías de la información (COBIT 5) aplicado a la Universidad Técnica de Machala.*** Esta investigación fue realizada por Wilmer Braulio Rivas Asanza en el año 2017, para optar el grado de magíster en Gestión Estratégica de Tecnologías de la Información, otorgado por la Universidad de Cuenca del Ecuador. El objetivo fue: Definir un plan de acción de las actividades que deben desarrollarse para la implementación de procesos definidos como prioritarios con la alta gerencia luego del análisis de resultados de un diagnóstico de situación inicial basado en COBIT 5.0 para la Universidad Técnica de Machala. Luego de un análisis de la situación actual de la universidad y el área de TI, el investigador realizó un diagnóstico de la capacidad de los procesos de COBIT en la universidad en base al Modelo de Evaluación de Procesos (PAM) de COBIT 5. Para este fin diseñó un diagrama de flujo que reflejara la secuencia de actividades que se debe realizar para obtener el nivel de capacidad de los procesos de COBIT 5 en la universidad. Como primera actividad, establece los indicadores de atributo para el Nivel 1, analiza las actividades de cada práctica de gestión o práctica base de los procesos que serán evaluados, identifica que estas actividades son muy abarcantes y que no conseguiría una respuesta acertada al hacer la evaluación respecto al cumplimiento de las actividades. Por lo tanto, el investigador decide desagregar las actividades hasta un nivel en que pueda conseguir una respuesta específica respecto a si la universidad cumple o no cumple con la actividad. Con las actividades desagregadas, elabora un instrumento de evaluación para cada proceso de gobierno y gestión, este instrumento verifica el nivel de cumplimiento de las actividades propuestas por COBIT lo que permite medir la capacidad de los procesos en el Nivel 1 del PAM. La segunda actividad del diagrama de flujo consiste en la aplicación de una auditoría de cumplimiento a las partes interesadas de la universidad con el fin de evaluar la capacidad de los procesos. La actividad 3 consistió en establecer un mecanismo de valoración – ponderación, este mecanismo tiene los siguientes elementos: el número total de preguntas por práctica de gobierno o gestión, número de preguntas cuya respuesta es afirmativa “si cumple”, peso por cada pregunta, la sumatoria de las preguntas que, si cumple, el porcentaje para saber la escala de valoración del proceso. En la actividad 4, el investigador establece la escala de valoración para determinar el nivel de capacidad de los procesos, para esto

considera la escala propuesta por el PAM que especifica, si el proceso tiene un logro entre 0% y 15% significa que el proceso no ha sido alcanzado, si el proceso tiene un logro entre el 15% y 50% significa que el proceso ha sido alcanzado parcialmente, si el proceso tiene un logro entre el 50% y 85%, significa que el proceso ha sido alcanzado ampliamente, y si el proceso tiene un logro entre el 85%y 100% significa que el proceso ha sido completamente alcanzado. Luego de realizar la evaluación siguiendo el diagrama de flujo definido, el resultado es que la universidad alcanza, en promedio, un 29.75% de capacidad de los procesos evaluados, lo que significa los procesos han sido alcanzados parcialmente. Luego de evaluar la capacidad de los procesos de COBIT en la Universidad Técnica de Machala, el investigador aplicó el mecanismo de la cascada de metas para identificar cuáles son los procesos que se alinean con la estrategia de la organización, el resultado fue de 6 procesos: EDM03, APO12, APO13, BAI06, DSS04, DSS05. Siendo que ya conocía el nivel de capacidad de los procesos, el investigador definió un plan de acción para que los procesos seleccionados alcancen el nivel deseado de completamente alcanzado. Finalmente, el investigador concluye que el estudio realizado permitió a la universidad identificar el nivel de capacidad de los procesos de TI y establecer los procesos prioritarios que permiten generar proyecciones de implementación para mejorar la gestión estratégica creando valor y minimizando los riesgos. Además, añade que para obtener el nivel de capacidad de los procesos se aplicó un instrumento con una gran cantidad de preguntas por proceso, lo que generó dificultades en la aplicación, lo cual pudo originar un sesgo en los resultados obtenidos. Recomienda que se designe un tiempo adecuado para la aplicación del instrumento y antes de aplicarlo se valide su pertinencia en la organización.[5]

b) ***Modelo de gestión y gobierno de tecnologías de información en la Universidad Estatal Amazónica.*** Esta investigación fue realizada por Verónica de las Mercedes Villareal Morales en el año 2018, para optar el grado de magíster en Gerencia Informática, otorgado por la Pontificia Universidad Católica del Ecuador. El objetivo fue: Implementar un modelo de gestión y gobierno de tecnologías de información en la Universidad Estatal Amazónica. La investigación inició con el análisis situacional de la universidad por medio de la identificación de la misión, visión, el plan de desarrollo estratégico y el mapa de procesos. Esta información sirvió para la identificación de las necesidades relacionadas a tecnologías de información que tenía la universidad. El siguiente paso, fue realizar un diagnóstico de la situación actual de la Unidad de Tecnologías de Información y Comunicaciones (UTIC) de

la universidad, encargada de la gestión de TI. Este diagnóstico concluyó en: la UTIC no cuenta con un modelo de gobierno y gestión de TI, la gestión se realizaba de manera empírica. A la vez, la investigadora identificó que la UTIC tenía alineados sus actividades a los objetivos institucionales, algo que se realizó de manera empírica, pero no cubría al 100% de los objetivos de la universidad. Luego de realizado el diagnóstico de la situación actual de la universidad y el área de TI, la investigadora dio inicio al diseño del modelo de gestión y gobierno de TI, el cual se basó en las buenas prácticas de Cobit 5 y la ISO 38500 y que cuenta con siete (7) fases. En la Fase 1, se logró la aceptación de una necesidad de cambio por parte de los responsables de la UTIC así como de la máxima autoridad de la universidad. En la Fase 2, se realizó la evaluación del estado actual de la gestión y gobierno de TI por medio del mecanismo de la Cascada de Metas y el PAM de Cobit 5. El resultado de esta fase fue la identificación de 14 procesos de los 37 procesos de Cobit 5 que se alineaban con la estrategia de la universidad. Luego los 14 procesos fueron sometidos a la evaluación del PAM, cuyo resultado fue, que los 14 procesos se encontraban en el Nivel 1 Proceso ejecutado. La Fase 3, consistió en la definición de la situación esperada, en esta fase se enfatizó el diseño de una estructura organizativa para la toma de decisiones y el enfoque en la comunicación entre los miembros de la universidad. La Fase 4 consistió en la definición de los proyectos. La implementación de cada proceso alineado se convirtió en un proyecto de implementación. En la Fase 5 se definieron las métricas para asegurar la adecuada implementación de los procesos. La Fase 6, consistió en la definición de un mecanismo de supervisión de beneficios el cual se logró por medio de un Sistema de manejo de cartera de proyectos. La Fase 7, consistió en la definición de un mecanismo de monitoreo y evaluación de los procesos de TI en desarrollo. La investigadora llega a las siguientes conclusiones: el modelo de gestión y gobierno de tecnologías de información para la universidad, permitió el alineamiento de las tecnologías de información a los objetivos institucionales, con esto se garantiza que la UTIC orienta sus estrategias para crear valor para la universidad en estudio. [6]

c) ***Diseño de un marco referencial de gobierno de TI basado en COBIT para instituciones educativas K-12 radicadas en el Ecuador.*** Esta investigación fue realizada por Ana Cristina Lozano Moreno y Juan David Ultreras Jácome en el año 2014, para optar el grado de magíster en Gerencia de Sistemas y Tecnologías de la Información, otorgado por la Universidad de las Américas. Las Instituciones Educativas K-12 del Ecuador se diferencian

por tener una acreditación internacional otorgada por AdvencED que define lineamientos y expectativas que este grupo de instituciones deben cumplir. Por otro lado, este tipo de instituciones educativas ofrecen una currícula de bachillerato internacional avalado por la International Baccalaureate, quien establece normas fundamentales para los programas de bachillerato internacional. Adicional a todo esto, las Instituciones Educativas K-12 están sujetas a los reglamentos y decretos oficiales emitidos por el Ministerio de Educación del Ecuador. Los investigadores necesitaban unificar todas estas normas, lineamientos, reglamentos entre otros, en un perfil de criterios integrados que las instituciones de este tipo deben cumplir. Para esto utilizaron la herramienta Matriz de Coherencia que les permitió unificar los diferentes criterios y establecer los objetivos estratégicos, políticas y estrategias que las instituciones de este tipo deben considerar. El Marco Referencial de Gobierno de TI que los investigadores proponen considera estas estrategias para iniciar con el alineamiento de las TI a la estrategia a través del mecanismo de la Cascada de Metas. En el primer nivel de la cascada relacionaron las estrategias identificadas con las Metas Corporativas de COBIT 5, en los siguientes niveles aplicaron las actividades que el mecanismo propone. Los procesos de COBIT considerados críticos para alcanzar las estrategias de las instituciones K-12 fueron: EDM02, APO01, APO02, APO04, APO08, BAI05. Cada uno de estos procesos fue estudiado y adaptado a la realidad de la organización. Posteriormente, los investigadores establecieron prerrequisitos que las instituciones interesadas en aplicar el marco referencial de gobierno de TI deberían cumplir. Luego, diseñaron el formato de evaluación técnica de la situación actual de los procesos seleccionados considerando lo establecido por el PAM. Este formato contiene la evaluación de los Resultados, las Prácticas base y los Productos de trabajo de cada uno de los procesos según se definen para el Nivel 1 del PAM. De los 6 procesos seleccionados 5 de ellos alcanzaron el Nivel 0, lo que significa que el proceso no se ejecuta o no logra su propósito, no existe o hay muy poca evidencia de algún logro sistemático del propósito. El único proceso que alcanzó el Nivel 1 fue el BAI05, logrando un nivel de ampliamente alcanzado. El Marco Referencial también estipula que se debe determinar la situación deseada de los procesos, los investigadores establecieron que los procesos seleccionados deberían alcanzar al Nivel 1 con un logro de ampliamente alcanzado ubicando el nivel de cumplimiento entre el 50% y 85%. Finalmente, para alcanzar el nivel deseado, los investigadores propusieron un plan de mejora de los procesos que incluyen acciones para cada uno de los procesos seleccionados. Las conclusiones de esta investigación son que el Marco Referencial de Gobierno de TI basado

en COBIT 5 para las Instituciones Educativas K-12 define una serie de lineamientos base que pueden ser adaptados a cada escenario institucional con el fin de obtener mayores beneficios reduciendo los riesgos y costos. Además, se concluye que la implementación del marco referencial requiere de seguir una secuencia definida de etapas y actividades que contemplen el cumplimiento del ciclo de vida del proceso de mejora continua. Por último, se considera que el nivel de detalle de cada proceso requiere de un análisis de acuerdo a las necesidades y expectativas institucionales.[7]

d) ***Modelo para la definición e implementación de procesos de gobierno de tecnologías de la información aplicado a CENIT Transporte y Logística de Hidrocarburos S.A.S.*** Esta investigación fue realizada por Andrea Paola Páez Ruiz y Fredy Vivas Hernández en el año 2015, para optar el grado de magíster en Dirección, otorgado por la Universidad del Rosario, Bogotá - Colombia. El objetivo fue: Proponer un modelo para la definición e implementación de procesos de gobierno de tecnologías de la información que permita cumplir con los requisitos del gobierno corporativo y fortalecer las capacidades de los procesos de tecnología que apalancan la estrategia de CENIT. La investigación se realizó en la empresa CENIT, que es la principal compañía orientada al transporte, logística y almacenamiento de hidrocarburos de Colombia. Fue fundada en el 2012 y forma parte del grupo empresarial Ecopretol S.A. Los investigadores desarrollan la investigación en 5 fases. En la fase 1, definen el diseño de la investigación identificando el problema, los objetivos, los resultados de la investigación y la justificación. En la fase 2, realizan una revisión de la literatura especializadas que se relaciona con el problema o tema de investigación. Al finalizar esta fase, concluyen que basarán su investigación en las buenas prácticas de COBIT 5 y la ISO 38500. En la fase 3, realizan un análisis de la situación actual del área de TI respecto a una guía corporativa proporcionada por Ecopetrol. Verificaron el nivel de cumplimiento y alineación del área de TI con la guía corporativa. El nivel de cumplimiento general alcanzado fue del 71%. Sin embargo, se identificaron oportunidades de mejora en aspectos relacionados con la estrategia, arquitectura empresarial y procesos. Para identificar la relación de los procesos de COBIT con las oportunidades de mejora, los investigadores decidieron evaluar el nivel de capacidad de 33 de los 37 procesos de COBIT 5 para luego establecer un nivel de capacidad objetivo teniendo en cuenta la estrategia de la organización. Para la evaluación de la capacidad de los procesos seleccionados utilizaron la Guía de Autoevaluación de COBIT 5. En la fase 4 diseñan el modelo para la definición e

implementación de procesos de gobierno de tecnologías de la información. Este modelo consta de 4 componentes: foco de análisis, nivel de madurez, matriz y brechas. El foco de análisis es la base estratégica que servirá para la valoración, clasificación y priorización de los procesos de COBIT. Para establecer la base estratégica se consideran la situación actual de la organización y sus oportunidades de mejora. El nivel de madurez permite establecer la situación actual de la organización respecto a los procesos y prácticas de COBIT, utilizando el Modelo de Evaluación de Procesos (PAM). Luego, se definen el nivel de madurez objetivo considerando la estrategia de la organización. La matriz de procesos permite la clasificación de los procesos de COBIT en 3 dimensiones, basándose en su nivel de importancia para el área de TI y su nivel de aporte al foco de análisis y el nivel de esfuerzo requerido para su implementación. El componente brechas permite la identificación de las brechas existentes en las salidas de las prácticas de gestión (documentos de trabajo) y los entregables que la organización maneja de forma interna. Finalmente, la fase 5 corresponde a la aplicación del modelo y valoración de los resultados obtenidos. Los investigadores concluyen que esta investigación permitió establecer un conjunto de buenas prácticas que ayudan al mejoramiento de las actividades que realiza toda área de TI, con el propósito de establecer el gobierno de TI con bases sólidas. Además, el modelo permitió la creación de una herramienta que fue usada para realizar el análisis y evaluación integral de los procesos teniendo en cuenta el foco de análisis relacionado con el gobierno de TI. Esta herramienta de análisis y evaluación se basa en el PAM, que fue aplicado de forma adecuada según lo explica el COBIT 5.[8]

e) ***Evolución de un modelo de gobernabilidad empresarial de TI en una empresa líder del sector agroindustrial***. Esta investigación fue realizada por Elsa Julia Mazo Arteaga en el año 2014, para optar el grado de magíster otorgado por la Escuela Colombiana de Ingeniería Julio Garavito de Bogotá – Colombia. El objetivo fue: Diseñar un modelo de Gobierno de TI que le permita a la organización de TI de la empresa, alcanzar el nivel 1: Proceso Ejecutado en la capacidad del proceso Establecimiento y Mantenimiento del Marco de Gobierno de TI. La investigación se desarrolló en una empresa agroindustrial colombiana. La investigadora aplicó el mecanismo de la cascada de metas para identificar los procesos de COBIT que se alinean a la estrategia de la empresa. De acuerdo al objetivo de la investigación, se enfocó en el proceso EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno, sobre el cual realizó la evaluación para identificar el

estado actual de la capacidad del proceso aplicando el Modelo de Evaluación de Procesos (PAM) del COBIT 5. El resultado alcanzado respecto a la capacidad del proceso fue del 12%, lo que significa que el proceso no ha logrado su propósito. En función a este resultado, la investigadora propone que el proceso debe alcanzar un estado deseable del 86%, lo que significa que el proceso está completamente logrado. Para esto, se plantearon acciones para cumplir con cada una de las prácticas de gobierno que el proceso tiene. Luego de implementar algunas de las acciones, se realizó una nueva evaluación de la capacidad del proceso, alcanzando un 63% lo que significa que el proceso está ampliamente logrado y que las acciones planteadas son las adecuadas para lograr la máxima capacidad del proceso. Finalmente, la investigadora concluye que la empresa agroindustrial donde realizó la investigación tiene el camino establecido para la implementación de un gobierno de TI alineado a la estrategia corporativa. Además, concluye que se definieron herramientas que permiten el análisis y la implementación de los demás procesos de gobierno y gestión de TI para la empresa. Sin embargo, cabe resaltar que el Modelo de Evaluación de Procesos que COBIT 5 ha definido para la evaluación de sus procesos, no fue aplicado en su totalidad o de forma conveniente, lo que sugiere que la evaluación de la capacidad del proceso estudiado no cumple con los requisitos que el modelo propone.[9]

2.2. Marco teórico

2.2.1. Introducción

Hoy en día todas las organizaciones, sin lugar a distinción, dependen de las tecnologías de información (TI) para su funcionamiento y desarrollo. Esta tecnología ha pasado de ser un instrumento operativo a convertirse en una herramienta estratégica. Por tal motivo, las empresas hacen enormes esfuerzos e inversiones en adquisiciones de TI con la idea de ser más eficientes, de cumplir con sus objetivos organizacionales y de estar protegidas y seguras.

Sin embargo, el problema persistente es que en las empresas existen tecnologías de información que funcionan de manera aislada e independiente y que se convierten en herramientas que hacen poco o nada para alcanzar el objetivo estratégico institucional haciéndose evidente la pobre alineación estratégica entre las TI y el gobierno corporativo.

Para entender la importancia del gobierno de TI es necesario comprender qué es el gobierno corporativo y cuál es su alcance, pues en esta práctica empresarial se definen los mecanismos y estructuras organizativas sobre las cuales se establecen las relaciones empresariales, los objetivos organizacionales y la dirección que tomará la empresa.

Cuando la organización tiene claro y bien definidos los objetivos estratégicos y el rumbo que seguirá entonces se puede establecer el gobierno de TI, lo que Carmona [10] define como el alineamiento de las estrategias de negocio y las tecnologías de información de manera eficaz y eficiente, de tal forma que las TI apoyen el cumplimiento de las metas y los objetivos estratégicos de las organizaciones.

Para tener un buen gobierno de las TI es necesario la aplicación de modelos de referencia existentes, probados y aceptados a nivel mundial. COBIT es un modelo de gobierno de TI que ha sido perfeccionado en el tiempo, llegando a su última versión, el COBIT 5. Este modelo provee un mecanismo para la alineación de los objetivos organizacionales con las tecnologías de información denominado Cascada de Metas que nos lleva a identificar los procesos de TI que se requieren implementar para alcanzar los objetivos estratégicos. La descripción de los procesos, sus elementos, prácticas y demás información están contenidos en el Modelo de Referencia de Procesos.[4]

Un aporte importante del modelo de gobierno de TI de COBIT es el Modelo de Evaluación de Procesos (PAM), pues permite medir el nivel de capacidad que tienen los procesos de TI en la organización para luego establecer las acciones que nos llevarán a la mejora del proceso y al logro de los objetivos empresariales.[11]

2.2.2. Gobierno corporativo y gobierno de TI

2.2.2.1. Gobierno corporativo

El gobierno corporativo es una forma de trabajo que se está fortaleciendo en las organizaciones modernas, establece mecanismos que regulan las relaciones entre los diferentes actores de la organización. Se aplica a todas las empresas sin importar el tipo o el alcance que tengan. Se lo define como el sistema por el cual las organizaciones son dirigidas y controladas. Su estructura especifica la distribución de los derechos y responsabilidades entre los diferentes participantes de la empresa: el directorio, los gerentes, los accionistas y los agentes económicos que tienen interés en la empresa. El gobierno corporativo provee las bases para el establecimiento de los objetivos empresariales, los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento a su desempeño.[12]

Para la Asociación de Auditoría y Control de Sistemas de Información (ISACA), asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información, el gobierno corporativo asegura que se evalúan las necesidades, condiciones y opciones de las partes

interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.[4]

En el ámbito de la educación superior, los investigadores [13] explican que el gobierno corporativo presenta connotaciones específicas que serán determinantes a la hora de evaluar la organización y las buenas prácticas desarrolladas. Las instituciones de educación superior deben responder a los nuevos requerimientos de las empresas y del entorno. Citando el Informe Lambert, expresan que el modelo de gobierno corporativo en las universidades se basa en el adoptado por las empresas. Según este modelo, las universidades deben estar dirigidas por profesionales con experiencia en la fijación de políticas corporativas, en la planificación de estrategias y con capacidad de dirigir y gestionar. La estructura de gobierno corporativo puede proporcionar una herramienta eficaz para que las instituciones de educación superior puedan implantar mecanismos de control y de rendición de cuentas, planifiquen su gestión a largo plazo, delimiten la misión y visión estratégica de la institución, construyan indicadores claves de rendimiento y eficiencia, establezcan sus presupuestos anuales y cumplan con los intereses de los diversos grupos de interés. Sin embargo, como en todas las organizaciones, alcanzar este ideal requiere del apoyo de las Tecnologías de Información (TI) como una plataforma que provee el soporte tecnológico para la toma de decisiones estratégica a nivel del gobierno corporativo.

La Organización para la Cooperación y el Desarrollo Económico (OCDE), ha establecido seis Principios de Gobierno Corporativo que tienen el propósito de proporcionar un marco de referencia identificando los cimientos de un buen gobierno corporativo y la orientación práctica para su aplicación a nivel nacional e internacional [14]. Estos principios se aplican a todo tipo de empresa, privada o pública, pues se asientan sobre elementos comunes y abarcan los diferentes modelos de gobierno existentes. A continuación, mencionamos los principios:

- *Principio 1*: *Consolidación de la base para un marco eficaz de gobierno corporativo. De acuerdo a este principio, el gobierno corporativo promueve la transparencia y la equidad de los mercados, y la asignación eficiente de los recursos. Será coherente con el Estado de Derecho y respaldará una supervisión y una ejecución eficaces*.[14]
- *Principio 2*: *Derechos y tratamiento equitativo de los accionistas y funciones de propiedad clave. El gobierno corporativo protege y facilita el ejercicio de los derechos de los accionistas y garantiza el trato equitativo a todos ellos, incluidos los minoritarios y los*

extranjeros. Todos tendrán la posibilidad de que se reparen de forma eficaz las violaciones de sus derechos.[14]

- *Principio 3: Inversores institucionales, mercados de valores y otros intermediarios. El gobierno corporativo proporciona incentivos sólidos a lo largo de toda la cadena de inversión y facilitar que los mercados de valores funcionen de forma que contribuya al buen gobierno corporativo.[14]*
- *Principio 4: El papel de los actores interesados en el ámbito del gobierno corporativo. El gobierno corporativo reconoce los derechos de los actores interesados que disponga el ordenamiento jurídico o se estipulen de mutuo acuerdo y fomenta la cooperación activa entre éstos y las sociedades con vistas a la creación de riqueza y empleo, y a la sostenibilidad de empresas sólidas desde el punto de vista financiero.[14]*
- *Principio 5: Divulgación de información y transparencia. El gobierno corporativo garantiza la comunicación oportuna y precisa de todas las cuestiones relevantes relativas a la empresa, incluida la situación financiera, los resultados, la propiedad y sus órganos de gobierno.[14]*
- *Principio 6: Las responsabilidades del consejo de administración. El gobierno corporativo garantiza la orientación estratégica de la empresa, el control efectivo de la dirección por parte del Consejo y la rendición de cuentas ante la empresa y los accionistas.[14]*

La consolidación del gobierno corporativo en una empresa será posible si cuenta con los recursos adecuados para la implementación de algún modelo de gobierno y de los principios de la OCDE. Entre los recursos necesarios se encuentran las tecnologías de información (TI), cuya influencia en las organizaciones de hoy se ha vuelto estratégica. Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como una parte importante dentro del negocio. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno corporativo y la gestión [4]. En este sentido, el éxito de un gobierno corporativo se soporta en la eficiencia y eficacia con que se gobiernan las tecnologías de información.

2.2.2.2. Gobierno de las TI

En la actualidad, el activo más importante de una organización es la información, por lo tanto, debe ser gestionada y protegida apropiadamente.[4] La tecnología que permite gestionar y proteger la información se denomina Tecnologías de Información (TI) y está compuesta por el conjunto de dispositivos electrónicos que permiten almacenar, procesar, distribuir y

visualizar la información. El gobierno corporativo se basa en la calidad de información sobre la cual toma decisiones. Los beneficios económicos, sociales, culturales, y de cualquier índole, que una organización alcanza son el resultado de la toma de decisiones bien informada.[15] La información es un recurso clave para todas las empresas y desde el momento en que se crea hasta que es destruida, la tecnología desempeña un papel importante.[4] En este sentido, según lo explica ISACA, en la actualidad, las empresas se esfuerzan por:

- Mantener información de alta calidad para soportar las decisiones del negocio.
- Generar valor al negocio con las inversiones en TI
- Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- Mantener los riesgos relacionados con TI en un nivel aceptable
- Optimizar el coste de los servicios y tecnologías de TI
- Cumplir con las leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Por lo tanto, las TI se convierten en un elemento importante en el gobierno corporativo de las organizaciones, por lo que deberían ser gobernadas con el fin de alinearse a los objetivos estratégicos de la empresa. Esto implica que los directivos deben establecer un buen sistema de gobierno de TI basado en una planificación estratégica e integral de las tecnologías de información de manera alineada con los objetivos globales de la organización. [16].

El gobierno de TI se define como el alineamiento de las estrategias de negocio y las tecnologías de información de manera eficaz y eficiente, de tal forma que las TI apoyen el cumplimiento de las metas y los objetivos estratégicos de las organizaciones [10].

Por otro lado, ISACA define el gobierno de TI como el aseguramiento de que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En el ámbito de la educación superior, [16] las TI tienen un carácter estratégico y su alcance es a toda la organización, por lo que deben formar parte de la planificación global de la universidad y las principales responsabilidades relacionadas con el gobierno de las TI deben recaer y ser apoyadas directamente por la alta dirección universitaria. Un uso más académico de las TI es el que Nakako [17], explica al decir que las TI favorecen el fortalecimiento de lazos institucionales y académicos pues facilitan la comunicación, el intercambio de información y mejores prácticas, al igual que ofrecen oportunidades de aprendizaje intercultural. Además, a

través del ofrecimiento de oportunidades y recursos educativos de forma remota se posibilita acceder a mayor diversidad de estudiantes y grupos en desventaja, ampliando el mercado educativo. A la par, estos medios permiten atraer a docentes e investigadores extranjeros sin movilizarlos físicamente.

En la actualidad, las instituciones de educación superior se esfuerzan por lograr la integración de las TI a los procesos de la organización. En su investigación, Nakako [17] identifica dos aspectos importantes que se vinculan a este esfuerzo: a) el reconocimiento, por parte de los directivos universitarios, de que la correcta integración de las TI es un componente esencial para fortalecer la calidad de la educación y afrontar los retos científicos, económicos, tecnológicos y sociales que se presenten, y; b) el proceso de implementación de las TI presenta una serie de barreras, que al no ser superadas, impiden una integración exitosa. Además, presenta cuales podrían ser las barreras en la integración de las TI en las universidades:

- *Desconocimiento sobre las TI. Existe un conocimiento limitado y vago sobre las TI, se las ve como una tecnología avanzada que requiere un alto nivel de experticia, mucho dinero y capacidades complejas. No se las aprecia como recursos que, bajo un enfoque de costo-beneficio, propician acciones eficientes. Esta situación se debe a que los tomadores de decisiones creen saber cuáles son las prioridades para la organización y qué TI brindará mayores beneficios. Se debería considerar que las TI por si mismas proporcionan poco o nada a la organización, más bien, es su rol mediador para la transformación y las oportunidades la que crea un cambio o mejora en el gobierno de la organización. Por ello, se hace necesario identificar los retos de la organización y cómo estos pueden ser cubiertos por medio de un uso efectivo de las TI.[17]*
- *Bajo o nulo involucramiento de las autoridades. Las grandes transformaciones e innovaciones en la organización requieren del involucramiento y compromiso de quienes toman las decisiones.[17]*
- *Definición del rol estratégico de las TI. Una correcta implementación de las TI debe seguir el enfoque de la misión, visión y objetivos estratégicos de la organización, con el fin de facilitar la realización de dichos objetivos. En ese sentido, definir una ruta de guía clara es un requisito previo.[17]*
- *Establecimiento de un proceso sistemático de implementación de las TI. Se debe contar con un plan estratégico de incorporación de las TI. Además de un sistema de seguimiento y monitoreo, e información de la gestión y sus resultados. [17]*

- *Sostenibilidad. La inversión económica que requiere la incorporación de las TI se debe evaluar desde una perspectiva de sostenibilidad. Las soluciones tecnológicas deben asegurar eficiencia y ser sostenibles en el tiempo.[17]*
- *Política institucional sobre las TIC. Se debe establecer los parámetros sobre los cuales se incorporarán las TI en la organización, y cómo deben interactuar las instancias encargadas y los flujos en la toma de decisiones.[17]*

Para superar estas barreras y lograr una adecuada integración de las TI a la organización y establecer un adecuado sistema de gobierno de TI, todas las universidades deberían: [17]

- *Establecer claramente cuál es su estrategia de TI y alinearla con la estrategia global de la universidad.*
- *Determinar quiénes son los responsables de la planificación estratégica de las TI, de la toma de decisiones y de la explotación de las TI.*
- *Establecer una gestión por proyectos y priorizar las inversiones, de manera que se ahorren costes.*
- *Gestionar los riesgos para conseguir que cada vez afecten menos al rendimiento de la universidad.*
- *Disponer, en todo momento, de una evaluación y seguimiento del rendimiento de los procesos y servicios basados en TI mediante los indicadores adecuados (cuadro de mandos de TI).*
- *Alcanzar el cumplimiento normativo e implantar estándares internacionales y certificaciones relacionadas con el gobierno de las TI.*

Existen varios modelos, estándares y marcos de referencia que apoyan la implementación del gobierno y la gestión de TI por medio de diferentes áreas, cada uno de estos se basan en diferentes aspectos como se puede observar en la Figura 1. Las principales áreas en que las TI debe ser gobernada y gestionada son: proyectos de TI, seguridad de la Información, servicios de TI, infraestructura tecnológica, riesgos de TI, auditorías de TI, entre otras. El marco de referencia Objetivos de Control para la Información y Tecnología Relacionada - COBIT por sus siglas en inglés, está orientado al Gobierno de las TI y cubre todas las áreas mencionadas. A continuación, profundizaremos el estudio sobre este marco de referencia.

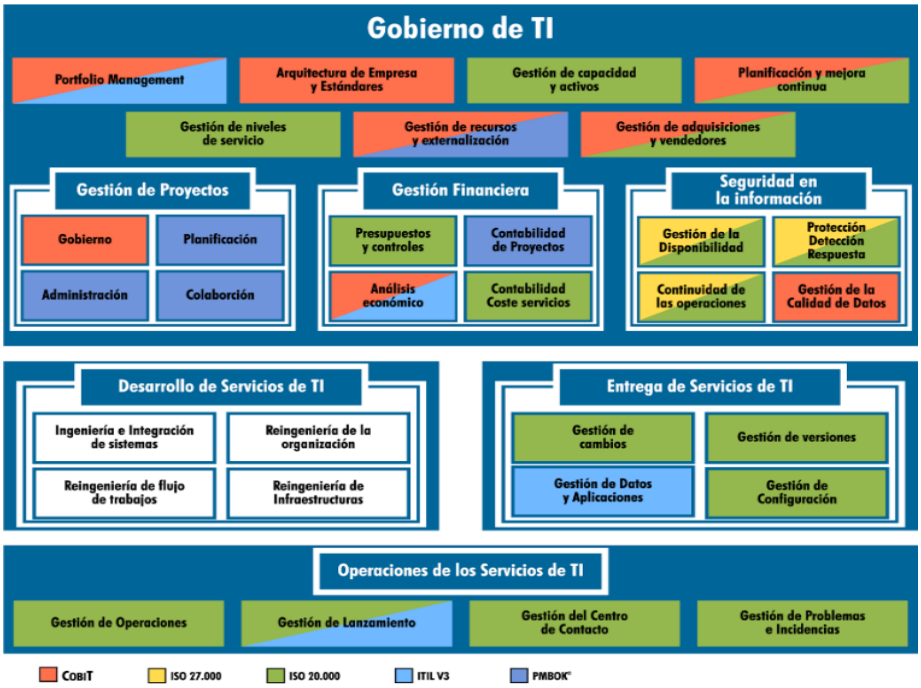


Figura 1 - Modelos, estándares y marcos de referencia para la implementación del gobierno y gestión de TI.

2.2.3. Marco de referencia COBIT 5

COBIT es el acrónimo de Control Objectives for Information and Related Technology, en español Objetivos de Control para la Información y Tecnología Relacionada. Es un marco de referencia que describe las mejores prácticas que las empresas pueden utilizar para gestionar la información por medio de las tecnologías de información y los riesgos que conllevan. [4]

La IT Governance Institute (ITGI) y la Information, Systems Audit and Control Associations (ISACA) son las encargadas de proveer las normas y guías que contiene. Fue publicado por primera vez en el año 1996 y ha sido actualizado hasta llegar a su última versión, COBIT 5 publicada en abril de 2012.

COBIT 5 provee la guía de nueva generación de ISACA para el gobierno y la gestión de las TI en la empresa. Es el resultado de más de 15 años de uso práctico y aplicación de COBIT por parte de muchas empresas y usuarios en ámbitos de negocio, TI, riesgo, seguridad y aseguramiento. [4]

Los beneficios de COBIT 5 para las empresas se resumen en:

- Provee un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI.
- Ayuda a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

- Permite a las TI ser gobernadas y gestionadas de un modo holístico, abarcando al negocio de principio a fin y las áreas funcionales de responsabilidad de TI.

COBIT 5 se basa en cinco principios clave para el gobierno y gestión de las tecnologías de información, estos principios se visualizan en la Figura 2.

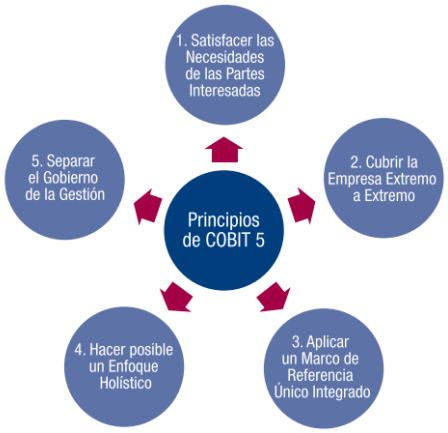


Figura 2 - Principios de COBIT 5

En el **Principio 1 - Satisfacer las necesidades de las partes interesadas**, este principio establece que las organizaciones de TI deben crear valor para sus partes interesadas. Esto significa que se existe equilibrio entre la realización de beneficios a un costo aceptable, la optimización de riesgos y el uso de recursos. Los beneficios, el valor percibido por la organización, pueden ser económicos para empresas privadas o de servicio público para organizaciones gubernamentales. Con este propósito, COBIT 5 provee procesos y otros elementos que permiten la creación de valor mediante el uso de la TI.[4]

Para identificar los procesos que permiten la creación de valor para una organización, COBIT 5 propone el mecanismo de la Cascada de Metas como una herramienta de análisis. La descripción de esta herramienta es presentada en los siguientes apartados.

En el **Principio 2 - Cubrir la empresa de extremo a extremo**, este principio establece que el gobierno y gestión de la TI se integran al gobierno corporativo. Es decir, cubre todas las funciones y procesos del negocio, no se enfoca solo en la función de TI, para lograr esto considera que los elementos relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa. Además, proporciona una visión integral y sistémica del gobierno y gestión de TI de la empresa basada en catalizadores (Ver Principio 4). El enfoque de gobierno de extremo a extremo se representa en la Figura 3, mostrando los componentes clave de un sistema de gobierno.[4]

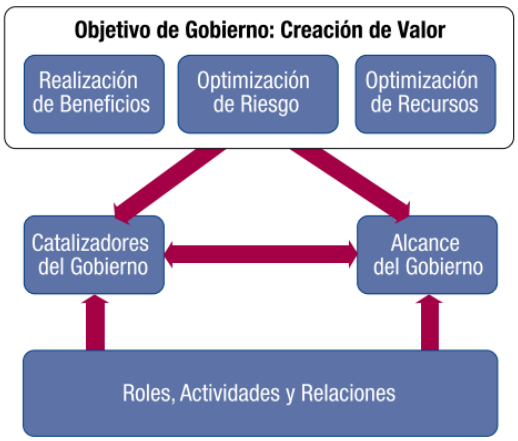


Figura 3 - Componentes clave de un sistema de gobierno

Los catalizadores de gobierno son: a) los recursos organizativos: marcos de referencia, principios, estructuras, procesos y prácticas, por medio de los cuales los objetivos estratégicos pueden ser alcanzados; b) los recursos corporativos: capacidades de servicios (infraestructura de TI, aplicaciones, etc.), personas e información. La falta de estos catalizadores puede afectar a la empresa en la creación de valor.[4]

De acuerdo a lo descrito en COBIT, el alcance del gobierno puede ser aplicado a toda la empresa. Sin embargo, también puede ser aplicado a un área o a un activo. Los roles, actividades y relaciones definen quién está involucrado en el gobierno, cómo se involucra, lo que hacen y cómo interactúan dentro del alcance definido. COBIT 5 hace una clara distinción entre las actividades de gobierno y las de gestión. [4]

Existen muchos estándares y buenas prácticas enfocadas al óptimo desempeño de las TI, sin embargo, en su mayoría, actúan de manera aislada, es decir, se aplican a un área de las TI en específico. El **Principio 3 - Aplicar un marco de referencia único integrado**, establece que COBIT 5 se alinea con los otros estándares y marcos de trabajo convirtiéndose en el marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.[4]

El enfoque del **Principio 4 - Hacer posible un enfoque holístico**, se refiere a la aplicación del conjunto de catalizadores o habilitadores definidos por COBIT 5, como componentes interactivos que apoyan la implementación de un sistema de gobierno y gestión de las TI en la empresa. Los catalizadores son factores que influyen sobre si algo funcionará, puede ser individual o grupal.

COBIT 5 define siete categorías de catalizadores (Ver Figura 4), estos son: 1) Principios, políticas y marcos de referencia, definen el comportamiento deseado para el día a día. 2) Procesos, conjunto organizado de prácticas y actividades para alcanzar los objetivos de TI. 3)

Estructuras organizativas, entidades de toma de decisiones clave en la empresa. 4) Cultura, ética y comportamiento de las personas y de la empresa. 5) Información, toda la producida y utilizada por la empresa, se requiere de la información para mantener la organización funcionando. 6) Servicios, infraestructuras y aplicaciones que proporcionan a la empresa servicios y tecnologías de procesamiento de información. 7) Personas, habilidades y competencias de los responsables de completar satisfactoriamente las actividades y la correcta toma de decisiones.[4]

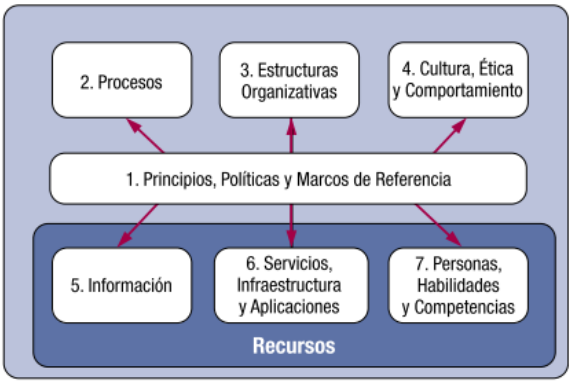


Figura 4 - Catalizadores de COBIT 5

COBIT 5 establece una marcada diferencia entre el gobierno y la gestión, es lo que se describe en el **Principio 5 - Separar el gobierno de la gestión**. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. De acuerdo a COBIT 5, el gobierno asegura que las necesidades, condiciones y opciones de las partes interesadas son evaluadas con el propósito de determinar que se alcanzan las metas corporativas, estableciendo la dirección a través de la priorización y la toma de decisiones, midiendo el rendimiento y el cumplimiento. Por otro lado, la gestión planifica, construye, ejecuta y controla las actividades alineadas con la dirección establecida por el gobierno.[4]

COBIT 5 propone que las empresas implementen procesos de gobierno y gestión que permitan cubrir todas las áreas fundamentales del gobierno de TI. La Figura 5 muestra las áreas clave de gobierno y gestión de COBIT 5. Cada empresa organiza sus procesos de la manera que mejor se adapte a su contexto, siempre y cuando las metas de gobierno y gestión estén cubiertas. [4]

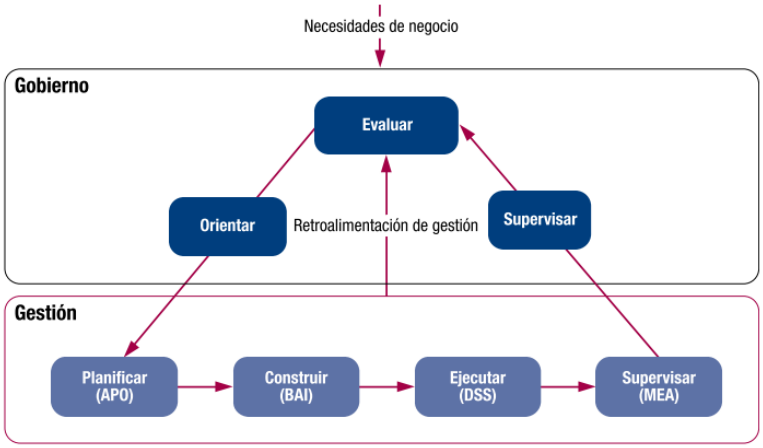


Figura 5 - Áreas clave de gobierno y gestión de COBIT 5

2.2.4. Cascada de metas

Para COBIT 5 la creación de valor es un objetivo de gobierno y esto se traduce en obtener beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. La satisfacción de las necesidades de las partes interesadas se convertirá en la estrategia de la organización con más confiabilidad. La Figura 6 muestra la relación entre las necesidades de las partes interesadas y la creación de valor.

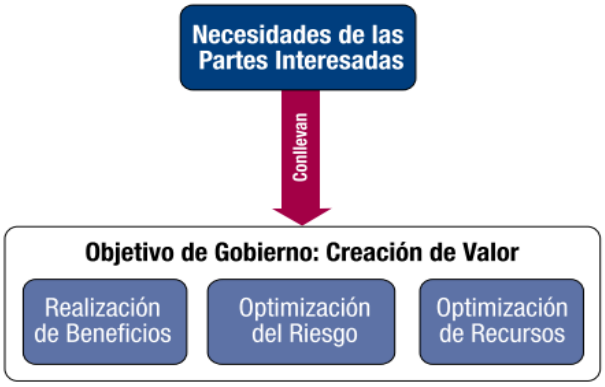


Figura 6 - Relación entre las necesidades de las partes interesadas y la creación de valor

El mecanismo que propone COBIT 5 para traducir las necesidades de las partes interesadas en estrategias que permitan el gobierno de TI se denomina Cascada de Metas. La Cascada de Metas permite el alineamiento de las necesidades de las partes interesadas con las metas corporativas, metas relacionadas con la TI y los “catalizadores” específicos, útiles y a medida. La finalidad es identificar los procesos de COBIT 5 necesarios de implementar para lograr las metas corporativas y satisfacer las necesidades de las partes interesadas. La Figura 7 muestra el mecanismo de la Cascada de Metas de COBIT 5.[4]

Figura 7 - Cascada de metas

Los motivos de las partes interesadas forman el primer nivel de la cascada, estos motivos se relacionan con el entorno, la tecnología, las leyes, etc., e influyen en las necesidades de beneficio, optimización de recursos y optimización de riesgos que son los objetivos de gobierno.

En el siguiente nivel de la cascada se identifican las Necesidades de las partes interesadas, el propósito es conocer cuáles se relacionan con las metas empresariales. Cobit 5 ha elaborado una lista de necesidades de las partes interesadas internas y externas que puede ser vinculada con las metas empresariales. Esta lista se puede usar para establecer y priorizar metas corporativas o las metas relacionadas con TI. Sin embargo, deben tomarse las precauciones necesarias puesto que la situación de cada empresa es diferente y no debe usarse la lista de forma mecánica, sino sólo como sugerencia de un conjunto genérico de situaciones. En la Figura 8 se muestran la lista de las Necesidades de las partes interesadas internas y externas definidas por Cobit 5.

Partes Interesadas Internas	Preguntas de las Partes Interesadas Internas
• Consejo de Administración • Director general ejecutivo (CEO) • Director financiero (CFO) • Director de sistemas de información (CIO) • Responsable de riesgos • Ejecutivos del negocio • Propietarios de los procesos del negocio • Responsables del negocio • Responsables de riesgos • Responsables de seguridad • Responsables del servicio • Responsables de recursos humanos • Auditoría interna • Responsables de privacidad • Usuarios de TI • Gerentes de TI • Etc.	• ¿Cómo consigo valor del uso de TI? ¿Están los usuarios finales satisfechos con la calidad del servicio de TI? • ¿Cómo gestiono el rendimiento de TI? • ¿Cómo puedo explotar mejor las nuevas tecnologías para nuevas oportunidades de negocio? • ¿Cómo construyo y estructuro mejor mi departamento de TI? • ¿Cuánto dependo de los proveedores externos? ¿Estoy gestionando bien los contratos de externalización de TI? • ¿Cómo obtengo aseguramiento sobre los proveedores externos? • ¿Cuáles son los requisitos (de control) para la información? • ¿Considero todos los riesgos relativos a TI? • ¿Estoy realizando una operación de TI eficiente y resiliente? • ¿Cómo controlo el coste de TI? ¿Cómo utilizo los recursos de TI de la manera más efectiva y eficiente? • ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes? • ¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento? • ¿Cómo consigo aseguramiento sobre TI? • ¿Está bien asegurada la información que se está procesando? • ¿Cómo puedo mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible? • ¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué? ¿Está siendo TI un obstáculo para ejecutar la estrategia de negocio? • ¿Cuán críticas son las TI para la sostenibilidad de la empresa? ¿Qué haría si las TI no estuvieran disponibles? • ¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio? • ¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI? • ¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio? • ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos? • ¿Cuánto se tarda en la toma de decisiones importantes de TI? • ¿Son transparentes el esfuerzo y las inversiones totales en TI? • ¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?
Partes Interesadas Externas	**Preguntas de las Partes Interesadas Externas**
• Aliados del negocio • Proveedores • Accionistas • Reguladores/gobierno • Usuarios externos • Clientes • Organizaciones de estandarización • Auditores externos • Consultores • Etc.	• ¿Cómo sé que las operaciones de mi aliado de negocio son seguras y fiables? • ¿Cómo sé que la empresa cumple con las normativas y regulaciones aplicables? • ¿Cómo sé que la empresa está manteniendo un sistema efectivo de control interno? • ¿Los aliados del negocio mantienen bajo control la cadena de información entre ellos?

Figura 8 - Necesidades de las partes interesadas

El siguiente nivel de la Cascada, se identifican las metas corporativas que se relacionan a las necesidades de las partes interesadas internas y externas.

Como resultado de una investigación realizada por la Universidad de Ambers y el aporte de expertos en gobierno corporativo y gobierno de TI, COBIT 5 ha definido 17 metas corporativas genéricas comúnmente aceptadas por las empresas, organizadas de acuerdo a las perspectivas del Cuadro de Mando Integral (CMI). Estás metas corporativas responden a las necesidades de las partes interesadas y se relacionan, de forma primaria o secundaria, con los tres principales objetivos de gobierno. La Figura 9 muestra las metas corporativas y su relación con los objetivos de gobierno.[4]

Dimensión del CMI	Meta Corporativa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Figura 9 - Metas corporativas propuestas por COBIT 5

Las metas corporativas se alcanzan con los resultados de las metas relacionadas con la TI, es decir, al óptimo uso de la información y el desempeño de la tecnología relacionada. Las metas de TI se estructuran de acuerdo a las dimensiones del CMI y son 17, como se puede ver en la Figura 10. En este nivel de la cascada de metas, el objetivo es alinear las metas de TI con las metas corporativas identificando el tipo de relación que existe entre ellas (primaria o secundaria). El resultado será una lista de metas de TI que aseguran el cumplimiento de las metas corporativas. [4]

Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Figura 10 - Metas de TI propuestas por COBIT 5

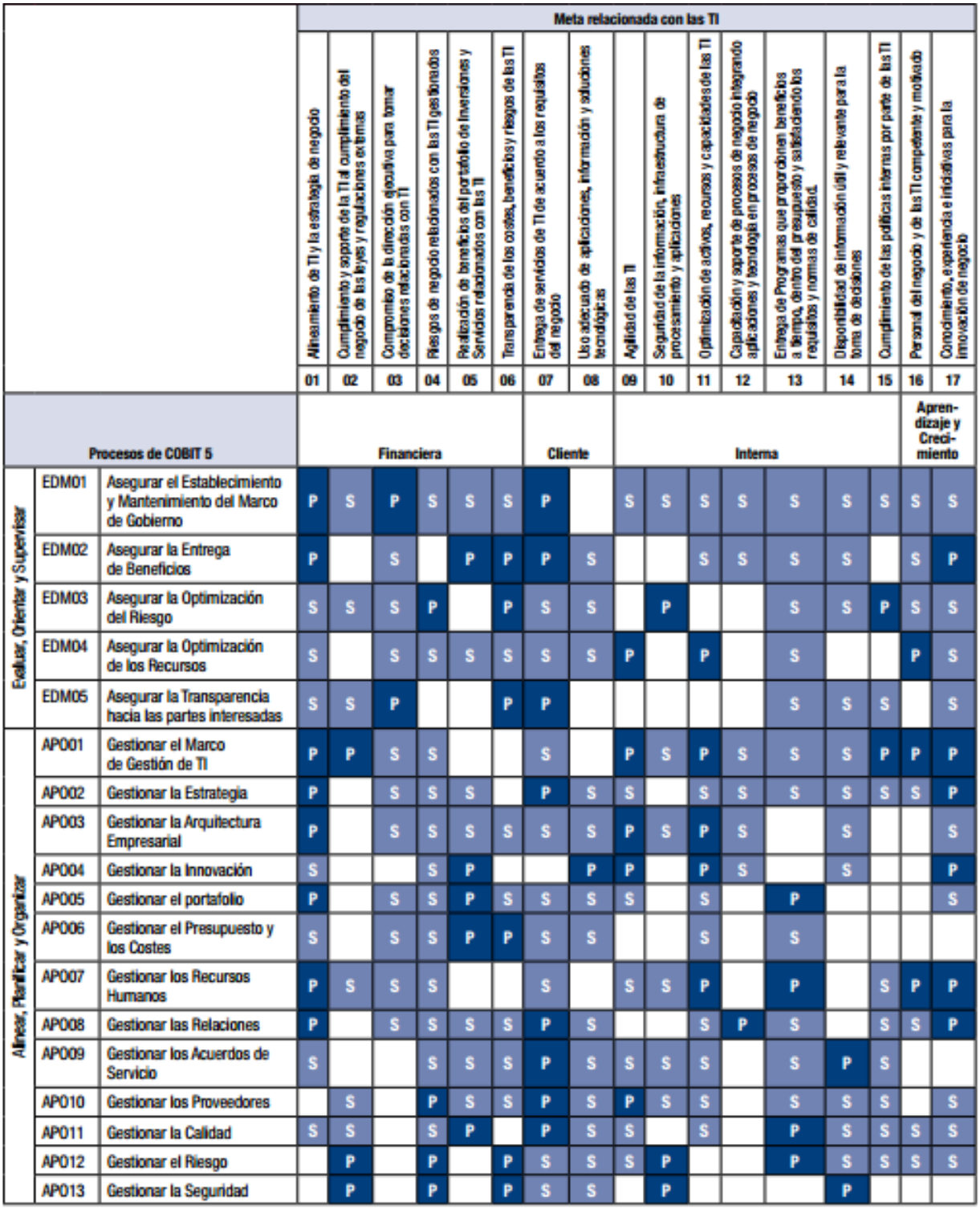
Alcanzar las metas relacionadas con las TI requiere de la aplicación satisfactoria y el uso adecuado de varios catalizadores. Los catalizadores incluyen procesos, estructuras organizativas e información, y para cada catalizador puede definirse un conjunto de metas relevantes en apoyo de las metas relacionadas con la TI.[4]

Los procesos son el tipo de catalizador que más se relaciona con el cumplimiento de las metas de TI. Un proceso es una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de recursos, manipula las entradas y produce salidas.[18]. Los otros tipos de catalizadores influyen sobre los procesos con recursos e información relevante para el logro de las metas relacionadas con TI.

En el último nivel de la cascada se identifican los procesos de COBIT 5 que se deben implementar para lograr las metas relacionadas con la TI y como consecuencia, alcanzar las metas corporativas. Las metas, prácticas y demás información relacionada a los procesos se definen en el Modelo de Referencia de Procesos.

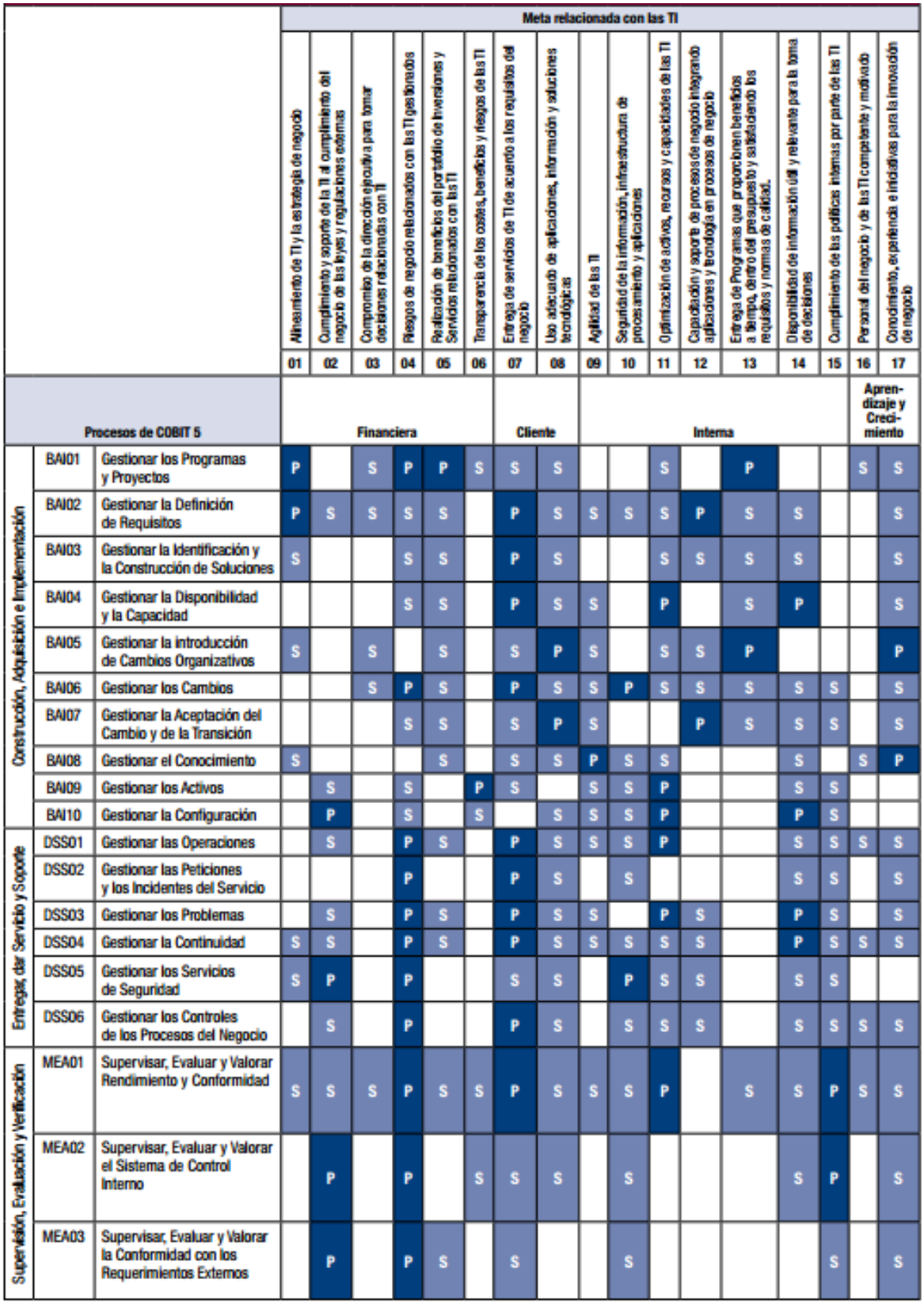
Aplicar la Cascada de Metas permite alinear las necesidades de las partes interesadas con los procesos de COBIT que se deben implementar para satisfacer esas necesidades. En el libro Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, una publicación de COBIT 5, se explica y provee la información, herramientas y técnicas para la correcta aplicación de la cascada de metas. Las Figuras 11 y 12 muestran el Mapeo de las Metas de TI y los procesos de Cobit 5.

Una vez identificados los procesos que apoyarán el logro de las metas de TI y las corporativas, se debe proceder a su implementación en la empresa, esto se alcanza con la aplicación de las Prácticas de Gobierno o de Gestión que COBIT ha definido para cada proceso. A la vez, los procesos resultantes de la Cascada de Metas que se alinean con los objetivos de la empresa deben ser evaluados, para identificar el nivel de capacidad que tienen y establecer las mejoras que se requieren implementar para alcanzar los objetivos esperados. El libro Procesos Catalizadores contiene la información detallada de cada proceso y las actividades que se deben realizar para su implementación. En el libro Modelo de Evaluación de Procesos (PAM) se tiene una visión clara de cómo realizar la evaluación de los procesos.



			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portfolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionan beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	AP001	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	AP002	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	AP003	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	AP004	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	AP005	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	AP006	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	AP007	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	AP008	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	AP009	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	AP010	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	AP011	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	AP012	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	AP013	Gestionar la Seguridad		P		P		P	S	S		P				P			

Figura 11 - Mapeo entre las Metas de TI y los procesos de Cobit 5 Parte 1



			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Figura 12 - Mapeo entre las Metas de TI y los procesos de Cobit 5 Parte 2

2.2.5. Modelo de referencia de procesos

El principio 5 de COBIT hace una marcada distinción entre el gobierno y la gestión de TI, en función a este principio las empresas deben implementar procesos de gobierno y procesos de gestión para lograr el adecuado gobierno y gestión de las TI.

Los procesos de gobierno se implementan con el propósito de alcanzar los objetivos de gobierno: entrega de valor, optimización del riesgo y optimización de los recursos. Además, incluye prácticas y actividades que permiten evaluar, orientar y supervisar las opciones estratégicas proporcionadas por la dirección de TI. Los procesos de gestión cubren la planificación, construcción, entrega del servicio y monitoreo de la TI de la empresa proporcionando una cobertura de TI de extremo a extremo [18].

El Modelo de Referencia de Procesos de COBIT 5 contiene 37 procesos organizados en 2 dominios principales: dominio de Gobierno y dominio de Gestión, como se puede apreciar en la Figura 13. El dominio de Gobierno se denomina Evaluar, Orientar y Supervisar y contiene 5 procesos. El dominio de Gestión se subdivide en 4 dominios: [18]

- El dominio Alinear, Planificar y Organizar (APO) contiene 13 procesos.
- El dominio Construir, Adquirir e Implantar (BAI) contiene 10 procesos.
- El dominio Entregar, dar Servicio y Soporte (DSS) contiene 6 procesos.
- El dominio supervisar, Evaluar y Valorar (MEA) contiene 3 procesos.

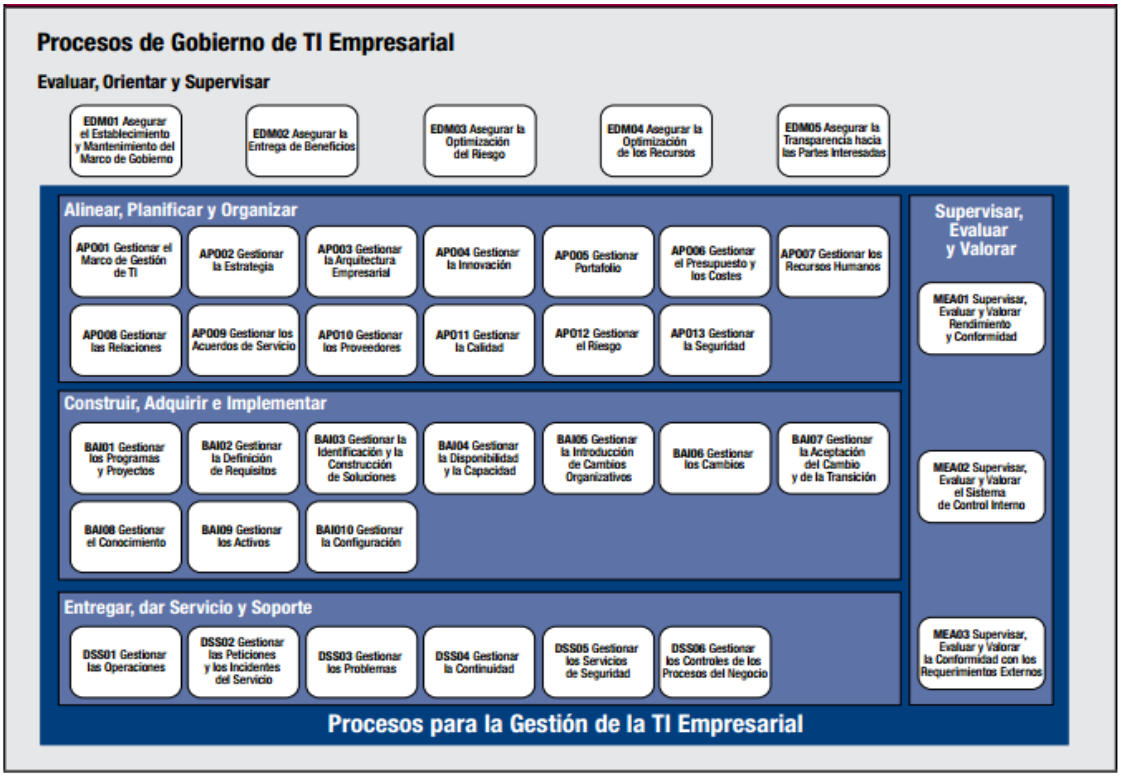


Figura 13 - Modelo de Referencia de Procesos de COBIT 5

Los procesos son uno de los siete tipos de catalizadores que propone COBIT para el gobierno y la gestión de TI. La Figura 14 muestra los detalles específicos que este catalizador tiene.

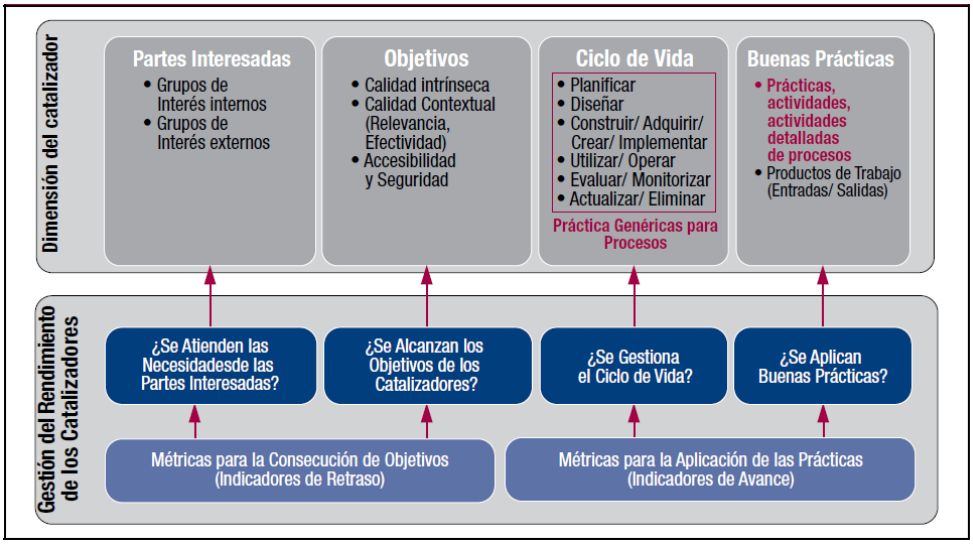


Figura 14 - Detalles específicos del catalizador procesos propuestos por COBIT 5

- ***Partes interesadas*:** todos los procesos tienen partes interesadas internas y externas con roles y niveles de responsabilidad definidos en la Matriz RACI. Clientes, socios de negocio, accionistas y entidades reguladoras son ejemplos de partes interesadas externas. Mientras que los interesados internos son el Consejo de Administración, la dirección, el personal y los voluntarios.[18]
- ***Metas/Objetivos*:** son declaraciones que describen el resultado deseado del proceso. Un resultado puede ser: un elemento, un cambio de estado, una mejora de la capacidad. Las metas del proceso apoyan las metas de TI, que a su vez apoyan a las metas corporativas. COBIT define 3 categorías de metas para los procesos: [18]
  - Metas intrínsecas: se refieren a la calidad del proceso, a la implementación de las buenas prácticas, y al cumplimiento de las reglas internas y externas.
  - Metas contextuales: se refieren a la adaptación del proceso al contexto de la empresa y si el proceso implementado es pertinente, entendible y fácil de aplicar.
  - Metas de accesibilidad y seguridad: se refieren a si el proceso mantiene la confidencialidad y si es conocido y accesible por quienes lo requieren.

  En todos los niveles de la cascada y en los procesos se definen métricas para medir hasta que puto dichas metas son alcanzadas. Las métricas en COBIT cumplen los criterios SMART (específicas, medibles, practicables, pertinentes y oportunas)

- ***Ciclo de vida**:* todos los procesos tienen un ciclo de vida. Se definen, crean, operan, supervisan, se ajustan o actualizan y finalmente, se retiran.[18]
- ***Buenas prácticas**:* cada proceso contiene un conjunto de buenas prácticas que se describen a un nivel de detalle: prácticas, actividades y actividades detalladas.[18]
  - Prácticas: De acuerdo a la naturaleza del proceso, las prácticas son de gobierno o de gestión. Estas proporcionan un conjunto de requerimientos de alto nivel para un gobierno y gestión de la TI eficaces y prácticos.
  - Actividades: Son las principales acciones para operar el proceso. Proporcionan el cómo, porqué y qué implantar para cada práctica de gobierno o gestión con el fin de mejorar el desempeño de la TI o tratar el riesgo en la entrega de soluciones y servicios de TI.
  - Actividades detalladas: Las actividades pueden no proporcionar en nivel de detalle suficiente para la implementación del proceso, y puede necesitarse una mayor orientación. Esta orientación se obtiene de estándares y buenas prácticas específicas tales como ITILv3, la serie ISO 27000, TOGAF, PRICE2, entre otros.
- **Entradas y salidas**: Son los productos y/o artefactos de los procesos que se consideran necesarios para apoyar la operación del proceso. Posibilitan las decisiones clave, proveen un registro y traza de auditoría de las actividades del proceso y posibilitan el seguimiento en caso de incidente.[18]

2.2.6. Proceso DSS05 Gestionar Servicios de Seguridad

Es un proceso de gestión que se ubica en el dominio Entrega, Servicio y Soporte. Su propósito es minimizar el impacto de las vulnerabilidades e incidentes operativos de seguridad en la información en el negocio. Este proceso protege la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.[18]

Las metas de TI a las que apoya son:

- 02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones
- 04 Riesgos de negocio relacionados con las TI gestionadas
- 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones

Las metas del proceso son:

- La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.

- La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.
- Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.
- Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida
- La información electrónica tiene las medidas de seguridad apropiadas mientas está almacenada, transmitida o destruida.

La Figura 15 muestra la Matriz RACI de proceso. En ella se identifican las partes interesadas internas y externas del proceso y su relación con las prácticas clave de gestión.[18]

Matriz RACI DSS05

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS05.01 Proteger contra software malicioso (*malware*).						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Gestionar la seguridad de la red y las conexiones.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Gestionar la seguridad de los puestos de usuario final.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Gestionar el acceso físico a los activos de TI.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.											I					C	C	A			R					
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Figura 15 - Matriz RACI del proceso DSS05 Gestionar los servicios de seguridad

Este proceso tiene siete prácticas de gestión que describen las actividades y documentos que se deben implementar para que la empresa alcance una adecuada gestión de los servicios de seguridad. Las prácticas de gestión son:

- ***DSS05.01 Proteger contra software malicioso:*** Implementar y mantener efectivas medidas, preventivas, de detección y correctivas a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso, por ejemplo: virus, gusanos, software espía y correo basura.[18]

- ***DSS05.02 Gestionar la seguridad de la red y las conexiones**:* Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.[18]
- ***DSS05.03 Gestionar la seguridad de los puestos de usuario final:*** Asegurar que los puestos de usuario final (laptops, PC de escritorio, servidores y otros dispositivos, software móvil y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.[18]
- ***DSS05.04 Gestionar la identidad del usuario y el acceso lógico:*** Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.[18]
- ***DSS05.05 Gestionar el acceso físico a los activos de TI**:* Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.[18]
- ***DSS05.06 Gestionar documentos sensibles y dispositivos de salida**:* Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.[18]
- ***DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad:*** Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.[18]

2.2.7. Modelo de evaluación de procesos – PAM

El Modelo de Evaluación de Procesos - PAM de COBIT 5 es un modelo que sirve como medio para medir el desempeño y la capacidad de los procesos de gobierno y gestión de TI e identificar las áreas de mejora. Está basado en la norma ISO/IEC 15504 de Ingeniería de Software – Evaluación de procesos. Se compone de dos tipos de indicadores: a) indicadores de desempeño del proceso, b) indicadores de capacidad del proceso.[11]

El PAM es bidimensional, como se muestra en la Figura 16. En la primera dimensión, la Dimensión de Procesos, los procesos están definidos y clasificados según el modelo de referencia de procesos de COBIT 5. En la segunda dimensión, la Dimensión de Capacidad, se definen los niveles de capacidad y el conjunto de atributos por nivel para evaluar los procesos. Los atributos del proceso proveen las características medibles de la capacidad de los procesos. [11]

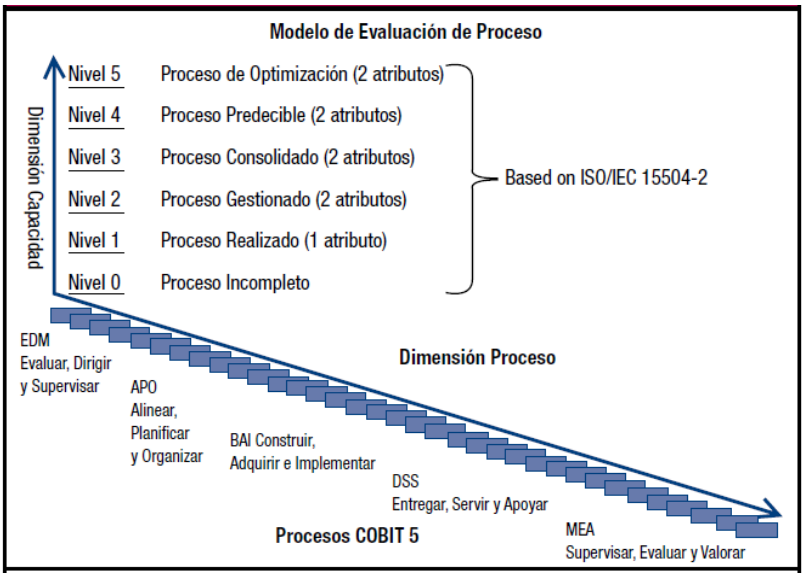


Figura 16 - Modelo de Evaluación de Procesos - PAM

- ***Dimensión de Procesos:*** La dimensión de procesos está compuesta por los 37 procesos de COBIT 5 agrupados en procesos de gobierno y procesos de gestión. El modelo PAM evalúa el nivel de capacidad en que se encuentran los procesos.[11]
- ***Dimensión de Capacidad:*** La dimensión de capacidad provee una medida de la capacidad de los procesos orientados al logro de los objetivos de negocio. La capacidad se mide en función a atributos del proceso, estos atributos están agrupados dentro de cada nivel de capacidad. El nivel de capacidad de un proceso se determina de acuerdo al cumplimiento de los atributos de los procesos de acuerdo a la norma ISO 15504-2. La Figura 17 muestra los niveles de capacidad y los atributos del proceso. [11]

ID del Atributo de Proceso	Niveles de Capacidad y Atributos de Proceso
	Nivel 0: Proceso incompleto
	Nivel 1: Proceso realizado
PA 1.1	Rendimiento del proceso
	Nivel 2: Proceso gestionado
PA 2.1	Gestion del rendimiento
PA 2.2	Gestión de productos del trabajo
	Nivel 3: Proceso consolidado
PA 3.1	Definición de proceso
PA 3.2	Despliegue del proceso
	Nivel 4: Proceso predecible
PA 4.1	Medición del proceso
PA 4.2	Control del proceso
	Nivel 5: Proceso optimizado
PA 5.1	Innovación del proceso
PA 5.2	Optimización del proceso

Figura 17 - Niveles de capacidad y atributos del proceso

- ***El Nivel 0 - Proceso Incompleto***, esto significa que el proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- ***El Nivel 1 - Proceso Ejecutado,*** es decir, el proceso implementado alcanza su propósito, pero presenta alguna debilidad. El atributo evaluado es el Rendimiento del proceso.
- ***El Nivel 2 - Proceso Gestionado,*** se refiere a que el proceso ejecutado del nivel anterior está implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- ***El Nivel 3 se denomina Proceso Establecido*** lo que significa que el proceso gestionado descrito anteriormente está implementado usando un proceso definido que es capaz de alcanzar sus resultados.
- ***En el Nivel 4 el proceso es Predecible***, es decir, se ejecuta dentro de límites definidos para alcanzar sus resultados esperados.
- ***En el último nivel, Nivel 5, el proceso está optimizado***, lo que significa que el proceso es mejorado de forma continua para cumplir con las metas empresariales presentes y futuras.

Los atributos del proceso de cada nivel de capacidad se muestran en la Figura 18. Como se observa el Nivel 0 no tiene ningún atributo. El Nivel 1, tiene un atributo denominado Atributo de Desempeño del Proceso. Del Nivel 2 al Nivel 5, existen dos atributos del proceso para cada nivel. El cumplimiento de estos atributos son los que definen el nivel de capacidad en el que se encuentra el proceso evaluado.[11]

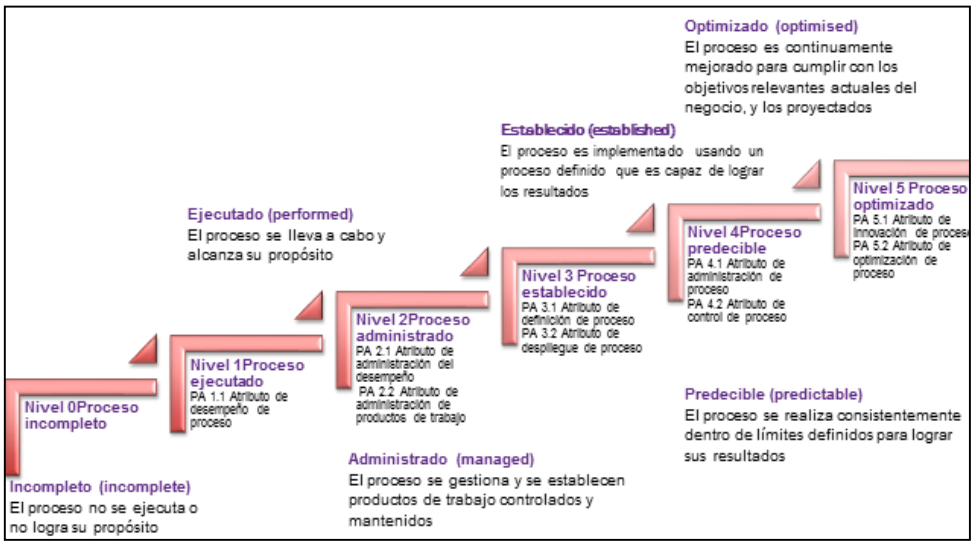


Figura 18 - Atributos del proceso en cada nivel de evaluación

2.2.7.1. Indicadores de evaluación

Los indicadores de evaluación se usan para evaluar si se han alcanzado los atributos del proceso y por lo tanto si se ha logrado el nivel deseado. Existen dos tipos de indicadores de evaluación:

- *Indicadores de desempeño del proceso*, se aplica exclusivamente al Nivel de capacidad 1. Son específicos para cada proceso y son usados para determinar si un proceso se encuentra en el nivel de capacidad 1. Para evaluar el rendimiento se utiliza las Prácticas Base (BP) y Productos de Trabajo (WP).[11]
- *Indicadores de capacidad de procesos*, se aplica a los niveles de capacidad del 2 al 5. Para evaluar si los procesos cumplen los atributos de los niveles del 2 al 5 se utilizan las Prácticas Genéricas (GP) y los Productos de Trabajo Genéricos (GWP).[11]

Las Prácticas Base, Productos de Trabajo, Prácticas Genéricas y los Productos de Trabajo Genéricos se describen con mayor detalle en el libro Modelo de Evaluación de Procesos (PAM) de COBIT 5.

2.2.7.2. Indicadores de desempeño de proceso

La evaluación de los procesos en el Nivel 1 se hace en función a su desempeño. El atributo es evaluado por medio de las Prácticas Base (BPs) y los Productos de trabajo de entrada y de salida (WPs). El Modelo de Referencia de Procesos de COBIT 5, proporciona esta información para cada uno de los 37 procesos del modelo.[11]

El PAM describe cada proceso en términos del nombre, propósito, Resultados (Os), Prácticas Base (BPs) y los Productos de Trabajo (WPs). En la Tabla 1 se describen los resultados, prácticas base y productos de trabajo que el PAM propone se deben considerar para la evaluación del proceso DSS05 Gestionar los servicios de seguridad en el Nivel 1.

Tabla 1 - Resultados, Prácticas base, Productos de Trabajo para el proceso DSS05 Gestionar servicios de seguridad

ID de proceso	DSS05	
Nombre del proceso	Gestión de servicios de seguridad	
Descripción del proceso	Proteger la información de la empresa para mantener un nivel de riesgo de seguridad de la información aceptable para la empresa de acuerdo con la política de seguridad. Establecer y mantener las funciones de seguridad de la información y los privilegios de acceso y de supervisión de la seguridad.	
Propósito del proceso	Minimizar el impacto en el negocio de las vulnerabilidades operacionales de seguridad de la información y de incidentes.	
Resultados (Os)		
Número	**Descripción**	
DSS05-01	Satisfacer las necesidades del negocio respecto a la seguridad de redes y comunicaciones.	
DSS05-02	La información procesada en, almacenada en y transmitida por medio de dispositivos de punto final está protegida.	
DSS05-03	Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa.	
DSS05-04	Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias al ser procesada, almacenada o transmitida.	
DSS05-05	La información electrónica se ha asegurado correctamente cuando se almacena, transmite o destruye.	
Prácticas Base (BPs)		
Número	**Descripción**	**Soporta**
DSS05-BP1	Protección contra el malware. Implementar y mantener medidas preventivas, detectivas y correctivas (especialmente hasta actualizar los parches de seguridad y de control de virus) en toda la empresa para proteger los sistemas de información y tecnología de software malicioso (por ejemplo, virus, gusanos, software espía, correo no deseado).	DSS05-01/02
DSS05-BP2	Administrar la seguridad de la red y la conectividad. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los sistemas de conectividad.	DSS05-01
DSS05-BP3	Administrar la seguridad del punto final. Asegurar que los puntos finales (por ejemplo, ordenadores portátiles, de escritorio, servidores y otros dispositivos móviles y de red o software) están securizados con un nivel igual o superior que los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.	DSS05-02
DSS05-BP4	Administrar la identidad de usuarios y accesos lógicos. Asegurar que todos los usuarios tienen derechos de acceso a la información acordes con sus requisitos de negocio y coordinarse con las unidades que gestionan sus propios derechos de acceso en los procesos de negocio.	DSS05-03

DSS05-BP5	Administrar el acceso físico a los activos de TI. Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluidas emergencias. El acceso a los locales, edificios y áreas debe justificarse, autorizarse, registrarse y supervisarse. Esto debería aplicarse a todas las personas que entran en los locales, incluidos personal interno, personal temporal, clientes, proveedores, visitantes o cualquier tercero.	DSS05-04
DSS05-BP6	Administrar documentos sensibles y dispositivos de salida. Establecer protecciones físicas apropiadas, prácticas de contabilidad y una gestión de inventario sobre activos sensibles de TI como formularios especiales, instrumentos negociables, impresoras de propósito especial o tokens de seguridad.	DSS05-05
DSS05-BP7	Supervisar la infraestructura de eventos relacionados con seguridad. Uso de herramientas de detección de intrusiones, supervisión de la infraestructura ante accesos no autorizados y asegurar que los eventos se integran en la supervisión general de eventos y la gestión de incidentes.	DSS05-01

Productos de Trabajo (WPs)

Entradas

Número	Descripción	Soporta
APO01-WP10	Directrices de clasificación de datos.	DSS05-BP2 DSS05-01
APO09-WP4	Acuerdos de nivel de servicio (SLAs).	
APO03-WP6	Modelo de Información de arquitectura.	DSS05-BP3 DSS05-02
APO09-WP4	Acuerdos de nivel de servicio (SLAs).	
APO09-WP5	Acuerdos de nivel operativo (OLAs).	
APO09-WP2	Resultados de controles sobre el inventario físico.	
DSS06-WP11	Informes de violaciones.	
APO01-WP4	Definición de roles y responsabilidades de TI.	DSS05-BP4 DSS05-03
APO03-WP6	Modelo de Información de arquitectura.	
APO03-WP6	Modelo de Información de arquitectura	DSS05-BP6 DSS05-05

Salidas

Número	Descripción	Entrada a	Soporta
DSS05-WP1	Política de prevención de software malicioso.	APO01.04	DSS05-BP1 DSS05-01/02
DSS05-WP2	Evaluaciones de potenciales amenazas.	APO12.02 APO12.03	
DSS05-WP3	Política de seguridad para conectividad.	APO01.04	DSS05-BP2 DSS05-01
DSS05-WP4	Resultados de pruebas de penetración.	MEA02.08	
DSS05-WP5	Políticas de seguridad para dispositivos de punto final.	APO01.04	DSS05-BP3 DSS05-01
DSS05-WP6	Derechos de acceso aprobados de usuarios.	Interna	DSS05-BP4 DSS05-03
DSS05-WP7	Resultados de revisiones de cuentas de usuario y privilegios.	Interna	
DSS05-WP8	Peticiones aprobadas de acceso.	Interna	DSS05-BP5 DSS05-04
DSS05-WP9	Registros de acceso (logs).	DSS06.03	
DSS05-WP10	Inventario de documentos y dispositivos sensibles.	Interna	DSS05-BP6 DSS05-05
DSS05-WP11	Privilegios de acceso.	Interna	
DSS05-WP12	Registros de eventos de seguridad (logs).	Interna	DSS05-BP7 DSS05-01
DSS05-WP13	Características de incidentes de seguridad.	Interna	
DSS05-WP14	Tickets de incidentes de seguridad.	DSS02.02	

2.2.7.3. Indicadores de capacidad de proceso

La evaluación de los procesos en los niveles del 2 al 5 se hace en función a los indicadores de capacidad del proceso. Los atributos de cada nivel son evaluados por las Prácticas Genéricas (GP) y los Productos de Trabajo Genéricos (GWP). Para cada atributo de los niveles 2 al 5 el PAM define Resultados del cumplimiento del atributo. El logro de estos resultados está en función al cumplimiento de las prácticas genéricas y los productos de trabajo genéricos definidos. [11].

2.2.7.4. Escala de calificación

Finalmente, el PAM establece una escala de calificación definido por la ISO 15504-2 que se utiliza para calificar a cada atributo [11]. Esta escala es:

- N – No alcanzado: Hay muy poca o ninguna evidencia de que se alcanza el atributo definido en el proceso evaluado.
- P – Parcialmente alcanzado: Hay alguna evidencia de aproximación y algún logro del atributo definido en el proceso evaluado.
- L - Ampliamente alcanzado: Hay evidencia de un enfoque sistemático y de un logro significativo del atributo definido en el proceso evaluado.
- F – Completamente alcanzado: Existe evidencia de un completo y sistemático enfoque y un logro completo del atributo definido en el proceso evaluado.

La Figura 19 muestra la escala de calificación y el porcentaje de logro que se asigna a los atributos luego de la evaluación.

Abreviación	Descripción	% Logro
N	No alcanzado	0 a 15% de logro
P	Parcialmente alcanzado	>15% a 50% de logro
L	Ampliamente alcanzado	>50% a 85% de logro

Figura 19 - Escala de Calificación del PAM

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo de investigación

Vara [19] expresa que cualquier investigación puede ser básica como aplicada, y que tendrá más valor si los resultados aportan condiciones para resolver problemas y si aumentan el conocimiento científico. Además, enfatiza que una investigación aplicada es práctica, pues los resultados son utilizados en la solución de problemas de la realidad, mientas que la investigación básica genera nuevos conocimientos.

La presente investigación es del tipo básica y aplicada. Es básica porque, sobre la base de los expuesto en el Marco de Referencia COBIT 5, se propone una forma mejorada de evaluación de procesos de gobierno y gestión de tecnologías de información (nuevo conocimiento) a través del Modelo de Evaluación de la Capacidad de Procesos (ECP), este modelo utiliza conceptos matemáticos para fundamentar su funcionamiento. Es aplicada porque, una vez diseñado y desarrollado el modelo se lo aplica al contexto de la universidad objeto de estudio con el fin de validar su funcionamiento y proponer las mejoras sobre el proceso evaluado.

De acuerdo a la naturaleza de los datos que intervienen, la investigación también es cualitativa y cuantitativa. Es del tipo cualitativa porque, para el diseño del modelo ECP se evalúa las necesidades de las partes interesadas de la universidad respecto a las tecnologías de información. Además, se evalúa cómo se pueden atender estás necesidades por medio de la identificación de los objetivos estratégicos y los procesos de TI que se alinean y que deben implementarse para satisfacer las necesidades de las partes interesadas. Es del tipo cuantitativo porque una vez diseñado el modelo ECP se evalúa la capacidad de un proceso en particular aplicando un instrumento de evaluación que permite obtener el porcentaje del nivel de capacidad alcanzado según una escalada de calificación. Este nivel alcanzado se interpreta y proponen mejoras.

3.2. Diseño de investigación

La investigación exploratoria se utiliza cuando el tema a investigar aún no ha sido estudiado lo suficiente. Las investigaciones exploratorias permiten esclarecer y delimitar problemas poco estudiados. Son flexibles y se sustentan en la revisión de la bibliografía, en los criterios de expertos, en el contacto y la observación directa y cotidiana de la realidad de la organización.

Por otro lado, las investigaciones cualitativas se concentran en la profundidad y la comprensión de un tema, sintetizar un proceso, esquematizarlo. Son investigaciones que buscan descubrir la complejidad de un problema y proponer una solución basada en la exploración realizada. [19]

Por lo expuesto, el diseño de la presente investigación es del tipo exploratoria cualitativa de estudio de casos, pues busca profundizar en el problema del gobierno y gestión de las tecnologías de información a través de procesos de TI alineados a la estrategia de la organización y la evaluación del nivel de capacidad de los procesos con el fin de identificar las mejoras necesarias para que aporten con el logro de las metas empresariales.

3.3. Técnica de recolección de datos

Por ser una investigación de diseño exploratorio cualitativo, las técnicas que se utilizaron para la recolección de los datos fueron: la revisión documental y las entrevistas.

a) Revisión documental. El diseño del Modelo ECP está basado en las buenas prácticas del Marco de Referencia COBIT 5, en ese sentido, se revisaron minuciosamente los siguientes libros de este marco:

- COBIT 5, un marco de negocio para el gobierno y gestión de las TI en la empresa
- COBIT 5, Procesos Catalizadores
- Modelo de Evaluación de Procesos (PAM) usando COBIT 5

Además, se revisaron investigaciones realizadas sobre gobierno y gestión de tecnologías de información que se basaron en COBIT 5, para analizar la manera como utilizaron las buenas prácticas en sus propuestas de solución.

Asimismo, se revisaron libros y guías de gobierno corporativo y gobierno de TI en diferentes contextos, entre ellos el universitario, que es el caso de estudio que orienta esta investigación.

Por último, se revisó el Plan Estratégico v2 2014 – 2018 de la Universidad para conocer sus objetivos estratégicos y el quehacer de la universidad.

b) Entrevistas. Se realizaron entrevistas guiadas a los principales actores que influyen en el gobierno corporativo y gobierno de TI de la universidad para conocer su nivel de satisfacción con el aporte de valor de las TI en el logro de los objetivos estratégicos. La entrevista siguió un esquema semiestructurado pues se utilizó una lista de preguntas que permitían guiar la entrevista, pero en función a la respuesta del entrevistado se podía

profundizar con preguntas libres que no se encontraban en la lista pero que si servían para aclarar alguna duda.

Entre los actores entrevistados destacan: Gerente General, Vicerrector, Decanos, Director de Escuela de Pos Grado, Jefes de Área, Director de DIGETI, entre otros.

También se entrevistó, utilizando un instrumento de evaluación (Ver Anexos), a los responsables de los servicios de seguridad de la información de la universidad con el propósito de identificar el nivel de capacidad que tiene el proceso DSS05 Gestionar los servicios de seguridad de COBIT 5 que fue el proceso que se utilizó para validar el modelo.

3.4. Sistema de variables

En el desarrollo de esta investigación intervienen las siguientes variables de estudio:

a) Variable Independiente: Modelo de evaluación de la capacidad de procesos basado en COBIT 5.

b) Variable Dependiente: Gobierno de Tecnologías de Información.

Dimensiones:

- Entrega de valor a las partes interesadas
- Alineamiento estratégico con la TI
- Medición del rendimiento de las TI

3.5. Metodología de la Investigación

En la figura 20 se muestran las etapas que comprende la metodología que se aplicaron en la presente investigación. En los párrafos siguientes se explica cada etapa describiendo las actividades realizadas.

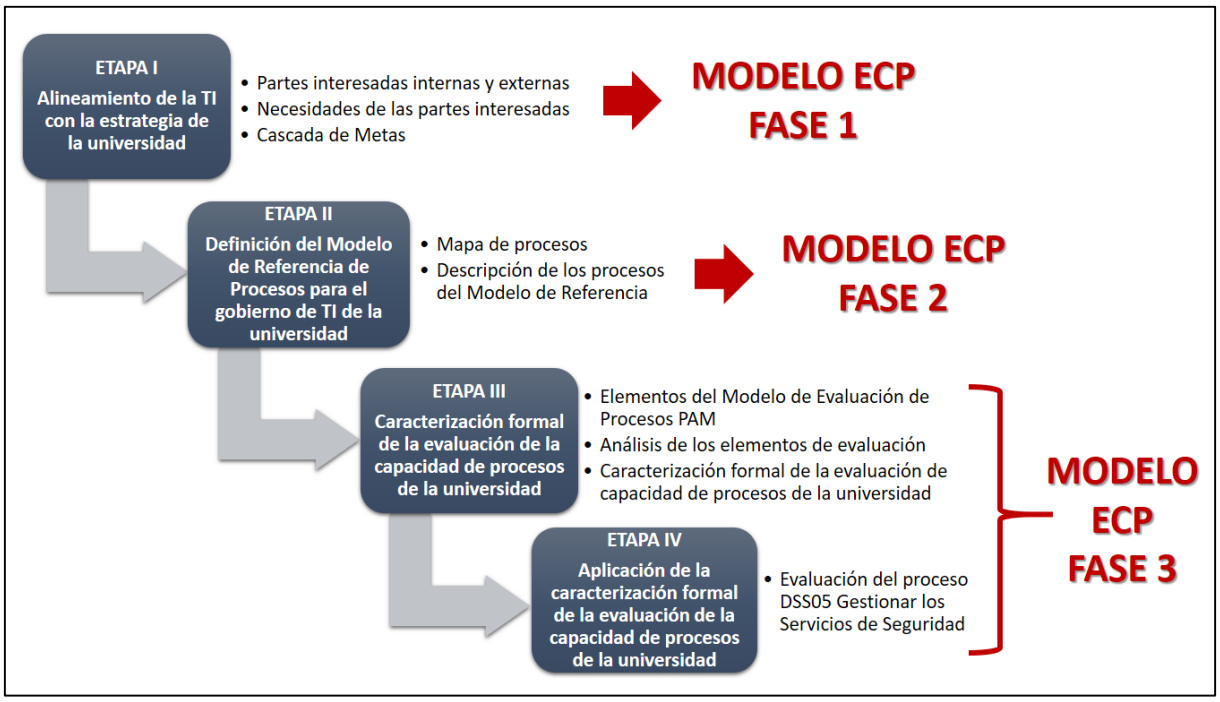


Figura 20 - Metodología aplicada a la investigación

3.5.1. Etapa I: Alineamiento de la TI con la estrategia de la universidad

En esta etapa aplicaremos el mecanismo de la Cascada de Metas para alinear las tecnologías de información con los objetivos estratégicos de la universidad. En esta etapa se desarrolla la Fase 1 del Modelo ECP.

Actividad 1.1. Identificación y definición de las partes interesadas internas y externas

Las partes interesadas son organizaciones, grupos, o personas que pueden afectar o ser afectados por las actividades de una empresa. Son muchas las partes interesadas que colaboran para alcanzar un buen rendimiento del gobierno de TI en una organización, y tienen necesidades específicas que deben ser satisfechas.[4] Existen partes interesadas internas y externas, cada una cumple un rol de acuerdo a su nivel de responsabilidad. Las partes interesadas internas lo constituyen el Consejo de Administración, la dirección, el personal y los voluntarios. Las partes

interesadas externas incluyen a los clientes, socios del negocio, accionistas, proveedores y entidades reguladoras.[4]

COBIT 5 documenta los roles y niveles de responsabilidad de las partes interesadas en la Matriz RACI para cada uno de los 37 procesos. Estas partes interesadas son genéricas, por lo que cada organización que desee implementar gobierno de TI debe identificar quienes son las partes interesadas internas y externas que están involucradas con el buen gobierno de TI.

Esta actividad consiste en identificar a las partes interesadas internas y externas de la universidad, sus roles y niveles de responsabilidad respecto al gobierno de TI.

Actividad 1.2. Identificación de las necesidades de las partes interesadas

El mecanismo de la cascada de metas inicia con la identificación de las necesidades de las partes interesadas internas y externas. Estas necesidades se relacionan con las metas empresariales para finalmente desencadenar en los procesos de gobierno y gestión de TI. COBIT 5 propone un listado de las necesidades de las partes interesadas respecto al gobierno de TI, estás necesidades son genéricas y deben ser adaptadas al contexto de la organización.[4]

Esta actividad consiste en identificar las necesidades de las partes interesadas internas y externas de la universidad, para este fin se utilizará una encuesta.

Actividad 1.3. Definición de la relación entre las necesidades de las partes interesadas y los objetivos estratégicos de la organización

Este es el segundo nivel de la cascada de metas, donde se identifica cómo se relacionan las necesidades de las partes interesadas con los objetivos estratégicos de la organización. COBIT 5 propone un listado de 17 metas corporativas organizadas de acuerdo a las perspectivas del BSC.[4] Sin embargo, para la presente investigación, se tomarán en cuenta los objetivos estratégicos de la universidad, extraídos del Plan Estratégico 2014-2018.[21]

En esta actividad se analizará y definirá la alineación de las necesidades de las partes interesadas con los objetivos estratégicos de la universidad.

Actividad 1.4. Definición de la relación entre los objetivos estratégicos de la organización y las metas de TI de COBIT 5

En el tercer nivel de la cascada de metas se evalúa la relación entre las metas corporativas y las metas de TI. COBIT 5 establece 17 metas de TI organizadas en función a las 4 perspectivas del BSC. [4]

En esta actividad se utilizará el resultado de la Actividad 1.3. (los objetivos estratégicos de la universidad) para alinearlos con las Metas de TI propuestas por COBIT.

Actividad 1.5. Definición de la relación entre las Metas de TI y los procesos de COBIT 5

En el último nivel de la cascada de metas, se relacionan las Metas de TI resultantes del nivel anterior con los 37 procesos del Modelo de Referencia de Procesos de COBIT 5. De esta manera se alinea la TI de la empresa con las estrategias de la organización.[4]

Esta actividad consiste en identificar los procesos de COBIT 5 que se alinean con los objetivos de la universidad y permiten el logro de los mismos.

3.5.2. Etapa II: Definición del modelo de Referencia de Procesos para el gobierno de TI en la universidad

En esta etapa se elaborará el Modelo de Referencia de Procesos de la universidad con la información resultante de la cascada de metas. Además, se describirá cada uno de los procesos que se alinean con la estrategia de la universidad. Esto comprende la Fase 2 del Modelo ECP.

Actividad 2.1. Elaboración del Mapa de Procesos del Modelo de Referencia de Procesos de la universidad

El Modelo de Referencia de Procesos organiza los 37 procesos de COBIT 5 en procesos de gobierno (5) y procesos de gestión (32). Los procesos de gestión se organizan en 4 dominios. El dominio APO con 13 procesos, dominio BAI con 10 procesos, dominio DSS con 6 procesos y el dominio MEA con 3 procesos.[18]

De acuerdo al resultado obtenido de la cascada de metas, esta actividad consiste en elaborar un mapa de procesos alineado a la estrategia de la universidad tomando como base el Modelo de Referencia de Procesos de COBIT 5. En este mapa se identificará cuáles son los procesos de gobierno y de gestión (se considera los dominios donde haya procesos) que apoyan el logro de los objetivos estratégicos de la universidad.

Actividad 2.2. Descripción de los procesos del Modelo de Referencia de Procesos de la universidad

Esta actividad consiste en describir cada proceso del mapa considerando los elementos que COBIT plantea y adaptarlos al contexto de la universidad. Esto incluye definir quién es el dueño del proceso, cuáles son las áreas o las partes interesadas con las que se relaciona, a que objetivo estratégico apoya, entre otros aspectos.

3.5.3. Etapa III: Caracterización formal de la Evaluación de la Capacidad de Procesos de TI de la universidad

Esta etapa es la medular, pues es aquí donde se diseñan cada uno de los elementos que tendrá la Fase 3 el modelo ECP de la universidad. De acuerdo a los diferentes niveles que tiene el PAM se propone una metodología para la elaboración de los instrumentos de evaluación y la forma de aplicación.

Actividad 3.1. Identificación de los elementos del Modelo de Evaluación de Procesos – PAM

Esta actividad consiste en hacer una revisión y análisis del PAM con el objetivo de identificar todos sus elementos y la forma cómo se relacionan entre sí. Además, analizar la Plantilla de Autoevaluación que provee COBIT como parte de su kit de herramientas de apoyo. Se propone la realización de este análisis porque al revisar investigaciones que hicieron uso del PAM se identificó que obviaron alguno de los elementos. Entonces, para diseñar y proponer un modelo de evaluación de capacidad de procesos basado en el PAM que sea robusto y completo es preciso conocer muy bien cómo se organiza y funciona.[11]

Actividad 3.2. Evaluación Nivel 1: Análisis de los Criterios o Resultado (Os), de las Prácticas Base (BP) y los Productos de Trabajo (WP)

Según el PAM, el Nivel 1 tiene 3 elementos básicos: los Resultados, las Prácticas Base y los Productos de Trabajo. Estos elementos se relacionan con la información propuesta por COBIT 5 para cada proceso. En el Nivel 1 se evalúa el atributo Rendimiento del proceso a través del cumplimiento de las actividades y los documentos de entrada y salida. [11]

Esta actividad consiste en analizar estos 3 elementos y diseñar la metodología para la elaboración del instrumento que evaluará el nivel de logro que tiene cada Resultado. Se tomará como referencia la Plantilla de Autoevaluación.

Actividad 3.3. Evaluación Nivel 2 – 5: Análisis de las Prácticas Genéricas (GP) y los Producto de Trabajo Genéricos (GWP)

Para la evaluación de los Niveles 2 al 5, COBIT establece 2 atributos por nivel. La evaluación de estos atributos se hace a través del cumplimiento de las Prácticas Genéricas y los Documentos de Trabajo Genéricos, estos se aplican a todos los procesos.[11]

Esta actividad consiste en analizar las prácticas genéricas y los productos de trabajo genéricos por cada atributo y por cada nivel para luego diseñar la metodología para la elaboración del instrumento que se utilizará para la evaluación de los procesos en estos niveles.

Actividad 3.4. Diseño del modelo ECP (Evaluación de la Capacidad de Procesos) de la universidad

Esta actividad consiste en diseñar el modelo, describiendo sus fases y elementos, de acuerdo a la investigación realizada y a los resultados obtenidos. Se debe mencionar, que el Modelo ECP inicia con el alineamiento de la TI a la estrategia de la organización y termina con la evaluación de los procesos que se identificaron, aportan al logro de los objetivos organizacionales.

3.5.4. Etapa IV: Aplicación de la caracterización formal de la evaluación de la capacidad de procesos de TI de la universidad

Luego de diseñada la Fase 3 del Modelo ECP, la siguiente etapa es la aplicación y validación de esta fase del modelo. Para este fin seleccionamos uno de los procesos que se alinean con la estrategia de la universidad (obtenido a través de la Cascada de Metas). En primer lugar, se realiza un estudio sobre el proceso y su adaptación con la realidad de la universidad. Luego, utilizando el modelo elaboramos los instrumentos de evaluación que serán aplicados.

Actividad 4.1. Evaluación del Nivel 1 del proceso DSS05 Gestionar los servicios de seguridad

Esta actividad consiste en evaluar el atributo 1.1. Rendimiento del proceso correspondiente al Nivel 1 del PAM. Para tal fin, se aplica la caracterización formal para la evaluación de la capacidad del proceso en el Nivel 1 para elaborar el instrumento de evaluación con el que se medirá la capacidad del proceso DSS05 Gestionar los servicios de seguridad.

Actividad 4.2. Evaluación del Nivel 2-5 del proceso DSS05 Gestionar los servicios de seguridad

Esta actividad consiste en evaluar los atributos de los niveles 2 al 5 del PAM. Para tal fin, se aplica la caracterización formal para la evaluación de la capacidad del proceso en los Niveles 2 al 5, con los que se medirá la capacidad del proceso DSS05 Gestionar los servicios de seguridad.

3.6. Validación del Modelo de Evaluación de la Capacidad de Procesos de TI de la universidad

El Modelo ECP fue sometido a una validación por juicio de expertos. Este tipo de validación se define como una opinión informada de personas con trayectoria y experiencia demostrada en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones. [22] Para que los expertos emitan un juicio sobre el modelo ECP, se elaboró un instrumento que en función a cinco criterios medía la validez de cada fase y actividad del modelo. La Figura 21 muestra el instrumento de validación utilizado.

INSTRUMENTO PARA VALIDACIÓN DEL MODELO DE EVALUACIÓN DE LA CAPACIDAD DE PROCESOS PARA EL GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN COBIT 5
(JUICIO DE EXPERTO)

Nombre de experto:
Especialidad:
Cargo/Empresa:

N°	ETAPAS/ FASES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Congruencia[4]		Contexto[5]		Sugerencias
	NOMBRE DE LA ETAPA O FASE	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	
1	Alineamiento de TI con la universidad											
1.1.	Identificación y definición de las partes interesadas internas y externas de la organización											
1.2.	Identificación de las necesidades de las partes interesadas											
1.3.	Definición de la relación entre las necesidades de las partes interesadas y los objetivos estratégicos de la organización											
1.4.	Definición de la relación entre los objetivos estratégicos de la organización y las metas de TI de COBIT 5											
1.5.	Definición de la relación entre las metas de TI y los procesos de COBIT 5											
2	Definición del Modelo de Referencia de Procesos para el gobierno y gestión de la TI de la universidad											
2.1.	Elaboración del modelo de referencia de procesos de la universidad											
2.2.	Adaptación de los procesos del modelo de referencia de procesos al contexto de la unviersidad											
3	Caracterización formal del modelo de Evaluación de la Capacidad de Procesos de la universidad											
3.1.	Caracterización de la evaluación del Nivel 1											
3.2.	Caracterización de la evaluación del Nivel 2 al Nivel 5											

CRITERIOS	
1	Se entiende con facilidad
2	La información presentada aporta significativamente a la fase o etapa
3	Utiliza los aspectos teóricos básicos para fundamentar la propuesta
4	Tiene relación coherente con la propuesta planteada
5	Está contextualizada a la realidad del estudio.

En mi opinión, el modelo revisado es:

	1. Aplicable
	2. Aplicable después de corregir
	3. No aplicable

Firma

Fecha:

Figura 21 - Instrumento de validación por juicio de expertos

Los criterios de validación utilizados fueron: Claridad, Pertinencia, Relevancia, Congruencia y Contexto. El significado de cada uno se explica a continuación:

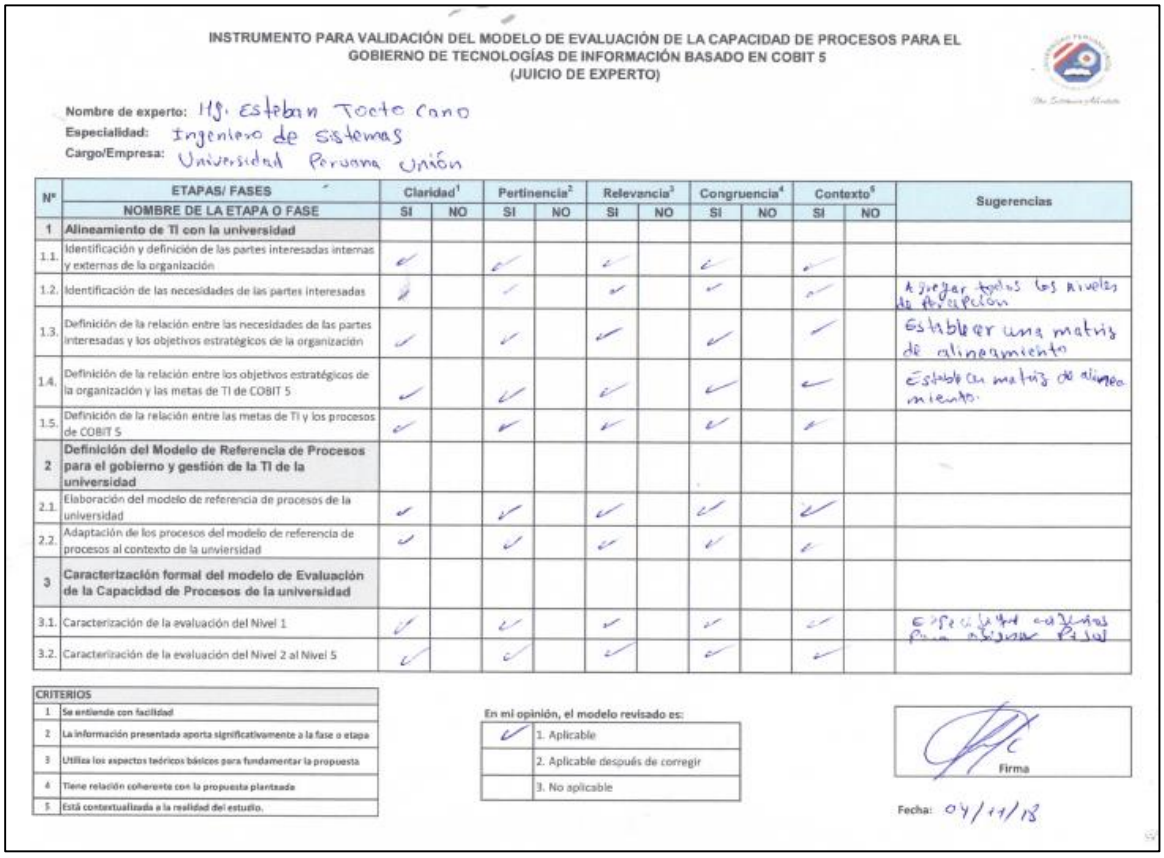
- **Claridad**: hace referencia a que el contenido de las fases y actividades del modelo ECP se entienden con facilidad.
- **Pertinencia**: se refiere a que la información presentada aporta significativamente a cada fase y actividad del modelo ECP.

- **Relevancia**: significa que el modelo ECP utiliza los aspectos teóricos básicos para fundamentar la propuesta.
- **Congruencia**: hace referencia que cada fase del modelo ECP tiene una relación coherente.
- **Contexto**: significa que el modelo ECP está contextualizado a la realidad del estudio.

Se seleccionaron a cuatro (4) expertos que son profesionales con experiencia y trayectoria demostrada en el ámbito académico y de las tecnologías de información. Cada experto fue notificado a través de una carta en la que se solicitaba su valioso apoyo con la investigación, a la carta se adjuntó el modelo ECP y la explicación de cómo fue su desarrollo y la aplicación en el contexto de la universidad objeto de estudio. Los expertos fueron:

- Mg. Esteban Tocto Cano, de profesión Ingeniero de Sistemas.
- Mg. José Bustamante Romero, de profesión Ingeniero de Sistemas
- Ing. Carlos Saavedra Vásconez, de profesión Ingeniero de Sistemas
- Ing. Elder Arohuanca Lagos, de profesión

A continuación, se presentan los resultados de la validación de cada uno de los expertos, (ver las Figuras 22 al 25)



INSTRUMENTO PARA VALIDACIÓN DEL MODELO DE EVALUACIÓN DE LA CAPACIDAD DE PROCESOS PARA EL GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN COBIT 5
(JUICIO DE EXPERTO)

Nombre de experto: Mg. Esteban Tocto Cano
Especialidad: Ingeniero de Sistemas
Cargo/Empresa: Universidad Peruana Unión

Nº	ETAPAS/ FASES / NOMBRE DE LA ETAPA O FASE	Claridad[1] SI	Claridad[1] NO	Pertinencia[2] SI	Pertinencia[2] NO	Relevancia[3] SI	Relevancia[3] NO	Congruencia[4] SI	Congruencia[4] NO	Contexto[5] SI	Contexto[5] NO	Sugerencias
1	**Alineamiento de TI con la universidad**											
1.1.	Identificación y definición de las partes interesadas internas y externas de la organización	✓		✓		✓		✓		✓		
1.2.	Identificación de las necesidades de las partes interesadas	✓		✓		✓		✓		✓		Agregar todos los niveles de ejecución
1.3.	Definición de la relación entre las necesidades de las partes interesadas y los objetivos estratégicos de la organización	✓		✓		✓		✓		✓		Establecer una matriz de alineamiento
1.4.	Definición de la relación entre los objetivos estratégicos de la organización y las metas de TI de COBIT 5	✓		✓		✓		✓		✓		Establecer matriz de alineamiento.
1.5.	Definición de la relación entre las metas de TI y los procesos de COBIT 5	✓		✓		✓		✓		✓		
2	**Definición del Modelo de Referencia de Procesos para el gobierno y gestión de la TI de la universidad**											
2.1.	Elaboración del modelo de referencia de procesos de la universidad	✓		✓		✓		✓		✓		
2.2.	Adaptación de los procesos del modelo de referencia de procesos al contexto de la unviersidad	✓		✓		✓		✓		✓		
3	**Caracterización formal del modelo de Evaluación de la Capacidad de Procesos de la universidad**											
3.1.	Caracterización de la evaluación del Nivel 1	✓		✓		✓		✓		✓		Especificar entradas para obtener Rating
3.2.	Caracterización de la evaluación del Nivel 2 al Nivel 5	✓		✓		✓		✓		✓		

CRITERIOS	
1	Se entiende con facilidad
2	La información presentada aporta significativamente a la fase o etapa
3	Utiliza los aspectos teóricos básicos para fundamentar la propuesta
4	Tiene relación coherente con la propuesta planteada
5	Está contextualizada a la realidad del estudio.

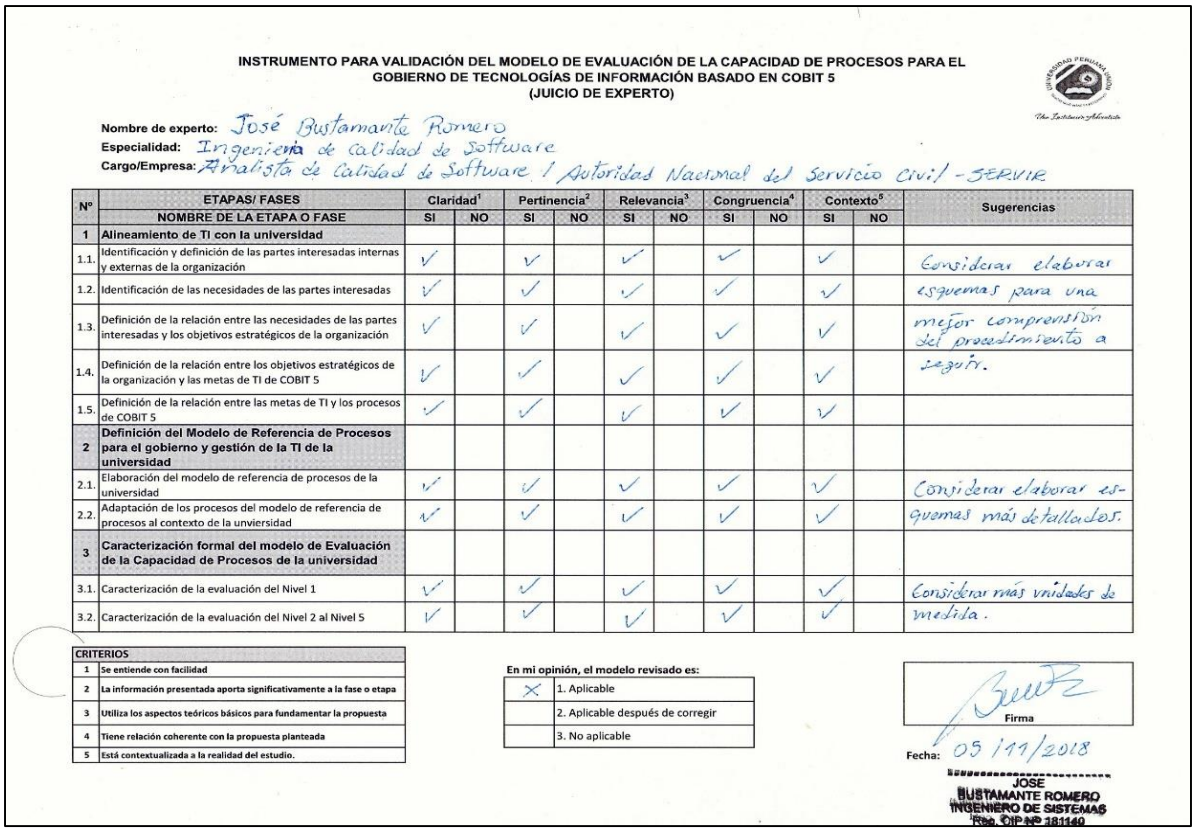
En mi opinión, el modelo revisado es:

✓	1. Aplicable
	2. Aplicable después de corregir
	3. No aplicable

Firma

Fecha: 04/11/18

Figura 22 - Validación del modelo ECP por juicio del Experto 01



INSTRUMENTO PARA VALIDACIÓN DEL MODELO DE EVALUACIÓN DE LA CAPACIDAD DE PROCESOS PARA EL GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN COBIT 5
(JUICIO DE EXPERTO)

Nombre de experto: José Bustamante Romero
Especialidad: Ingeniería de Calidad de Software
Cargo/Empresa: Analista de Calidad de Software / Autoridad Nacional del Servicio Civil - SERVIR

Nº	ETAPAS/ FASES NOMBRE DE LA ETAPA O FASE	Claridad[1] SI	Claridad[1] NO	Pertinencia[2] SI	Pertinencia[2] NO	Relevancia[3] SI	Relevancia[3] NO	Congruencia[4] SI	Congruencia[4] NO	Contexto[5] SI	Contexto[5] NO	Sugerencias
1	**Alineamiento de TI con la universidad**											
1.1.	Identificación y definición de las partes interesadas internas y externas de la organización	✓		✓		✓		✓		✓		Considerar elaborar
1.2.	Identificación de las necesidades de las partes interesadas	✓		✓		✓		✓		✓		esquemas para una
1.3.	Definición de la relación entre las necesidades de las partes interesadas y los objetivos estratégicos de la organización	✓		✓		✓		✓		✓		mejor comprensión
1.4.	Definición de la relación entre los objetivos estratégicos de la organización y las metas de TI de COBIT 5	✓		✓		✓		✓		✓		del procedimiento a
1.5.	Definición de la relación entre las metas de TI y los procesos de COBIT 5	✓		✓		✓		✓		✓		seguir.
2	**Definición del Modelo de Referencia de Procesos para el gobierno y gestión de la TI de la universidad**											
2.1.	Elaboración del modelo de referencia de procesos de la universidad	✓		✓		✓		✓		✓		Considerar elaborar es-
2.2.	Adaptación de los procesos del modelo de referencia de procesos al contexto de la unviersidad	✓		✓		✓		✓		✓		quemas más detallados.
3	**Caracterización formal del modelo de Evaluación de la Capacidad de Procesos de la universidad**											
3.1.	Caracterización de la evaluación del Nivel 1	✓		✓		✓		✓		✓		Considerar más unidades de
3.2.	Caracterización de la evaluación del Nivel 2 al Nivel 5	✓		✓		✓		✓		✓		medida.

CRITERIOS	
1	Se entiende con facilidad
2	La información presentada aporta significativamente a la fase o etapa
3	Utiliza los aspectos teóricos básicos para fundamentar la propuesta
4	Tiene relación coherente con la propuesta planteada
5	Está contextualizada a la realidad del estudio.

En mi opinión, el modelo revisado es:

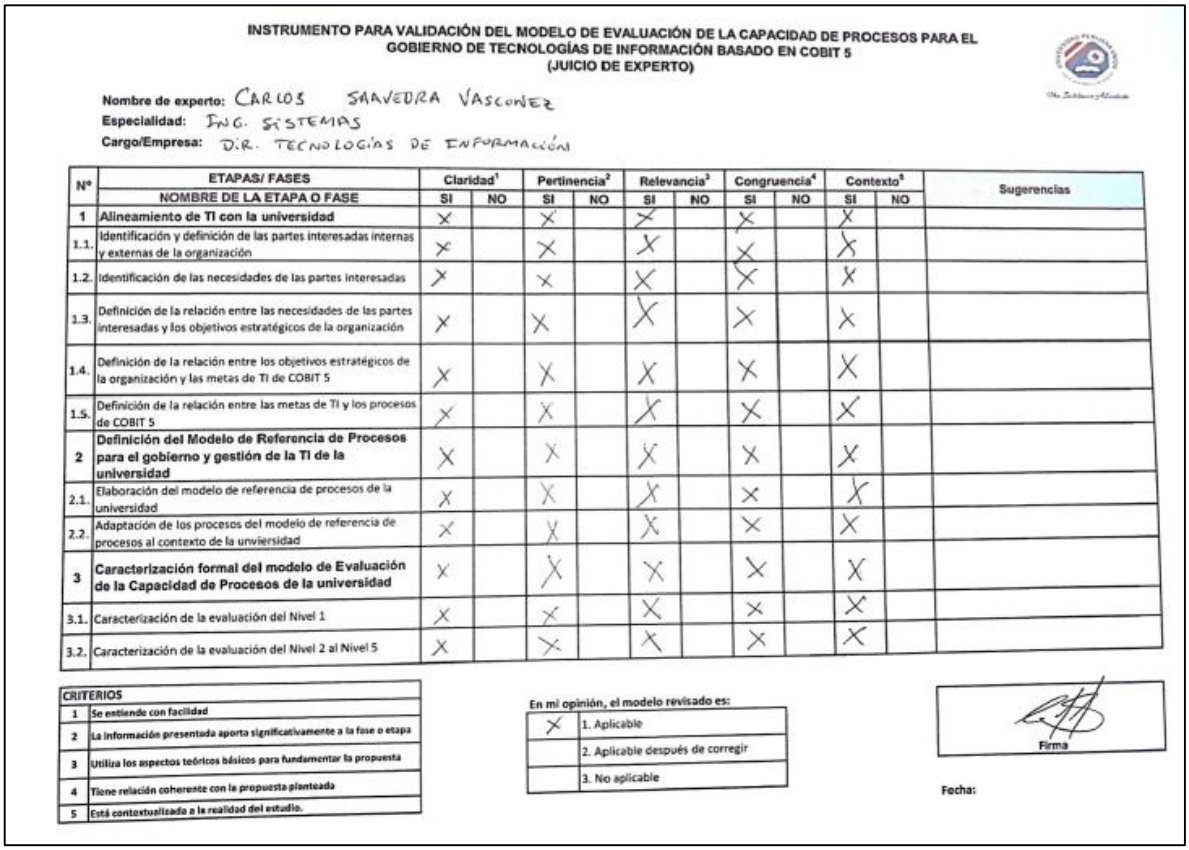
✓	1. Aplicable
	2. Aplicable después de corregir
	3. No aplicable

Firma

Fecha: 05/11/2018

JOSE BUSTAMANTE ROMERO
INGENIERO DE SISTEMAS
Reg. CIP Nº 181140

Figura 23 - Validación del modelo ECP por juicio del Experto 02



INSTRUMENTO PARA VALIDACIÓN DEL MODELO DE EVALUACIÓN DE LA CAPACIDAD DE PROCESOS PARA EL GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN COBIT 5
(JUICIO DE EXPERTO)

Nombre de experto: CARLOS SAAVEDRA VASCONEZ
Especialidad: ING. SISTEMAS
Cargo/Empresa: D.R. TECNOLOGÍAS DE INFORMACIÓN

Nº	ETAPAS/ FASES NOMBRE DE LA ETAPA O FASE	Claridad[1] SI	Claridad[1] NO	Pertinencia[2] SI	Pertinencia[2] NO	Relevancia[3] SI	Relevancia[3] NO	Congruencia[4] SI	Congruencia[4] NO	Contexto[5] SI	Contexto[5] NO	Sugerencias
1	**Alineamiento de TI con la universidad**	X		X		X		X		X		
1.1.	Identificación y definición de las partes interesadas internas y externas de la organización	X		X		X		X		X		
1.2.	Identificación de las necesidades de las partes interesadas	X		X		X		X		X		
1.3.	Definición de la relación entre las necesidades de las partes interesadas y los objetivos estratégicos de la organización	X		X		X		X		X		
1.4.	Definición de la relación entre los objetivos estratégicos de la organización y las metas de TI de COBIT 5	X		X		X		X		X		
1.5.	Definición de la relación entre las metas de TI y los procesos de COBIT 5	X		X		X		X		X		
2	**Definición del Modelo de Referencia de Procesos para el gobierno y gestión de la TI de la universidad**	X		X		X		X		X		
2.1.	Elaboración del modelo de referencia de procesos de la universidad	X		X		X		X		X		
2.2.	Adaptación de los procesos del modelo de referencia de procesos al contexto de la unviersidad	X		X		X		X		X		
3	**Caracterización formal del modelo de Evaluación de la Capacidad de Procesos de la universidad**	X		X		X		X		X		
3.1.	Caracterización de la evaluación del Nivel 1	X		X		X		X		X		
3.2.	Caracterización de la evaluación del Nivel 2 al Nivel 5	X		X		X		X		X		

CRITERIOS	
1	Se entiende con facilidad
2	La información presentada aporta significativamente a la fase o etapa
3	Utiliza los aspectos teóricos básicos para fundamentar la propuesta
4	Tiene relación coherente con la propuesta planteada
5	Está contextualizada a la realidad del estudio.

En mi opinión, el modelo revisado es:

X	1. Aplicable
	2. Aplicable después de corregir
	3. No aplicable

Firma

Fecha:

Figura 24 - Validación del modelo ECP por juicio del Experto 03

De acuerdo con lo expresado por los expertos en sus validaciones, el Modelo de Evaluación de la Capacidad de Procesos de TI (ECP) desarrollado y aplicado en la presente investigación es aplicable.

CAPÍTULO IV: INGENIERÍA DE LA PROPUESTA

4.1. Alcance del proyecto

Para el logro del objetivo de la investigación que es diseñar un modelo de evaluación de la capacidad de procesos para el gobierno y gestión de tecnologías de información, basado en las buenas prácticas de COBIT 5, se requiere acceder a información que permita conocer la filosofía, el comportamiento y las operaciones sobre las cuáles la universidad basa su funcionamiento. En ese sentido, el alcance del proyecto comprende los objetivos estratégicos y los procesos del negocio establecidos en el Plan Estratégico 2014 – 2018 v2. A la vez, se requiere conocer las necesidades de las partes interesadas internas y externas, para lo cual se incluye dentro del alcance a administradores, docentes, personal no docente, estudiantes, padres de familia y entidades externas. Por otro lado, para la aplicación y validación del modelo se considera al proceso DSS05 Gestionar los servicios de seguridad de COBIT 5, que también se incluye en el alcance.

4.2. Entregables a producir

La Tabla 2, Entregables de la investigación, muestra los documentos resultantes de cada etapa de la investigación.

Tabla 2 - Entregables de la investigación

Etapas de la investigación	Entregable
Etapa I: Alineamiento de la TI con la estrategia de la universidad	Cuadro de alineamiento de la TI con la estrategia de la universidad
Etapa II: Definición del modelo de Referencia de Procesos para el gobierno de TI en la universidad	Modelo de referencia de procesos para el gobierno de TI de la universidad
Etapa III: Caracterización formal de la Evaluación de la Capacidad de Procesos de la universidad	Caracterización formal de la evaluación de la capacidad de procesos del Nivel 1 y de los Niveles 2 al 5.
Etapa IV: Aplicación de la caracterización de la evaluación de la capacidad de procesos de la universidad	Resultados de la aplicación de la evaluación de la capacidad el proceso DSS05 Gestionar los servicios de seguridad de la universidad

4.3. Desarrollo e implementación

Etapa I: Alineamiento de las TI con la estrategia de la universidad

Para realizar el alineamiento de las TI con la estrategia de la universidad se aplicó el mecanismo de la Cascada de Metas, cuyo funcionamiento se explicó en el Capítulo II, apartado 2.2.4.

Actividad 1.1. Identificación y definición de las partes interesadas internas y externas

El mecanismo de la Cascada de Metas inicia con la identificación de las necesidades de las partes interesadas. Por lo tanto, la primera actividad en el desarrollo del modelo fue identificar a las partes interesadas de la universidad.

Las partes interesadas internas y externas de la universidad se identificaron de acuerdo a la función que realizan y su nivel de influencia sobre los procesos de negocio. La Figura 25 muestra el Mapa de Procesos de negocio de la universidad, este mapa está organizado en tres grupos de procesos: estratégicos, de formación y de apoyo.

Se utilizó este mapa de procesos con el fin de identificar las partes interesadas que se relacionan con cada proceso. Se consideraron a los administradores estratégicos, administradores tácticos, personal operativo, personal administrativo, estudiantes, docentes, padres de familia, instituciones externas, entre otros.

La Tabla 3 muestra la lista de las partes interesadas internas y externas de la universidad, el grupo de procesos con el que se relacionan y una breve descripción sobre la función que cumplen.

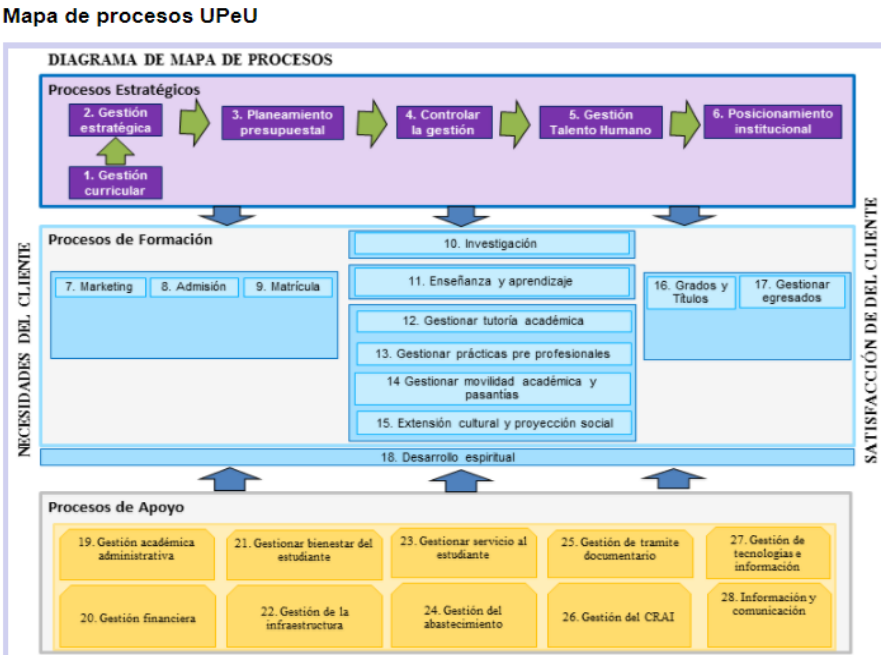


Figura 25 - Mapa de procesos de la Universidad

Tabla 3 - Partes interesadas internas y externas de la universidad

Nª	Parte interesada	Grupo de proceso	Descripción
Partes interesadas internas			
1	Rector	Estratégico	Es la máxima autoridad de la universidad
2	Gerente General	Estratégico De apoyo	Es el responsable de la gestión financiera e infraestructura
3	Vicerrector	Estratégico De formación	Es el responsable de la gestión académica en pregrado y posgrado
4	Director de Bienestar Universitario	Estratégico De apoyo	Es responsable de la gestión de los servicios educacionales complementarios
5	Decanos de facultades	Estratégico De formación	Son responsables de la gestión académica y financiera de una unidad académica (facultad)
6	Director de Escuela de Posgrado	Estratégico De formación	Es responsable de la gestión académica y financiera de la Escuela de Posgrado
7	Director de PROESAD	De formación	Es responsable de la gestión académica y financiera de PROESAD
8	Director de Investigación	De formación	Es responsable de gestionar la visibilidad científica de la universidad
9	Gerente Financiero	De apoyo	Es responsable de asistir en la gestión financiera
10	Director de Admisión	De formación	Es responsable de la gestión de los postulantes e ingresantes en pregrado y posgrado
11	Estudiantes pregrado	De formación	Son los beneficiarios directos de los programas académicos de pregrado
12	Estudiantes posgrado	De formación	Son los beneficiarios directos de los programas académicos de posgrado
13	Docentes	De formación	Son los responsables de brindar los conocimientos y habilidades en la formación profesional
14	Personal administrativo	De apoyo	Son los responsables de brindar los servicios administrativos complementarios en cada unidad académica
15	Personal de servicio/apoyo	De apoyo	Son los responsables de brindar los servicios de apoyo
Partes interesadas externas			
16	Padres de familia/apoderados	De formación	Son los que
17	Proveedores	De apoyo	
18	Promotora	De formación	Es la encargada de establecer los lineamientos y políticas sobre las cuáles se desarrollan las actividades de la universidad
19	IASD	De formación	Es el mercado ocupacional donde se desempeñan laboralmente los egresados
20	Comunidad	De formación	Es el mercado ocupacional donde se desempeñan laboralmente los egresados

Actividad 1.2. Identificación de las necesidades de las partes interesadas

Una vez identificadas las partes interesadas, lo siguiente fue identificar cuáles eran sus necesidades respecto a las tecnologías de información en la función en la que se desempeñaban.

COBIT 5 incluye una lista de las "típicas cuestiones de gobierno y gestión sobre la TI", esta lista ha sido explicada en el Capítulo II, en el apartado 2.2.4. La idea es conocer cuáles de estas cuestiones se corresponden con las metas corporativas según lo expresen las partes interesadas internas y externas.

El contexto y situación de cada empresa es diferente, por lo que no debe usarse la información de esta lista como un asunto mecánico, sino tomarla como sugerencia de un conjunto genérico de necesidades de las partes interesadas, analizarla y contextualizarla de acuerdo a la realidad de la empresa.

En este sentido, para identificar las necesidades de las partes interesadas de la universidad, se analizaron las 22 cuestiones típicas de gobierno y gestión propuestas por COBIT, las contextualizamos a la situación actual de la universidad y finalmente elaboramos una lista de las necesidades de las partes interesadas acorde a la realidad de la universidad. La Tabla 4 muestra el análisis realizado.

Tabla 4 - Análisis y contextualización de las necesidades de las partes interesadas de la universidad

	Necesidades de las partes interesadas de COBIT 5		Necesidades de las partes interesadas de la universidad	Parte interesada Interna / Externa
1	¿Cómo se consigue valor mediante el uso de TI? ¿Está el usuario final satisfecho con la calidad del servicio de TI?	1	Las tecnologías de información de la universidad aportan valor a la organización	Interna
		2	Los servicios de tecnologías de información cubren las expectativas de los usuarios	Interna/Externa
2	¿Cómo se gestiona el rendimiento de TI?	3	El rendimiento de las tecnologías de información es el adecuado para la universidad	Interna
3	¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?	4	Las tecnologías de información que tiene la universidad permiten nuevas oportunidades para mejorar los servicios educativos que se ofrecen	Interna/Externa
4	¿Cómo puedo construir y estructurar mejor mi departamento de TI	5	El área de tecnologías de información de la universidad está estructurada y organizada	Interna
5	¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?	6	Los servicios de tecnologías de información externos (proveedores) son gestionados conforme a los contratos establecidos (garantías)	Interna/Externa
6	¿Cuáles son los requisitos de control para la información?	7	La universidad tiene requisitos de control para el manejo de la información	Interna
7	¿He contemplado todo los riesgos relacionados con TI?	8	La universidad tiene identificados y gestionados los riesgos asociados a las tecnologías de información	Interna
8	¿Estoy ejecutando una operación de TI eficiente y robusta?	9	Las tecnologías de información de la universidad operan de forma eficiente y confiable.	Interna
9	¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?	10	Los costos de las tecnologías de información de la universidad son controlados	Interna
		11	Los recursos de tecnologías de información usados de forma efectiva y eficiente	Interna
10	¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento?	12	El área de tecnologías de información de la universidad tiene suficiente personal para atender las necesidades tecnológicas de la universidad	Interna

		13	Existe un plan de capacitación y perfeccionamiento para el personal del área de tecnologías de información de la universidad	Interna
		14	El rendimiento del personal del área de tecnologías de información de la universidad es gestionado	Interna
11	¿Cómo consigo confianza sobre TI?	15	Los servicios de tecnologías de información que se ofrecen a la universidad son confiables	Interna
12	¿Está bien securizada la información que se está procesando?	16	La información de la universidad que se gestiona a través de las tecnologías de información está segura y protegida.	Interna/Externa
13	¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible?	17	Las tecnologías de información de la universidad permiten la innovación del servicio educativo y su adaptación al entorno cambiante	Interna/Externa
14	¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? ¿Por qué permanece la TI en el camino de ejecutar la estrategia de negocio?	18	Los proyectos de tecnologías de información emprendidos se cumplen en tiempo y costos alcanzando los objetivos trazados.	Interna/Externa
15	¿Cómo es de crítica la TI para la sostenibilidad de la empresa?¿Qué pasaría si la TI no estuviera disponible?	19	Las tecnologías de información son críticas (importantes, vitales, imprescindibles) para la entrega del servicio educativo en la universidad	Interna
16	¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?	20	Los procesos críticos de la universidad (admisión, matrícula, enseñanza, investigación, entre otros) dependen de las tecnologías de información	Interna/Externa
17	¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?	21	Los gastos o inversiones en tecnologías de información se ajustan a los presupuestos	Interna
18	¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?	22	El área de tecnologías de información normalmente está "apagando fuegos" en lugar de facilitar las mejoras a la universidad	Interna
19	¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa?	23	Los recursos e infraestructura de tecnologías de información son suficientes para lograr los objetivos estratégicos de la universidad	Interna
20	¿Cuánto se tarda en la toma de decisiones importantes de TI?	24	Las decisiones sobre tecnologías de información se toman de forma oportuna.	Interna
21	¿Son transparentes el esfuerzo y las inversiones totales de TI?	25	Las inversiones en tecnologías de información son transparentes y adecuadas a las necesidades de la universidad	Interna
22	¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?	26	Las tecnologías de información de la universidad la respaldan en el cumplimiento de las leyes y normas de todo tipo.	Interna

Con esta lista se elaboró una encuesta que contenía los 26 ítems y 5 niveles de conformidad. La encuesta se aplicó a las partes interesadas para identificar como es que ellos percibían cada una de estas cuestiones. El resultado de este análisis se observa en la Tabla 5, esta percepción

permitió enfocar mejor la lista al momento de relacionarlas con los objetivos del Plan Estratégico de la universidad.

Tabla 5 - Percepción de las partes interesadas sobre las necesidades de TI de la universidad

	Necesidades de las partes interesadas de la universidad		Percepción de las partes interesadas
1	Las tecnologías de información de la universidad aportan valor a la organización	4	Muy de acuerdo
2	Los servicios de tecnologías de información cubren las expectativas de los usuarios	4	Muy de acuerdo
3	El rendimiento de las tecnologías de información es el adecuado para la universidad	3	Ni de acuerdo, ni en desacuerdo
4	Las tecnologías de información que tiene la universidad permiten nuevas oportunidades para mejorar los servicios educativos que se ofrecen	4	Muy de acuerdo
5	El área de tecnologías de información de la universidad está estructurada y organizada	4	Muy de acuerdo
6	Los servicios de tecnologías de información externos (proveedores) son gestionados conforme a los contratos establecidos (garantías)	3	Ni de acuerdo, ni en desacuerdo
7	La universidad tiene requisitos de control para el manejo de la información	2	Poco de acuerdo
8	La universidad tiene identificados y gestionados los riesgos asociados a las tecnologías de información	2	Poco de acuerdo
9	Las tecnologías de información de la universidad operan de forma eficiente y confiable.	2	Poco de acuerdo
10	Los costos de las tecnologías de información de la universidad son controlados	2	Poco de acuerdo
11	Los recursos de tecnologías de información usados de forma efectiva y eficiente	2	Poco de acuerdo
12	El área de tecnologías de información de la universidad tiene suficiente personal para atender las necesidades tecnológicas de la universidad	3	Ni de acuerdo, ni en desacuerdo
13	Existe un plan de capacitación y perfeccionamiento para el personal del área de tecnologías de información de la universidad	3	Ni de acuerdo, ni en desacuerdo
14	El rendimiento del personal del área de tecnologías de información de la universidad es gestionado	3	Ni de acuerdo, ni en desacuerdo
15	Los servicios de tecnologías de información que se ofrecen a la universidad son confiables	4	Muy de acuerdo
16	La información de la universidad que se gestiona a través de las tecnologías de información está segura y protegida.	3	Ni de acuerdo, ni en desacuerdo
17	Las tecnologías de información de la universidad permiten la innovación del servicio educativo y su adaptación al entorno cambiante	4	Muy de acuerdo
18	Los proyectos de tecnologías de información emprendidos se cumplen en tiempo y costos alcanzando los objetivos trazados.	3	Ni de acuerdo, ni en desacuerdo
19	Las tecnologías de información son críticas (importantes, vitales, imprensindibles) para la entrega del servicio educativo en la universidad	4	Muy de acuerdo
20	Los procesos críticos de la universidad (admisión, matrícula, enseñanza, investigación, entre otros) dependen de las tecnologías de información	4	Muy de acuerdo
21	Los gastos o inversiones en tecnologías de información se ajustan a los presupuestos	3	Ni de acuerdo, ni en desacuerdo
22	El área de tecnologías de información normalmente está "apagando fuegos" en lugar de facilitar las mejoras a la universidad	3	Ni de acuerdo, ni en desacuerdo

23	Los recursos e infraestructura de tecnologías de información son suficientes para lograr los objetivos estratégicos de la universidad	3	Ni de acuerdo, ni en desacuerdo
24	Las decisiones sobre tecnologías de información se toman de forma oportuna.	4	Muy de acuerdo
25	Las inversiones en tecnologías de información son transparentes y adecuadas a las necesidades de la universidad	3	Ni de acuerdo, ni en desacuerdo
26	Las tecnologías de información de la universidad la respaldan en el cumplimiento de las leyes y normas de todo tipo.	4	Muy de acuerdo

Actividad 1.3. Definición de la relación entre las necesidades de las partes interesadas y los objetivos estratégicos de la organización

En el primer nivel de la cascada de metas, se relacionan las necesidades de las partes interesadas con las metas corporativas. COBIT 5 propone una lista de 17 metas corporativas que son el resultado una investigación realizada por la Escuela de Negocios de Alineamiento de TI de la Universidad de Amberes y el Instituto de Gobierno de Bélgica. La Tabla 6 muestra las 17 metas corporativas organizadas de acuerdo a las perspectivas del BSC.[4]

Tabla 6 - Metas corporativas de COBIT 5

Dimensión BSC		Meta Corporativa
Financiera	1	Valor para las partes interesadas de las inversiones de negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados
	4	Cumplimiento de leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de decisiones basada en información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje y	16	Personas preparadas y motivadas
Crecimiento	17	Cultura de innovación de producto y negocio

Sin embargo, COBIT recomienda no usar el mecanismo de la cascada y sus elementos de manera mecánica pues cada organización tiene sus propios objetivos y prioridades que cambian con el tiempo. Por lo tanto, cuando una organización va a utilizar la cascada de metas, debe personalizarla teniendo en cuenta su situación específica. [4].

La universidad en estudio cuenta con un Plan Estratégico (PE) para el quinquenio 2014-2018, donde se especifican los objetivos estratégicos que serían las metas corporativas. El PE

está estructurado por Ejes estratégicos los que albergan los objetivos. Los objetivos estratégicos por cada eje se pueden ver en los mapas estratégicos en la sección Anexos.

En la Actividad 1.2. analizamos la percepción que tienen las partes interesadas sobre sus necesidades de TI respecto a la universidad. Tomando como base el resultado de este análisis se realizó el análisis del primer nivel de la cascada, la relación entre los objetivos estratégicos con las necesidades de las partes interesadas.

De acuerdo a los mapas estratégicos de cada eje, la universidad cuenta con 38 objetivos estratégicos. Se consideraron la totalidad de los objetivos para el análisis del primer nivel de la cascada de metas. El resultado fue, de los 38 objetivos estratégicos que tiene el PE de la universidad, se identificaron 22 como los más importantes que satisfacen las necesidades de las partes interesadas. La Tabla 7 muestra los 22 objetivos estratégicos que se consideraron para el análisis de la cascada de metas.

Tabla 7 - Objetivos estratégicos o Metas corporativas de la universidad

Dimensión		Meta Corporativa
Financiero	1	Consolidar el programa de becas y servicios para el desarrollo integral
Aprendizaje	2	Contar con docentes capacitados y especializados
	3	Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
	4	Incrementar los investigadores activos en redes de investigación
	5	Desarrollar capacidades en investigación
	6	Ampliar la disponibilidad y uso de biblioteca virtual
	7	Desarrollar competencias para proyectos y programas
Procesos	8	Lograr una planificación de Enseñanza – Aprendizaje acorde a los estándares
	9	Alcanzar la excelencia en el desarrollo de las sesiones de clase
	10	Consolidar la atención en tutorías
	11	Alcanzar la efectividad de la gestión de prácticas pre profesionales
	12	Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
	13	Lograr la eficacia de los procesos de investigación científica
	14	Fortalecer la cultura de investigación en diferentes niveles de enseñanza
	15	Alcanzar participación activa en proyectos según líneas de investigación
	16	Lograr que los estudiantes y docentes registren proyectos según líneas de investigación
	17	Administrar banco de problemas y necesidades
	18	Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual
Clientes	19	Lograr el posicionamiento y reconocimiento en la IASD y la sociedad
	20	Fidelizar a la comunidad educativa
	21	Difundir la producción intelectual en diferentes medios
	22	Lograr posicionamiento por el logro de la investigación

Actividad 1.4. Definición de la relación entre los objetivos estratégicos de la organización y las metas de TI de COBIT 5

En el segundo nivel de la cascada de metas, se analiza la relación entre las metas corporativas y las metas de TI. Para este análisis se consideraron los 22 objetivos estratégicos

o metas corporativas de la universidad que resultaron del análisis del primer nivel de la cascada y las 17 metas de TI que COBIT 5 propone.[4]

Para analizar la relación entre las metas corporativas y las metas de TI se evalúa si la relación es primaria o secundaria. Se asigna una letra P cuando la relación es primaria o principal, y una letra S cuando la relación es secundaria. Finalmente, se consideraron aquellas cuya relación es P, puesto que es la primera vez que se realiza esta alineación y se quería identificar las relaciones más importantes. En esta actividad se analizaron las 22 metas corporativas y su relación con las 17 metas de TI de COBIT 5, obteniendo el resultado que se muestra en la Tabla 8.

Tabla 8 - Metas de TI de la universidad alineadas a las metas corporativas

Dimensión BSC		Meta de TI
Financiera	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	4	Riesgos de negocio relacionados con las TI gestionados
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	9	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
	14	Disponibilidad de información útil y fiable para la toma de decisiones
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado

Del análisis realizado se concluye que 10 de las 17 metas de TI de COBIT 5 se relacionan con las metas corporativas de la universidad.

Actividad 1.5. Definición de la relación entre las Metas de TI y los procesos de COBIT 5

En el último nivel de la cascada de metas se analiza la relación entre las metas del TI y los procesos del Modelo de Referencia de Procesos de COBIT. Para esta actividad se utilizó el Apéndice C del Framework COBIT 5 que muestra los 37 procesos por dominios de gobierno y gestión y su relación con las Metas de TI. Las relaciones entre las metas de TI y los procesos se explicaron en el Capítulo II, apartado 2.2.4.

Para este análisis se consideraron las 10 Metas de TI que resultaron de la Actividad 1.4. y los 37 procesos del Marco de Referencia de Procesos de COBIT 5. Se identificaron las relaciones del tipo P. El resultado fue, 15 procesos que se alinean con las Metas de TI y como

consecuencia a las Metas corporativas de la universidad. La Tabla 9 muestra la relación de los procesos alineados a la estrategia de la universidad.

Tabla 9 - Procesos de gobierno y gestión de TI de la universidad

Dominio		Proceso	Meta TI
EDM	1	EDM04 Asegurar la optimización de recursos	9, 11, 16
APO	2	APO01 Gestionar el marco de Gestión de TI	4,9,11,16
	3	APO04 Gestionar la innovación	8,9,11
	4	APO07 Gestionar los recursos humanos	11,13,16
	5	APO10 Gestionar los proveedores	4,7,9
	6	APO12 Gestionar el riesgo	2,4,10,13
	7	APO13 Gestionar la seguridad	2,4,10,14
BAI	8	BAI04 Gestionar la disponibilidad y la capacidad	7,11,14
	9	BAI06 Gestionar los cambios	4,7,10
	10	BAI10 Gestionar la configuración	2,11,14
DSS	11	DSS01 Gestionar las operaciones	4,7,11
	12	DSS03 Gestionar los problemas	4,7,11,14
	13	DSS04 Gestionar la continuidad	4,7,14
	14	DSS05 Gestionar los servicios de seguridad	2,4,10
MEA	15	MEA01 Supervisar, evaluar y valorar rendimiento y conformidad	4,7,11

Etapa II: Definición del modelo de Referencia de Procesos para el gobierno y gestión de TI en la universidad

Actividad 2.1. Elaboración del Modelo de Referencia de Procesos de la universidad

Cada empresa puede organizar sus procesos de la mejor manera de acuerdo a sus necesidades, siempre y cuando, los objetivos de gobierno y gestión estén cubiertos. Por un lado, las empresas pequeñas tendrán menos procesos implementados, y por otro, las empresas grandes quizá implementen más procesos, todo en función a cubrir los objetivos organizacionales. [18]

El Modelo de Referencia de Procesos de COBIT 5, “define y describe en detalle” los procesos de gobierno y gestión que conforman el framework. Este modelo representa a todos los procesos que “normalmente” existen en una empresa respectos a las actividades de TI y que son entendibles para los gerentes del negocio y de la TI. Cada empresa debe definir su propio modelo de procesos de TI considerando su organización y situación actual. [18]

Esta actividad consistió en organizar los procesos resultantes del desarrollo de la Cascada de Metas aplicado a la universidad de estudio (Ver Tabla 9). Esta organización se hizo en función a los lineamientos dados por COBIT: procesos de gobierno y procesos de gestión. La Figura 26 muestra el Modelo de Referencia de Procesos para el gobierno y gestión de la TI en la Universidad de estudio.

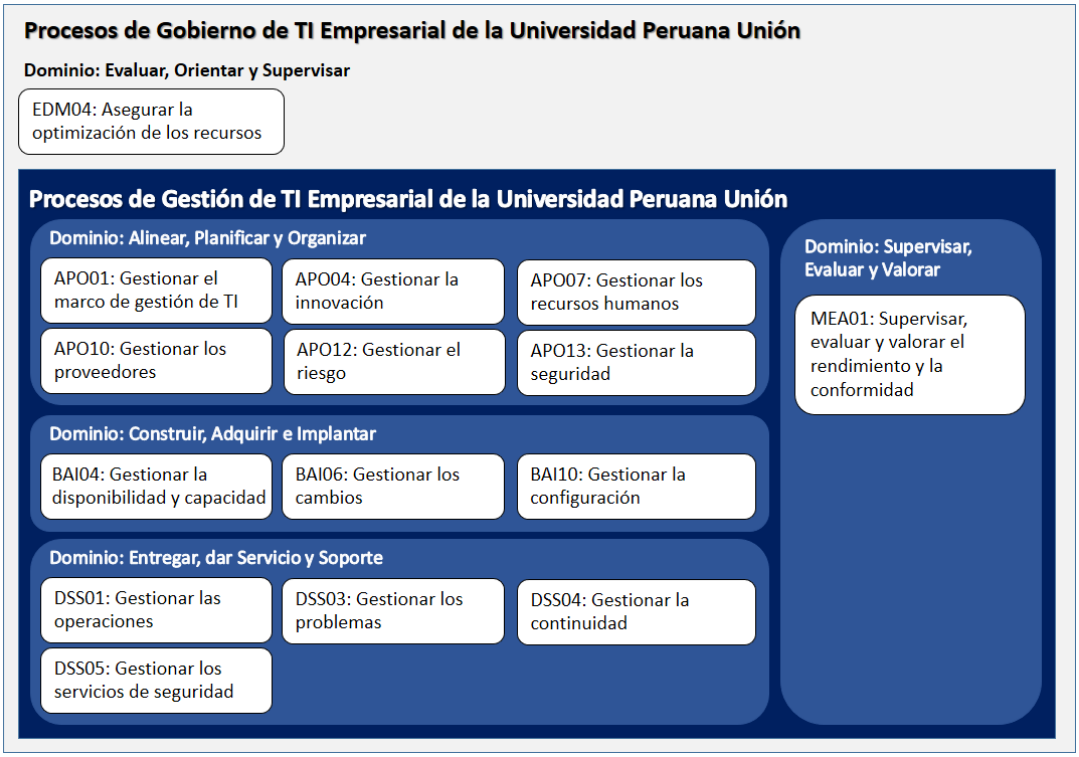


Figura 26 - Modelo de Referencia de procesos de gobierno y gestión de la universidad

Actividad 2.2. Descripción de los procesos del modelo de Referencia de Procesos de la universidad

Los 15 procesos que conforman el Modelo de Referencia de Procesos para la universidad se adaptaron al contexto de la universidad, asignando un dueño del proceso, las partes interesadas internas y externas, la relación con las metas corporativas y metas de TI. La demás información que propone COBIT 5, se mantuvo tal cual, pues son especificaciones de las actividades que se debe realizar en cada práctica de gobierno o gestión del proceso.

En la Tabla 10 se muestra la adaptación del proceso DSS05 Gestionar los servicios de seguridad, proceso utilizado en la investigación para la aplicación del modelo ECP. Este proceso cuenta con 7 prácticas de gestión. Las actividades, entradas y salidas de cada práctica, se han mantenido según lo especificado por COBIT 5. Sin embargo, si se desea implementar el proceso, se debe considerar esta información como una guía, siempre dando prioridad al contexto de la organización. La adaptación de los 14 procesos restantes se puede visualizar en el apartado Anexos.

Tabla 10 - Adaptación del Proceso DSS05 Gestionar los servicios de seguridad

<table>
<tr><td colspan="2">DSS05: Gestionar los servicios de seguridad</td><td>Área: Gestión
Dominio: Entrega, Servicio y Soporte</td></tr>
<tr><td colspan="3">Descripción: Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.</td></tr>
<tr><td colspan="3">Propósito: Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.</td></tr>
<tr><td colspan="2">Dueño del proceso:
Director de DIGETI</td><td>Partes interesadas:
- Vicerrector
- Decanos de facultad
- Director de EPG
- Director de PROESAD
- Director de Investigación
- Estudiantes de pregrado y posgrado
- Docentes
- Personal administrativo</td></tr>
<tr><td colspan="3">Metas corporativas relacionadas:</td></tr>
<tr><td colspan="3">03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes
10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
11 Incrementar los investigadores activos en redes de investigación
13 Ampliar la disponibilidad y uso de biblioteca virtual
20 Alcanzar la excelencia en el desarrollo de las sesiones de clase
23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
24 Lograr la eficacia de los procesos de investigación científica
25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza
28 Administrar banco de problemas y necesidades
31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual
34 Fidelizar a la comunidad educativa
35 Difundir la producción intelectual en diferentes medios
36 Lograr posicionamiento por el logro de la investigación</td></tr>
<tr><td colspan="3">Metas de TI relacionadas:</td></tr>
<tr><td colspan="2">02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas</td><td>- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI.</td></tr>
<tr><td colspan="2">04 Riesgos de negocio relacionados con las TI gestionados</td><td>- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos
- Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos</td></tr>
<tr><td colspan="2">10 Seguridad de la información, infraestructura y aplicaciones</td><td>- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública
- Número de servicios de TI con los requisitos de seguridad pendientes
- Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados</td></tr>
<tr><td colspan="3">Metas del proceso:</td></tr>
<tr><td colspan="2">La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio</td><td>- Número de vulnerabilidades descubiertas
- Número de rupturas (breaches) de cortafuegos</td></tr>
<tr><td colspan="2">La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida</td><td>- Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final
- Número de incidentes que impliquen dispositivos de usuario final
- Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno</td></tr>
</table>

Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio	- Promedio de tiempo entre los cambios y actualizaciones de cuentas - Número de cuentas (con respecto al número de usuarios/empleados autorizados)
Se han implantado medidas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida	- Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno - Clasificación media para las evaluaciones de seguridad física - Número de incidentes relacionados con seguridad física
La información electrónica tiene las medidas de seguridad apropiadas mientas está almacenada, transmitida o destruida	- Número de incidentes relacionados con accesos no autorizados a la información

Prácticas de Gestión

DSS05.01 Proteger contra software malicioso

Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).

Iniciativas y/o Documentos E/S

Entrada: -	Salida: - Política de prevención de software malicioso - Evaluaciones de amenazas potenciales

1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.

DSS05.02 Gestionar la seguridad de la red y las conexiones

Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

Iniciativas y/o Documentos E/S

Entrada: - Guía de clasificación de la información - SLAs	Salida: - Política de seguridad en la conectividad - Resultados de las pruebas de intrusión

Actividades:

1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
4. Cifrar la información en tránsito de acuerdo con su clasificación.
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.
6. Configurar los equipamientos de red de forma segura.
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.

DSS05.03 Gestionar la seguridad de los puestos de usuario final

Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Modelo de arquitectura de la información - SLAs y OLAs - Resultados de pruebas de inventarios físicos	- Política de seguridad para dispositivos de usuario final

Actividades:

1. Configurar los sistemas operativos de forma segura.
2. Implementar mecanismos de bloqueo de los dispositivos.
3. Cifrar la información almacenada de acuerdo a su clasificación.
4. Gestionar el acceso y control remoto.
5. Gestionar la configuración de la red de forma segura.
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
7. Proteger la integridad del sistema.
8. Proveer de protección física a los dispositivos de usuario final.
9. Deshacerse de los dispositivos de usuario final de forma segura.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico

Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Definiciones de roles y responsabilidades relacionadas con TI - Modelo de arquitectura de la información	- Derechos de acceso de los usuarios aprobados - Resultados de las revisiones de cuentas y privilegios de los usuarios

Actividades

1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
5. Segregar y gestionar cuentas de usuario privilegiadas.
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.

DSS05.05 Gestionar el acceso físico a los activos de TI

Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.

Iniciativas y/o Documentos E/S

Entrada	Salida
-	- Peticiones de acceso aprobadas - Registros de acceso

Actividades

1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.
3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.
5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.
7. Realizar regularmente formación de concienciación de seguridad física.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida

Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (*token*) de seguridad.

Iniciativas y/o Documentos E/S

Entrada	Salida
- Modelo de arquitectura de la información	- Inventario de documentos y dispositivos sensibles - Privilegios de acceso

Actividades

1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.
4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.
5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

Iniciativas y/o Documentos E/S

Entrada	Salida
-	- Registros de incidentes de seguridad - Características de incidentes de seguridad - Tickets de incidentes de seguridad

Actividades

1. Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.

4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

Etapa III: Caracterización formal del modelo de Evaluación de la Capacidad de Procesos de la universidad

Actividad 3.1. Identificación de los elementos del modelo de Evaluación de Procesos – PAM de COBIT 5

El desarrollo del modelo de Evaluación de la Capacidad de Procesos (ECP) para la universidad en estudio, se basa en los elementos del Modelo de Evaluación de Procesos – PAM de COBIT 5. La Figura 27 muestra una visión general de los elementos principales de este modelo.

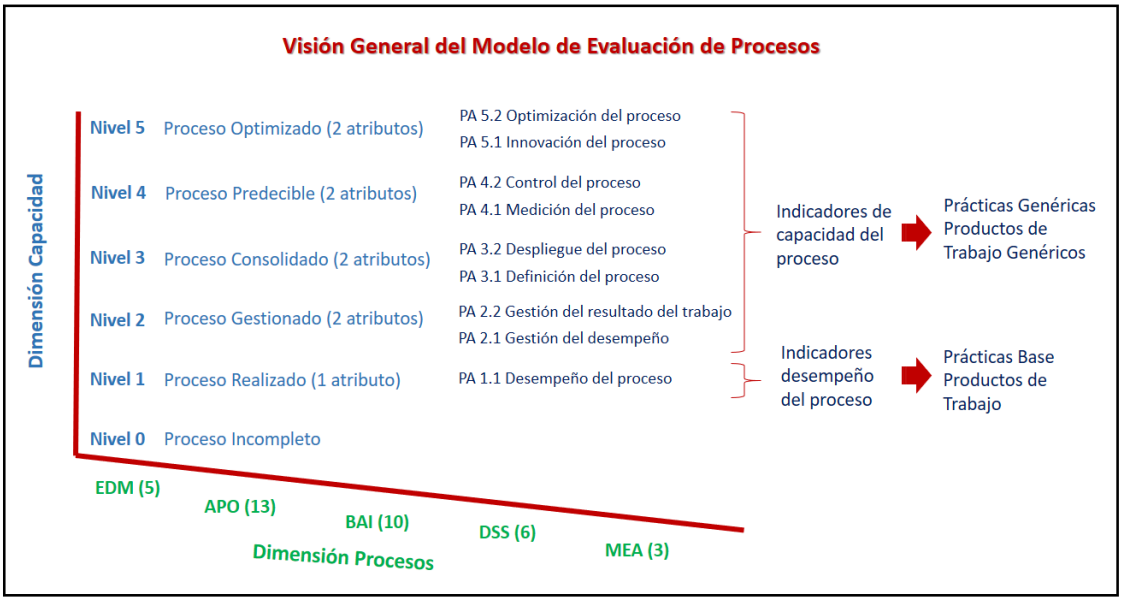


Figura 27 - Visión general de los elementos del PAM

Cómo ya se explicó en el Capítulo II, el PAM tiene dos dimensiones: la Dimensión Capacidad (DC) y la Dimensión Procesos (DP). En la DP se encuentran los 37 procesos del Modelo de Referencia de Procesos de COBIT 5, agrupados en los 5 dominios del modelo: Evaluar, Dirigir y Supervisar (EDM) con 5 procesos de gobierno; Alinear, Planificar y Organizar (APO) con 13 procesos; Construir, Adquirir e Implementar (BAI) con 10 procesos; Entregar, dar Servicio y Soporte (DSS) con 6 procesos y Supervisar, Evaluar y Valorar (MEA) con 3 procesos.

La DC contiene 6 niveles que cada proceso evaluado puede alcanzar o lograr. El Nivel 0, indica que el proceso está incompleto, es decir, que no se ejecuta o no logra su propósito. El Nivel 1, indica que el proceso está realizado, es decir logra su propósito. En el Nivel 2, el proceso está gestionado, es decir, el proceso se planifica y supervisa. El Nivel 3, indica que el proceso está consolidado, esto significa que la implementación del proceso se hace siguiendo un proceso definido. En el Nivel 4 el proceso es predecible, esto quiere decir que el proceso opera dentro de límites y logra los resultados esperados. Y finalmente, en el Nivel 5 el proceso es optimizado, es decir, el proceso se mejora continuamente para satisfacer los objetivos presentes y futuros de la organización. [11].

Cada nivel del 1 al 5 tiene atributos definidos, los cuales son evaluados para identificar si el proceso alcanzó el nivel analizado. Esto quiere decir, que el nivel de capacidad de los procesos se evalúa por medio de los atributos que tiene cada nivel.

La evaluación del Nivel 1 es diferente a los demás niveles. Para este nivel se evalúa un solo atributo, el Desempeño del proceso, y para esta evaluación se utilizan los Indicadores de desempeño que vienen a ser las Prácticas Base (BP) y los Productos de Trabajo (PWP, estos elementos son las actividades, las entradas y salidas de los procesos. Para la evaluación de los niveles del 2 al 5, se utilizan 2 atributos y para esta evaluación se utilizan los Indicadores de capacidad que son las Prácticas Genéricas (GP) y los Productos de Trabajo Genéricos (GWP). Estos elementos están definidos en el PAM para cada nivel y atributo, y se aplican a todos los procesos de manera genérica.[11].

La Tabla 11 muestra la relación de todos los elementos del PAM que se tomarán como base para el Modelo de Evaluación de la Capacidad de Procesos de la universidad. Estos elementos son: Nivel de capacidad, Atributos, Indicadores de evaluación.

Tabla 11 - Relación entre Nivel de capacidad, atributos e indicador de evaluación del PAM

Nivel de capacidad	Atributos	Indicador de evaluación
Nivel 0 Proceso incompleto	Ningún atributo	
Nivel 1 Proceso realizado	PA1.1. Desempeño/rendimiento del proceso	Prácticas Base (BP) Productos de Trabajo (WP)
Nivel 2 Proceso gestionado	PA2.1. Gestión del desempeño/rendimiento PA2.2. Gestión de productos de trabajo	
Nivel 3 Proceso consolidado	PA3.1. Definición de proceso PA3.2. Despliegue del proceso	Prácticas genéricas (GP) Productos de trabajo genéricos (GWP)
Nivel 4 Proceso predecible	PA4.1. Medición del proceso PA4.2. Control del proceso	
Nivel 5 Proceso optimizado	PA5.1. Innovación del proceso PA5.2. Optimización del proceso	

Profundizando en el análisis del PAM, se identifica que para la evaluación de la capacidad de los procesos en el Nivel 1, se describe cada proceso del Modelo de Referencia de Procesos en términos de: nombre, propósito y Resultados (Os) del proceso. Además de las Prácticas Base (BP) y los Productos de Trabajo (WP) de entrada y salida que ya explicamos anteriormente. Cada BP se asocia explícitamente a un resultado del proceso, y los WP se pueden relacionar a uno o más resultados. [11]

La Tabla 12 detalla los Resultados (Os), Prácticas Base (BP) y Producto de Trabajo (WP) que se consideran para la evaluación de la capacidad del proceso DSS05 Gestionar los Servicios de Seguridad (proceso que se considera para la investigación) en el Nivel 1 del PAM. De igual manera, el PAM define estos elementos para cada uno de los 37 procesos de COBIT.

Tabla 12 - Elementos de evaluación del Nivel 1 del proceso DSS05 Gestionar los servicios de seguridad

Resultados (Os)	Prácticas Base (BP)	Productos de Trabajo (WP)	
		Entrada	Salida
DSS05-01 Satisfacer las necesidades del negocio respecto a la seguridad de redes y comunicaciones.	DSS05-BP1 Protección contra software malicioso DSS05-BP2 Administrar la seguridad de la red y la conectividad DSS05-BP7 Supervisar la infraestructura de eventos relacionados con la seguridad	APO01-WP10 Directrices de clasificación de datos APO09-WP4 Acuerdos de nivel de servicio SLA	DSS05-WP1 Política de prevención de software malicioso DSS05-WP2 Evaluaciones de potenciales amenazas DSS05-WP3 Política de seguridad para conectividad DSS05-WP4 Resultados de pruebas de penetración DSS05-WP12 Registro de eventos de seguridad DSS05-WP13 Características de incidentes de seguridad DSS05-WP14 Tickets de incidentes de seguridad
DSS05-02 La información procesada, almacenada y transmitida por medio de dispositivos de punto final está protegida.	DSS05-BP1 Protección contra software malicioso DSS05-BP3 Administrar la seguridad del punto final	APO03-WP6 Modelo de información de arquitectura APO09-WP4 Acuerdos de nivel de servicios SLA APO09-WP5 Acuerdos de nivel operativo OLA BAI09-WP2 Resultados de controles sobre el inventario físico	DSS05-WP1 Política de prevención de software malicioso DSS05-WP2 Evaluaciones potenciales de amenazas DSS05-WP5 Políticas de seguridad para dispositivos de punto final
DSS05-03 Todos los usuarios tienen un único identificador y los derechos de acceso	DSS05-BP4 Administrar la identidad de usuarios y accesos lógicos	APO01-WP4 Definición de roles y responsabilidades de TI APO03-WP6 Modelo de información de arquitectura	DSS05-WP6 Derechos de acceso de usuarios aprobados

acordes con su función en la empresa			DSS05-WP7 Resultados de revisiones de cuentas de usuario y privilegios
DSS05-04 Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias al ser procesada, almacenada o transmitida	DSS05-BP5Administrar el acceso físico a los activos de TI		DSS05-WP8 Peticiones de acceso aprobadas DSS05-WP9 Registros de acceso
DSS05-05 La información electrónica se ha asegurado correctamente cuando se almacena, transmite o destruye.	DSS05-BP6Administrar documentos sensibles y dispositivos de salida	APO03-WP6 Modelo de información de arquitectura	DSS05-WP10 Inventario de documentos y dispositivos sensibles DSS05-WP11 Privilegios de acceso

Para la evaluación de la capacidad de los procesos en los Niveles del 2 al 5, el PAM propone las Prácticas Genéricas (GP) y los Productos de Trabajo Genéricos (GWP) que se aplican a todos los procesos del Modelo de Referencia de Procesos. La Tabla 13 muestra las GP y GWP para cada atributo de los niveles 2 al 5 del PAM.

Tabla 13 - Elementos de evaluación del Nivel 2 al Nivel 5 del proceso DSS05 Gestionar los servicios de seguridad

Nivel	Atributo	Objetivo/Resultado	Práctica Genérica	Producto de trabajo genérico
2	PA2.1 Gestión del rendimiento	a. Los objetivos para el rendimiento del proceso están identificados.	GP2.1.1 Identificar los objetivos	GWP1.0 Documentación del proceso GWP2.0 Plan del proceso
		b. El rendimiento del proceso está planificado y monitorizado	GP2.1.2 Planificar y monitorizar el rendimiento	GWP2.0 Plan del proceso GWP9.0 Registros de desempeño del proceso
		c. El rendimiento del proceso está ajustado para satisfacer planes	GP2.1.3 Ajustar el rendimiento del proceso	GWP4.0 Registros de calidad
		d. Las responsabilidades y autoridades del proceso están definidas, asignadas y comunicadas.	GP2.1.4 Definir las responsabilidades y autoridades	GWP1.0 Documentación del proceso GWP2.0 Plan del proceso
		e. Los recursos y la información del proceso se han identificado, están disponibles, asignados y utilizados.	GP2.1.5 Identificar los recursos y la información y hacer que estén disponibles	GWP2.0 Plan del proceso
		f. Las interfaces entre las partes involucradas garantizan una comunicación eficaz y clara asignación de responsabilidades.	GP2.1.6 Gestionar las interfaces	GWP1.0 Documentación del proceso GWP2.0 Plan del proceso
	PA2.2 Gestión del	a. Los requisitos para los productos de trabajo del proceso están definidos.	GP2.2.1 Definir los requisitos para los resultados de trabajo	GWP3.0 Plan de calidad

	resultado de trabajo	b. Los requisitos para la documentación y el control de los productos de trabajo están definidos	GP2.2.2 Definir los requisitos de documentos y control	GWP1.0 Documentación del proceso GWP3.0 Plan de calidad
		c. Los resultados de trabajo están identificados, documentados y controlados.	GP2.2.3 Identificar, documentar y controlar	GWP3.0 Plan de calidad
		d. Los resultados de trabajo son revisados en función a las disposiciones planificadas y ajustados	GP2.2.4 Revisar y ajustar los resultados de trabajo	GWP4.0 Registros de calidad
3	PA3.1 Definición del proceso	a. Se ha definido un proceso estándar y describe los elementos que deben ser incorporados en un proceso definido.	GP3.1.1 Definir el proceso estándar	GWP5.0 Políticas y normas
		b. La secuencia y la interacción del proceso estándar con otros procesos está determinada	GP3.1.2 Determinar la secuencia e interacción entre los procesos	GWP5.0 Políticas y normas
		c. Las competencias y roles para llevar a cabo un proceso están identificados en el proceso estándar	GP3.1.3 Identificar los roles y competencias del proceso estándar	GWP5.0 Políticas y normas
		d. La infraestructura y el ambiente de trabajo para realizar un proceso están identificados como parte del proceso estándar	GP3.1.4 Identificar el entorno de infraestructura y trabajos para el proceso estándar	GWP5.0 Políticas y normas
		e. Los métodos para el seguimiento de la eficacia y adecuación del proceso están definidos	GP3.1.5 Determinar los métodos adecuados de monitoreo del proceso	GWP4.0 Registros de calidad GWP5.0 Políticas y normas
	PA3.2 Despliegue del proceso	a. El proceso definido está desplegado sobre la base de un proceso estándar seleccionado y a medida	GP3.2.1 Implementar el proceso definido que satisface el contexto	GWP5.0 Políticas y normas
		b. Los roles, responsabilidades y autoridades del proceso están asignados y comunicados	GP3.2.2 Asignar y comunicar los roles, responsabilidades y autoridades	GWP5.0 Políticas y normas
		c. El personal del proceso definido es competente en formación y experiencia	GP3.2.3 Garantizar las competencias del personal	GWP1.0 Documentación del proceso GWP2.0 Plan del proceso
		d. Los recursos y la información están disponibles, asignados y utilizados	GP3.2.4 Proporcionar recursos e información	GWP2.0 Plan del proceso
		e. La infraestructura y el ambiente de trabajo del proceso está disponible, gestionado y mantenido	GP3.2.5 Proporcionar infraestructura de proceso adecuada	GWP2.0 Plan del proceso
		f. Los datos se recogen y analizan para entender el comportamiento del proceso y sus posibles mejoras	GP3.2.6 Recoger y analizar datos del rendimiento del proceso	GWP4.0 Registros de calidad GWP9.0 Registros de desempeño del proceso
4	PA4.1 Medición del proceso	a. La información que soporta al proceso es definida según los objetivos del negocio	GP4.1.1 Identificar de la información para el proceso	GWP6.0Plan de mejora del desempeño

		b. Los objetivos de medida del proceso se derivan de la necesidad de información	GP4.1.2 Deducir objetivos de medición	GWP7.0 Plan de medida del proceso
		c. Se definen objetivos cuantitativos para el correcto funcionamiento del proceso	GP4.1.3 Establecer objetivos cuantitativos	GWP7.0 Plan de medida del proceso
		d. Se identifican y definen medidas y frecuencias alineados a los objetivos de medición para el correcto funcionamiento del proceso	GP4.1.4 Identificar productos y medidas de procesos	GWP7.0 Plan de medida del proceso
		e. El resultado de las medidas se recolectan, analizan y reportan para monitorear el funcionamiento del proceso	GP4.1.5 Recolectar los resultados del producto y medición del proceso	GWP7.0 Plan de medida del proceso GWP9.0 Registros de desempeño del proceso
		f. El resultado de las mediciones es usado para la mejora del proceso	GP4.1.6 Usar los resultados de las mediciones del proceso	GWP9.0 Registros de desempeño del proceso
	PA4.2 Control del proceso	a. Se ha determinado para el proceso técnicas de análisis y control	GP4.2.1 Determinar las técnicas de análisis y control del proceso	GWP1.0 Documentación del proceso GWP8.0 Plan de control del proceso
		b. Se ha definido los límites de control de variación del funcionamiento normal del proceso	GP4.2.2 Definir los parámetros para controlar el rendimiento del proceso	GWP8.0 Plan de control del proceso
		c. Las mediciones son analizadas para detectar variaciones producidas	GP4.2.3 Analizar los procesos y los resultados de medición de los productos	GWP9.0 Registros de desempeño del proceso
		d. Se toman acciones correctivas que evitan las variaciones producidas	GP4.2.4 Identificar e implementar acciones correctivas	GWP9.0 Registros de desempeño del proceso
		e. Se reestablecen límites de control de acuerdo a las acciones correctivas	GP4.2.5 Re-establecer los límites de control del proceso	GWP8.0 Plan de control del proceso
5	PA5.1 Innovación del proceso	a. Los objetivos de mejora del proceso están definidos	GP5.1.1 Definir los objetivos de mejora del proceso	GWP7.0 Plan de medida del proceso
		b. Se analiza la información para identificar las causas de las variaciones del proceso	GP5.1.2 Analizar los datos de medición del proceso	GWP9.0 Registros de desempeño del proceso
		c. Se analiza la información para identificar las oportunidades de buenas prácticas e innovación	GP5.1.3 Identificar oportunidades de mejora del proceso	GWP6.0Plan de mejora del desempeño
		d. Se identifican oportunidades de mejoras para el proceso	GP5.1.4 Derivar las oportunidades de mejora del proceso	GWP6.0Plan de mejora del desempeño
		e. Se establece una estrategia para alcanzar los objetivos de mejora del proceso	GP5.1.5 Definir una estrategia de implementación	GWP6.0Plan de mejora del desempeño
	PA5.2 Optimización del proceso	a. Se evalúa el impacto de los cambios de acuerdo a los objetivos de proceso	GP5.2.1 Evaluar el impacto de cada cambio propuesto	GWP6.0Plan de mejora del desempeño
		b. Se gestiona la implementación de los cambios para asegurar el rendimiento del proceso	GP5.2.2 Gestionar la implementación de los cambios	GWP6.0Plan de mejora del desempeño GWP1.0 Documentación del proceso

	c. Se evalúa la efectividad de los cambios en el proceso	GP5.2.3 Evaluar la efectividad del cambio	GWP5.0 Políticas y normas GWP6.0Plan de mejora del desempeño

Actividad 3.2. Caracterización de la Evaluación Nivel 1: Análisis de los Criterios o Resultados (Os), de las Prácticas Base (BP) y los Productos de Trabajo (WP)

De acuerdo a lo explicado en la actividad anterior para la Evaluación del Nivel 1 del PAM se hace uso de los Criterios/Resultados (Os), Prácticas Base (BP) y Productos de Trabajo (WP). La forma como se utilizan estos elementos es como sigue:

a) Para cada proceso el PAM ha definido una cantidad de Criterios/Resultados (Os). Se evalúa el nivel alcanzado de cada criterio con el cumplimiento de las Prácticas Base y los Productos de Trabajo. Además, el PAM define, para cada proceso, la relación entre los Criterios/Resultados y las Prácticas Base y los Productos de Trabajo. La Tabla 14 muestra un ejemplo de esta relación tomada del proceso DSS05 Gestionar los servicios de seguridad.

Tabla 14 - Relación entre los Criterios/Resultado y las Prácticas Base o Prácticas de Gestión del proceso DSS05 Gestionar los servicios de seguridad

Criterios / Resultados		Prácticas Base o Práctica de Gestión	
Código	**Descripción**	**Código**	**Descripción**
DSS05-01	Satisfacer las necesidades del negocio respecto a la seguridad de redes y comunicaciones.	DSS05.01	Protección contra software malicioso
		DSS05.02	Administrar la seguridad de la red y la conectividad
		DSS05.07	Supervisar la infraestructura de eventos relacionados con la seguridad
DSS05-02	La información procesada, almacenada y transmitida por medio de dispositivos de punto final está protegida.	DSS05.01	Protección contra software malicioso
		DSS05.03	Administrar la seguridad del punto final
DSS05-03	Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa	DSS05.04	Administrar la identidad de usuarios y accesos lógicos
DSS05-04	Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias al ser procesada, almacenada o transmitida	DSS05.05	Administrar el acceso físico a los activos de TI
DSS05-05	La información electrónica se ha asegurado correctamente cuando se almacena, transmite o destruye.	DSS05.06	Administrar documentos sensibles y dispositivos de salida

De la Tabla 14 se puede concluir que, para identificar el nivel alcanzado por el Criterio o Resultado DSS05-01 se evalúa el cumplimiento de las actividades de las Prácticas de Gestión 01, 02 y 07. De la misma manera para los otros 4 Criterios.

b) Las Prácticas Base son las actividades que cada proceso tiene definidos como parte de las Prácticas de Gobierno o Gestión según el dominio al cuál pertenezca el proceso.

c) Los Productos de Trabajo son las entradas y salidas que están definidas para cada Práctica de Gobierno o Gestión de los procesos. Estos pueden ser: documentos, reportes, informes, o cualquier otro tipo de entregable.

El PAM especifica qué elementos se deben utilizar para hacer la evaluación del Nivel 1, más no especifica el cómo. Al revisar las actividades de cada práctica de gestión, en su mayoría contienen más de un requisito y condiciones sobre las que se debe evaluar el cumplimiento de la misma. Entonces, para medir el cumplimiento de una u otra actividad es necesario desmenuzar cada actividad en la cantidad de requisitos y condiciones que tiene para analizar si cumple o no el requisito.

Para hacer este análisis se propuso un Indicador de evaluación que consistía en identificar el o los verbos que contenía la actividad, el objeto de evaluación asociado al verbo y la o las condiciones (si es que hubieran). La Tabla 15 muestra estos elementos y un ejemplo con dos actividades extraídas de la Práctica de Gestión DSS05.01 Proteger contra software malicioso

Tabla 15 - Ejemplo de elaboración de Indicador de Evaluación para el Nivel 1

Proceso: DSS05 Gestionar los servicios de seguridad				
Práctica de gestión: DSS05.01 Proteger contra software malicioso				
N°	**Actividad**	**Indicador de evaluación**		
		Verbo	**Objeto de evaluación**	**Condición**
1	**Divulgar concienciación sobre el software malicioso** y **forzar procedimientos** y **responsabilidades** de prevención	**Divulgar**	**Concienciación sobre software malicioso**	
		Forzar / Establecer	**Procedimientos** de prevención sobre software malicioso	
			Responsabilidades de prevención sobre software malicioso	
2	**Instalar** y **activar herramientas de protección** frente a software malicioso en todas las instalaciones de proceso, con **ficheros de definición** de software malicioso que se **actualicen según se requiera** (automática o semi-automáticamente).	**Instalar**	**herramientas de protección** frente a software malicioso	**Ficheros de definición de software malicioso** **Actualizan de forma automática o semiautomática**
		Activar	**herramientas de protección** frente a software malicioso	**Ficheros de definición de software malicioso** **Actualizan de forma automática o semiautomática**

De esta manera, para cada actividad se identifican 2 a más sub actividades a las que se denominaron Indicadores de Evaluación, cada una de estas sub actividades hacen referencia a

una sola acción, lo que permite un mejor análisis sobre el cumplimiento de la actividad de la Práctica de Gestión. Este mismo procedimiento se aplica a todas las actividades de cada una de las prácticas de gestión que tienen los procesos de COBIT que se desee evaluar.

Respecto a los Productos de Trabajo, al ser documentos, reportes o cualquier otro tipo de entregable, solo se los incluye en el modelo para evaluar si el proceso cumple o no con el producto especificado.

Para medir el nivel de capacidad del proceso en el Nivel 1, cada Criterio/Resultado debe alcanzar uno de los 4 Niveles de Clasificación que el PAM ha definido. Los niveles de clasificación se explicaron en el Capítulo II, apartado 2.2.7.4. El valor porcentual que cada Criterio/Resultado alcanza, se obtiene evaluando el nivel de cumplimiento de las prácticas base del proceso.

Para obtener el nivel de calificación de la capacidad del proceso en el Nivel 1 del PAM, se promedian los valores porcentuales alcanzados por cada Criterio/Resultado. El valor que se obtiene se lo ubica en el Nivel de Calificación que corresponde y se interpreta. La capacidad del proceso en el Nivel 1 puede ser: No alcanzado, Parcialmente alcanzado, Ampliamente alcanzado o Completamente alcanzado.

Ahora bien, para obtener el valor porcentual de cada Criterio/Resultado se debe evaluar el nivel de cumplimiento de las actividades de las prácticas de gobierno o de gestión. Para iniciar con esta evaluación, se asigna un peso o valor porcentual a cada actividad, de tal manera que sumados todos los valores el resultado sea 100%. El valor asignado se realiza de acuerdo a la importancia que tenga la actividad para la Práctica de Gestión. La Tabla 16 muestra los valores asignados a las actividades de la Práctica de Gestión DSS05.01 Proteger contra software malicioso.

Tabla 16 - Asignación de peso o valor porcentual a las actividades de la Práctica de Gestión DSS05.01 Proteger contra software malicioso

Proceso: DSS05 Gestionar los servicios de seguridad		
Práctica de Gestión DSS05.01 Proteger contra software malicioso		
N°	**Actividad**	**Peso**
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	15%
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	25%
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	15%

4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	10%
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	20%
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	15%
		100%

De acuerdo a lo explicado anteriormente, cada actividad es analizada para identificar los Indicadores de Evaluación a considerar. Una vez identificados estos indicadores, se les asigna un valor porcentual que sumados debe resultar en 100%. Sobre la base de este valor se realiza la evaluación para identificar el nivel de cumplimiento de las actividades de las Prácticas de Gestión del proceso.

La Tabla 17 muestra los valores asignados a los Indicadores de Evaluación identificados para las actividades de la Práctica de Gestión DSS05.01 Proteger contra software malicioso.

Tabla 17 - Asignación de peso o valor porcentual a los Indicadores de Evaluación de cada actividad analizada de la Práctica de Gestión DSS05.01 Proteger contra software malicioso

Proceso: DSS05 Gestionar los servicios de seguridad						
Práctica de gestión: DSS05.01 Proteger contra software malicioso						
N°	**Actividad**	**Peso**	**Indicador de evaluación**			
			Verbo	**Objeto de evaluación**	**Condición**	**Peso**
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	15%	Divulgar	Concienciación sobre software malicioso		30%
			Forzar / Establecer	Procedimientos de prevención sobre software malicioso		40%
				Responsabilidades de prevención sobre software malicioso		30%
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	25%	Instalar	herramientas de protección frente a software malicioso	Ficheros de definición de software malicioso	30%
					Actualizan de forma automática o semiautomática	30%
			Activar	herramientas de protección frente a software malicioso	Ficheros de definición de software malicioso	20%
					Actualizan de forma automática o semiautomática	20%
3	Distribuir todo el software de protección de forma centralizada (versión y nivel	15%	Distribuir	software de protección frente a software malicioso	forma centralizada (versión y nivel de parchado)	50%

	de parcheado) usando una configuración centralizada y la gestión de cambios.				usando configuración	50%
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	10%	Revisar	información sobre nuevas amenazas		50%
			Evaluar	información sobre nuevas amenazas		50%
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	20%	Filtrar	tráfico entrante (correo electrónicos, descargas)		100%
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	15%	Realizar	formación periódica sobre software malicioso	uso de correo electrónico e internet	50%
			Orientar	usuarios	no instalar software compartido o no autorizado	50%

Finalmente, para consolidar todo lo expuesto respecto a la Fase 3 del Modelo de Evaluación de Capacidad de Procesos (ECP) para la universidad objeto de estudio, se propone el diagrama de la Figura 28 que muestra la caracterización formal de los elementos que forman parte del modelo para evaluar la capacidad de los procesos en el Nivel 1. Debemos recordar que el atributo evaluado en este nivel es Rendimiento del proceso.

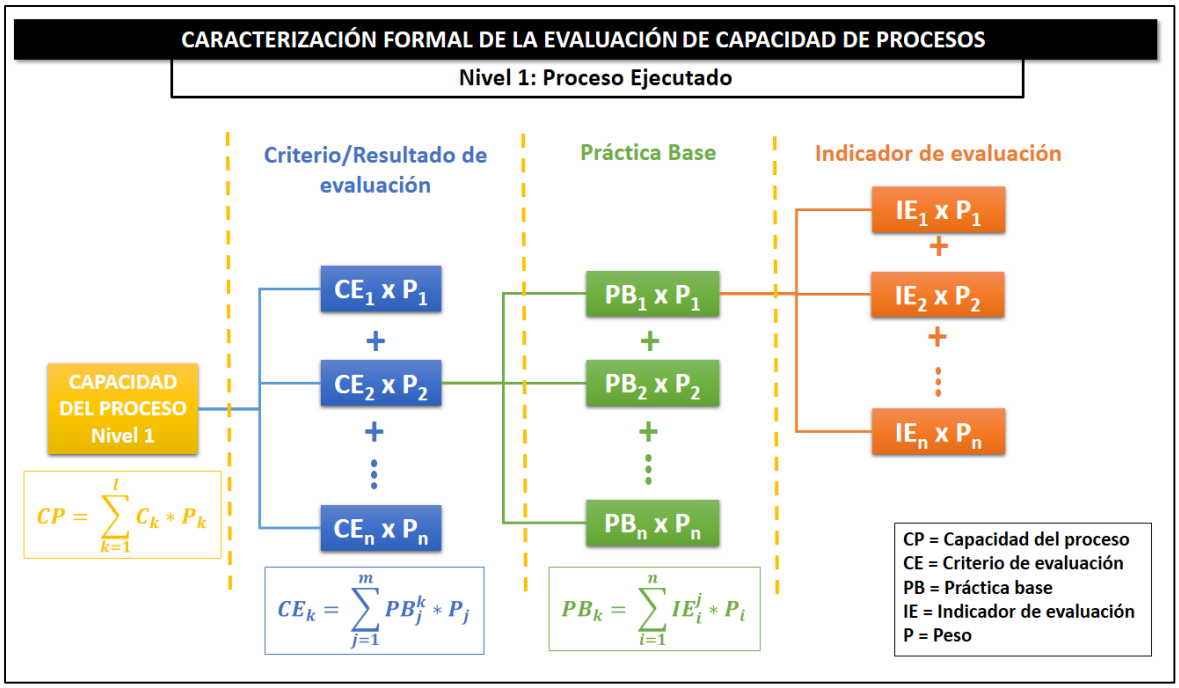


Figura 28 - Modelo de Evaluación de la Capacidad de Procesos - Nivel 1: Proceso Ejecutado

Actividad 3.3. Evaluación Nivel 2 – 5: Análisis de las Prácticas Genéricas (GP) y los Productos de Trabajo Genéricos (GWP)

La evaluación de los Niveles 2 al 5 se realiza solo si el nivel anterior fue alcanzado completamente, es decir, si la capacidad del proceso evaluado en el nivel anterior alcanzó un Nivel de Calificación entre >85% y 100%. [11]

Con lo explicado en la Actividad 3.1., para evaluar los Niveles 2 al 5 se utilizan las Prácticas Genéricas (GP) y los Productos de Trabajo Genéricos (GWP) que permiten evaluar los atributos que cada nivel tiene definidos. Recordemos que, para los niveles del 2 al 5 el PAM ha definido 2 atributos por cada nivel. La Tabla 18 muestra los atributos que cada nivel tiene y que se evalúan con las GP y GWP.

Tabla 18 - Niveles de Capacidad y atributos del proceso

Nivel de Capacidad	ID Atributo	Atributo
Nivel 2: Proceso gestionado	PA 2.1	Gestión del rendimiento
	PA 2.2	Gestión de productos de trabajo
Nivel 3: Proceso consolidado	PA 3.1	Definición del proceso
	PA 3.2	Despliegue del proceso
Nivel 4: Proceso predecible	PA 4.1	Medición del proceso
	PA 4.2	Control del proceso
Nivel 5: Proceso optimizado	PA 5.1	Innovación del proceso
	PA 5.2	Optimización del proceso

Para cada atributo el PAM ha definido un número de resultados/objetivos que se deben alcanzar para el logro del atributo. Estos resultados son evaluados por las Prácticas Genéricas y los Productos de Trabajo Genéricos. La Tabla 13 (ubicada en la Actividad 3.1.) describe los Resultados, las Prácticas Genéricas y los Productos de Trabajo Genéricos para los 2 atributos de cada nivel.

Para la evaluación de los niveles 2 al 5, el modelo ECP propone realizar las siguientes acciones:

a) Asignar un peso o valor porcentual a cada resultado/objetivo de cada atributo. La suma de estos valores debe ser 100%.
b) Identificar las prácticas genéricas y los productos de trabajos genéricos de cada atributo. Asignar un peso o valor porcentual a cada uno que sumado de 100%.
c) Analizar cada práctica genérica para identificar el o los Indicadores de Evaluación, de la misma manera como se analizaron las actividades de las prácticas de gestión en el Nivel 1. Recordar, que el Indicador de Evaluación se compone por un verbo, un objeto de evaluación y una condición (en caso de que existiera).

d) Finalmente, a cada Indicador de Evaluación identificado, asignar un peso o valor porcentual que sumado de 100%.

La Tabla 19 muestra un ejemplo del análisis de los Resultados/Objetivos del Atributo PA2.1 Gestión del rendimiento del Nivel 2: Proceso gestionado y su relación con las Prácticas genéricas y los productos de trabajo genéricos y la identificación de los Indicadores de Evaluación.

Tabla 19 - Ejemplo del Análisis de Resultados, Prácticas Genéricas y Productos de Trabajo Genéricos para la evaluación de los procesos en los niveles 2 al 5

Nivel 2: Proceso Gestionado								
Atributo PA2.1 Gestión del rendimiento								
Resultado/Objetivo			**Práctica Genérica (GP) / Producto de Trabajo Genérico (GWP)**				**Indicador de evaluación**	
N°	**Descripción**	**Peso**	**N°**	**Tipo**	**Descripción**	**Peso**	**Verbo**	**Objeto de evaluación**
1	Los objetivos para el rendimiento del proceso están identificados.	20%	2.1.1.	GP	Identificar los objetivos para el rendimiento del proceso. Los objetivos de rendimiento, junto con los supuestos y limitaciones, están definidos y comunicados.	60%	Definir	Objetivos para el rendimiento del proceso Supuestos para el rendimiento del proceso Limitaciones para el rendimiento del proceso
							Comunicar	Objetivos, supuestos y limitaciones para el rendimiento del proceso
			1.0	GWP	**Documentación del proceso**: debe describir el alcance del proceso.	20%	Proporcionar	Alcance en la documentación del proceso
			2.0	GWP	**Plan del proceso:** debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	Proporcionar	Objetivos de rendimiento en el plan del proceso
2	El rendimiento del proceso está planificado y monitorizado.	20%	2.1.2.	GP	Planificar y monitorizar el rendimiento del proceso para cumplir con los objetivos identificados. Medidas básicas de rendimiento de procesos vinculados a los objetivos de negocio están establecidas y monitorizadas. Incluyen hitos clave, actividades requeridas, estimaciones y planificaciones.	60%	Planificar	Rendimiento del proceso para cumplir con los objetivos definidos
							Establecer	Medidas básicas de rendimiento (hitos, actividades, estimaciones)
							Monitorear	Rendimiento del proceso para cumplir con los objetivos definidos

2.0	GWP	**Plan del proceso:** debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	Proporcionar	Objetivos de rendimiento en el plan del proceso
9.0	GWP	**Registros del desempeño del proceso:** deben proporcionar detalles de los resultados.	20%	Proporcionar	Resultados del rendimiento en los registros de desempeño del proceso

Para consolidar las acciones expuestas de la Fase 3 se presenta el diagrama de la Figura 29 que muestra la caracterización formal de los elementos del Modelo de Evaluación de Capacidad de Procesos (ECP) de la universidad objeto de estudio, para la evaluación de los niveles 2 al 5.

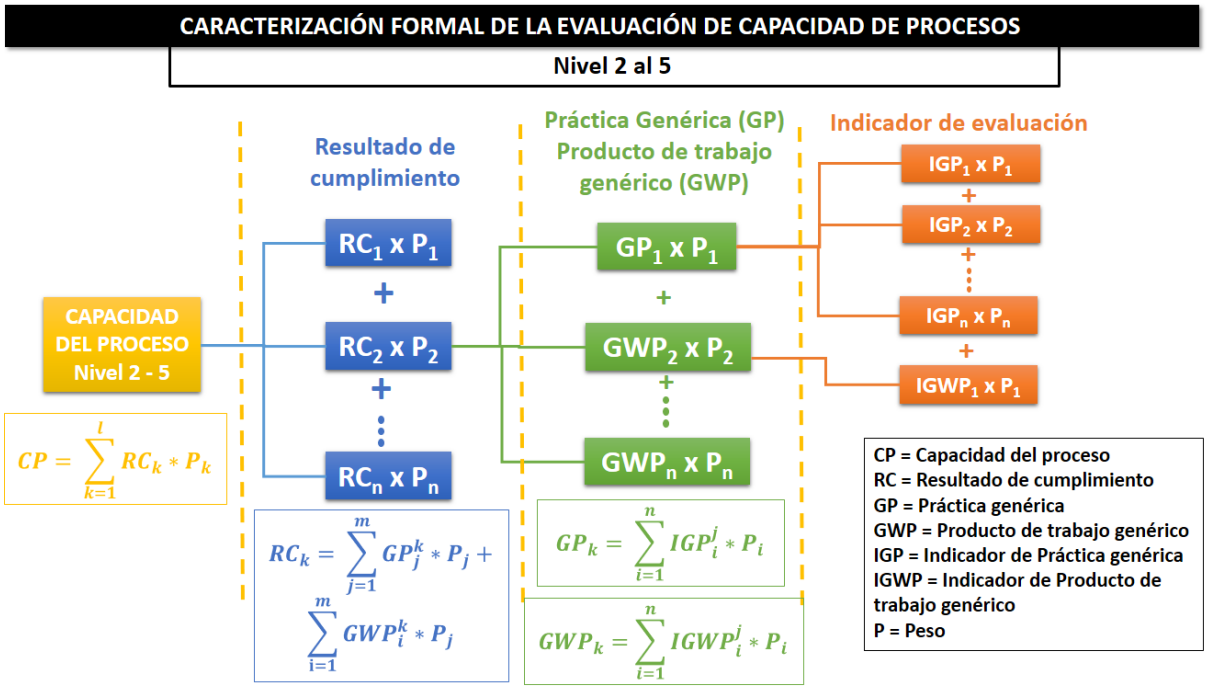


Figura 29 - Modelo de Evaluación de la Capacidad de Procesos - Nivel 2 al Nivel 5

Actividad 3.4. Diseño del modelo ECP (Evaluación de la Capacidad de Procesos) de la universidad

De acuerdo a lo descrito y explicado en las Actividades anteriores, el Modelo de Evaluación de la Capacidad de Procesos (ECP) se agrupa en 3 Fases, estas son:

a) Fase 1: Alineamiento de TI con la universidad

El objetivo de esta fase es alinear las tecnologías de información (TI) de la universidad con los objetivos estratégicos, de esta manera se prevé que el uso que se da a las TI permitan el

logro de los objetivos estratégicos de la universidad. Esta fase está basada en el mecanismo de la cascada de metas del COBIT 5, la que se adaptó al contexto de la universidad objeto de estudio. El desarrollo explicado de esta fase se encuentra en las Actividades 1.1. al 1.5.

b) Fase 2: Referencia de procesos

Esta fase se orienta a analizar los procesos resultantes de la Fase 1 para organizarlos en un modelo de referencia de procesos y adaptarlos al contexto de la universidad. La organización de los procesos está basada en el Modelo de Referencia de Procesos de COBIT 5. El desarrollo explicado de esta fase se encuentra en las Actividades 2.1. y 2.2.

c) Fase 3: Evaluación de capacidad de procesos

En esta fase lo que se pretende es evaluar la capacidad de los procesos que conforman el modelo de referencia de los procesos de la universidad con el propósito de conocer en qué nivel se encuentran y las mejoras que se deben aplicar para que permitan alcanzar los objetivos estratégicos de la universidad. Recordemos que los procesos identificados son los que están alineados a los objetivos estratégicos de la universidad. Existen dos tipos de evaluación: la evaluación del Nivel 1 y la evaluación de los Niveles 2 al 5. El desarrollo explicado de esta fase se encuentra en las Actividades 3.1., 3.2., y 3.3.

La Figura 30 muestra el Modelo de Evaluación de la Capacidad de Procesos, las tres fases que la conforman y la forma como estas se relacionan.

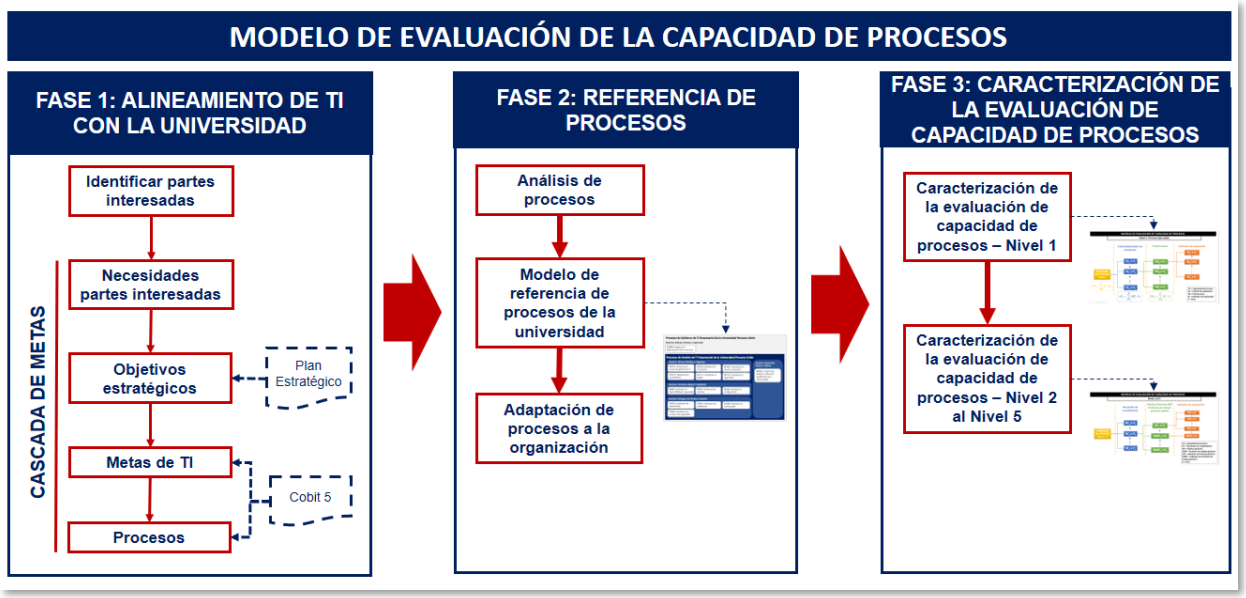


Figura 30 - Modelo de Evaluación de la Capacidad de Procesos de la Universidad

Etapa IV: Aplicación de la caracterización formal para la evaluación de la capacidad del proceso DSS05 Gestionar los servicios de seguridad

Actividad 4.1. Evaluación del Nivel 1 del proceso DSS05 Gestionar los servicios de seguridad

La evaluación del Nivel 1 del proceso DSS05 Gestionar los servicios de seguridad se basó en el modelo ECP y se desarrolló de la siguiente manera:

a) Elaboración y validación del instrumento de evaluación:

En primer lugar, se elaboró un instrumento de evaluación aplicando lo expuesto en el modelo ECP para la evaluación del Nivel 1. El instrumento de evaluación contempla las siete Prácticas de Gestión que tiene este proceso. Parte del instrumento se muestra en la Figura 31, para ver el instrumento completo acceder en el apartado Anexos.

INSTRUMENTO DE EVALUACION DE CAPACIDAD DE PROCESOS
NIVEL 1: PROCESO EJECUTADO
ATRIBUTO: 1.1. RENDIMIENTO DEL PROCESO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

PRÁCTICA DE GESTIÓN: DSS05.01 - PROTEGER CONTRA SOFTWARE MALICIOSO

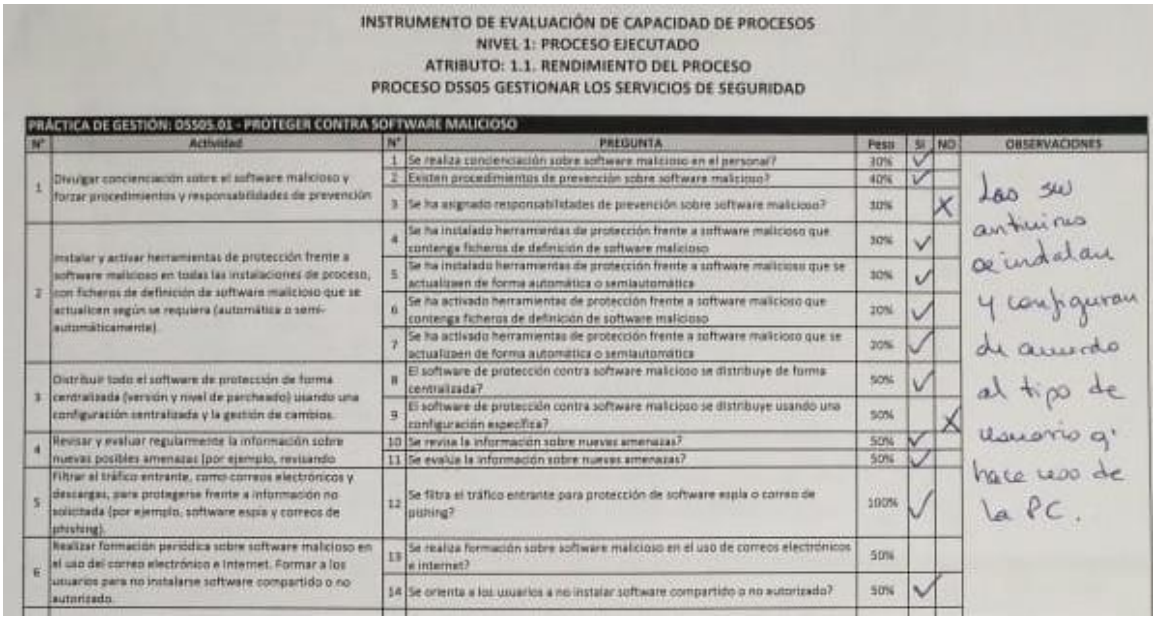
N°	Actividad	N°	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	1	Se realiza concienciación sobre software malicioso en el personal?	30%			
		2	Existen procedimientos de prevención sobre software malicioso?	40%			
		3	Se ha asignado responsabilidades de prevención sobre software malicioso?	30%			
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	4	Se ha instalado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	30%			
		5	Se ha instalado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	30%			
		6	Se ha activado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	20%			
		7	Se ha activado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	20%			
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	8	El software de protección contra software malicioso se distribuye de forma centralizada?	50%			
		9	El software de protección contra software malicioso se distribuye usando una configuración especifica?	50%			
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando	10	Se revisa la información sobre nuevas amenazas?	50%			
		11	Se evalúa la información sobre nuevas amenazas?	50%			
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	12	Se filtra el tráfico entrante para protección de software espía o correo de pishing?	100%			
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	13	Se realiza formación sobre software malicioso en el uso de correos electrónicos e internet?	50%			
		14	Se orienta a los usuarios a no instalar software compartido o no autorizado?	50%			

Figura 31 - Instrumento de evaluación para el Nivel 1

El instrumento de evaluación fue validado por revisión de contenidos y por juicio de expertos. Los expertos que participaron en la validación fueron el Director del Área de TI de la universidad en estudio y de un docente de la EP de Ingeniería de Sistemas de la misma universidad. La validación de contenidos significa que el instrumento está basado en las buenas prácticas de COBIT 5, de acuerdo a todo el análisis que se hizo en el desarrollo de la Fase 3 del Modelo ECP.

b) Aplicación del instrumento de evaluación a la Dirección General de Tecnologías de Información (DIGETI) de la universidad:

Solicitados los permisos correspondientes, se procedió a evaluar el nivel de capacidad del proceso DSS05 Gestionar los servicios de seguridad en la DIGETI. El instrumento se aplicó en el mes de octubre del año 2017 con la participación de dos trabajadores responsables de la seguridad en la universidad. La Figura 32 muestra el instrumento con las marcas y observaciones que se recogieron al momento de la aplicación. El instrumento de evaluación completo se encuentra en el apartado Anexos.



INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 1: PROCESO EJECUTADO
ATRIBUTO: 1.1. RENDIMIENTO DEL PROCESO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

PRÁCTICA DE GESTIÓN: DSS05.01 - PROTEGER CONTRA SOFTWARE MALICIOSO

N°	Actividad	N°	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	1	Se realiza concienciación sobre software malicioso en el personal?	10%	✓		Los SW antivirus se instalan y configuran de acuerdo al tipo de usuario q' hace uso de la PC.
		2	Existen procedimientos de prevención sobre software malicioso?	40%	✓		
		3	Se ha asignado responsabilidades de prevención sobre software malicioso?	30%		X	
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	4	Se ha instalado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	30%	✓		
		5	Se ha instalado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	30%	✓		
		6	Se ha activado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	20%	✓		
		7	Se ha activado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	20%	✓		
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	8	El software de protección contra software malicioso se distribuye de forma centralizada?	50%	✓		
		9	El software de protección contra software malicioso se distribuye usando una configuración específica?	50%		X	
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando	10	Se revisa la información sobre nuevas amenazas?	50%	✓		
		11	Se evalúa la información sobre nuevas amenazas?	50%	✓		
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	12	Se filtra el tráfico entrante para protección de software espía o correo de pishing?	100%	✓		
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	13	Se realiza formación sobre software malicioso en el uso de correos electrónicos e internet?	50%			
		14	Se orienta a los usuarios a no instalar software compartido o no autorizado?	50%	✓		

Figura 32 – Instrumento de evaluación aplicado para la evaluación de la capacidad del proceso DSS05 Gestionar servicios de seguridad de la universidad

c) Procesamiento de la información obtenida

Luego de aplicado el instrumento de evaluación, se realizó el procesamiento de la información obtenida para determinar el nivel de capacidad que lograba el proceso. De acuerdo al modelo ECP para el Nivel 1, a cada actividad se asignó un peso o valor porcentual, de igual manera a los Indicadores de Evaluación. Este peso o valor porcentual se utilizó para el procesamiento de la información obtenida.

Cada respuesta afirmativa se identificaba con el número 1. Luego, se aplicaba una fórmula que sumaba los pesos o valores porcentuales de todas las respuestas afirmativas. Si todas las respuestas eran afirmativas, entonces se alcanzaba el valor esperado de cumplimiento de la actividad evaluada. Sin embargo, no todas las respuestas eran afirmativas, por lo que se calculó el nivel de cumplimiento respecto al peso asignado a la actividad.

El mismo procesamiento se aplicó para evaluar el nivel de cumplimiento de todas las actividades del proceso. La Figura 34 muestra parte de este procesamiento, el documento completo se encuentra en el apartado Anexos. La columna de color celeste es la sumatoria de los pesos asignados a las preguntas del instrumento cuya respuesta era un SI (1). La columna de color crema es el logro alcanzado respecto al peso asignado a la actividad. La columna de color verde es el peso asignado a cada actividad.

Finalmente, se procesó la información para determinar el nivel de cumplimiento por cada Práctica de Gestión del proceso evaluado. Esto se hizo sumando los valores logrados por cada actividad (la columna de color crema). En la Figura 33 se puede observar que la Práctica de Gestión DSS05.01 Proteger contra software malicioso alcanzó un 81% de cumplimiento de las actividades. Para determinar el valor alcanzado por el proceso se utilizó la plantilla propuesta por COBIT.

INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 1: PROCESO EJECUTADO
ATRIBUTO: 1.1. RENDIMIENTO DEL PROCESO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

PRÁCTICA DE GESTIÓN: DSS05.01 - PROTEGER CONTRA SOFTWARE MALICIOSO

N°	Actividad	Peso	Logrado		N°	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	15%	11%	70%	1	Se realiza concienciación sobre software malicioso en el personal?	30%	1		
					2	Existen procedimientos de prevención sobre software malicioso?	40%	1		
					3	Se ha asignado responsabilidades de prevención sobre software malicioso?	30%			
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	25%	25%	100%	4	Se ha instalado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	30%	1		
					5	Se ha instalado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	30%	1		
					6	Se ha activado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	20%	1		
					7	Se ha activado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	20%	1		
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	15%	8%	50%	8	El software de protección contra software malicioso se distribuye de forma centralizada?	50%	1		
					9	El software de protección contra software malicioso se distribuye usando una configuración específica?	50%			
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando	10%	10%	100%	10	Se revisa la información sobre nuevas amenazas?	50%	1		
					11	Se evalúa la información sobre nuevas amenazas?	50%	1		
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	20%	20%	100%	12	Se filtra el tráfico entrante para protección de software espía o correo de pishing?	100%	1		
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	15%	8%	50%	13	Se realiza formación sobre software malicioso en el uso de correos electrónicos e internet?	50%			
					14	Se orienta a los usuarios a no instalar software compartido o no autorizado?	50%	1		
		100%	81%							

Figura 33 - Procesamiento de la información para la evaluación del Nivel 1

d) Resultado: logro alcanzado por el proceso DSS05 Gestionar los servicios de seguridad en el Nivel 1.

Luego de procesada la información, se determinó el nivel de logro alcanzado por el proceso DSS05 Gestionar los servicios de seguridad en la Universidad en estudio. La presentación de este resultado se hizo utilizando la plantilla propuesta por COBIT 5, la que se muestra en la Figura 34. Los datos de color rojo son los valores porcentuales alcanzados por cada

Criterio/Resultado. El resultado final de la capacidad del proceso en el Nivel 1 es de 69.6% esto significa que el proceso está ampliamente alcanzado. También es posible concluir que el rendimiento del proceso es de 69.6%.

DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD							
PROPÓSITO	Minimizar el impacto en el negocio de las vulnerabilidades operacionales de seguridad de la información y de incidentes						
Calificación por criterios / resultados	69.6%						
Nivel de capacidad alcanzado	Ampliamente alcanzado						
Evaluar si los siguientes resultados son alcanzados		Criterios / Resultados	¿Criterios alcanzados? S/N	Comentario	No alcanzado (0-15%)	Parcialmente Alcanzado (>15% -50%)	Ampliamente Alcanzado (>50% - 85%)	Completamente Alcanzado (>85-100%)
Nivel 1 Proceso Ejecutado	PA 1.1 Desempeño del proceso. El proceso implementado consigue su propósito	DSS05-O1 Satisfacer las necesidades del negocio respecto a la seguridad de redes y comunicaciones.	S				75%	
		DSS05-O2 La información procesada, almacenada y transmitida por medio de dispositivos de punto final está protegida.	S				71%	
		DSS05-O3 Todos los usuarios tienen un púnico identificador y los derechos de acceso acordes con su función en la empresa.	S				72%	
		DSS05-O4 Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias al ser procesada, almacenada o transmitida	S			45%		
		DSS05-O5 La información electrónica se ha asegurado correctamente cuando se almacena, transmite o destruye.	S				85%	

Figura 34 - Resultados de la evaluación de la capacidad del proceso DSS05 Gestionar los servicios de seguridad

Actividad 4.2. Evaluación del Nivel 2 al 5 del proceso DSS05 Gestionar los servicios de seguridad

Para evaluar la capacidad del proceso en el Nivel 2, el resultado de la evaluación en el Nivel 1 debió alcanzar un valor entre >85% a 100%, es decir, que el proceso está Completamente logrado. De acuerdo a lo expuesto sobre el resultado alcanzado en la evaluación del proceso en el Nivel 1, no se ha alcanzado el resultado esperado, por lo tanto, no se podría evaluar al proceso en el Nivel 2 hasta que este alcance un valor entre el rango especificado.

Sin embargo, como parte de la investigación se elaboró el instrumento de evaluación que permite la evaluación del proceso en el Nivel 2. La Figura 35 contiene una parte de este instrumento. El instrumento completo está en el apartado Anexos.

INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 2: PROCESO GESTIONADO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

Atributo: 2.1. Gestión del rendimiento

RESULTADO DE CUMPLIMIENTO			PRÁCTICA GENÉRICA (GP) PRODUCTO DE TRABAJO GENÉRICO (GWP)				N°	PREGUNTA	PESO	SI	NO
N°	DESCRIPCIÓN	PESO	N°	TIPO	DESCRIPCIÓN	PESO					
1	Los objetivos para el rendimiento del proceso están identificados.	20%	2.1.1.	GP	Identificar los objetivos para el rendimiento del proceso. Los objetivos de rendimiento, junto con los supuestos y limitaciones, están definidos y comunicados.	60%	1	Se ha definido los objetivos para el rendimiento del proceso?	25%		
							2	Se ha definido los supuestos para el rendimiento del proceso?	25%		
							3	Se ha definido las limitaciones para el rendimiento del proceso?	25%		
							4	Los objetivos, supuestos y limitaciones para el rendimiento del proceso fueron comunicados a los interesados?	25%		
			1.0	GWP	**Documentación del proceso**: debe describir el alcance del proceso.	20%	5	La documentación del proceso proporciona el alcance del proceso?	100%		
			2.0	GWP	**Plan del proceso**: debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	6	El plan del proceso proporciona los objetivos de rendimiento del proceso?	100%		
2	El rendimiento del proceso está planificado y monitorizado.	20%	2.1.2.	GP	Planificar y monitorizar el rendimiento del proceso para cumplir con los objetivos identificados. Medidas básicas de rendimiento de procesos vinculados a los objetivos de negocio están establecidas y monitorizadas. Incluyen hitos clave, actividades requeridas, estimaciones y planificaciones.	60%	7	Se ha planificado el rendimiento del proceso que permita cumplir con los objetivos?	35%		
							8	Se ha establecido medidas básicas de rendimiento (hitos, actividades, estimaciones)?	35%		
							9	Se monitorea el rendimiento del proceso para ver el cumplimiento de los objetivos?	30%		
			2.0	GWP	**Plan del proceso**: debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	10	El plan del proceso proporciona los objetivos de rendimiento del proceso?	100%		
			9.0	GWP	**Registros del desempeño del proceso**: deben proporcionar detalles de los resultados.	20%	11	Los registros de desempeño del proceso proporcionan los resultados del rendimiento del proceso?	100%		

Figura 35 - Instrumento de evaluación de la capacidad del procesos - Nivel 2

CAPÍTULO V: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

5.1. Resultados de la aplicación metodológica

La Metodología de la Investigación realizada está conformada por 4 etapas, en cada una se obtuvieron resultados que fueron formando el Modelo de Evaluación de la Capacidad de Procesos (ECP) de la universidad. A continuación, explicaremos los resultados de cada etapa.

5.1.1. Etapa I: Alineamiento de la TI con la estrategia de la Universidad

En esta etapa se desarrolló la Fase 1 – Alineamiento de TI con la estrategia de la universidad del Modelo de Evaluación de la Capacidad de Procesos. Esta fase consta de cinco actividades. La explicación de cómo se desarrolló cada actividad se encuentra en el Capítulo IV.

El resultado esperado de esta fase del modelo era la alineación de los procesos de gobierno y gestión de TI con los objetivos estratégicos de la universidad especificados en el Plan Estratégico v2 2014 – 2018. La Figura 36 muestra la alineación de los 15 procesos resultantes de la Cascada de Metas con los 22 objetivos estratégicos que satisfacían las necesidades de las partes interesadas de la universidad. Esta alineación se indica con una letra P en la intersección.

En la Tabla 20 se muestran los resultados de la alineación de procesos de TI a los objetivos estratégicos. De la información de la tabla, se concluye que 8 procesos de TI, que representan al 53.3% de los procesos alineados soportan al 100% de los objetivos estratégicos de la universidad (ver los procesos que suman 22). Esto significa que, para establecer el gobierno de TI en la universidad, se debe implementar y medir el rendimiento de estos procesos pues son el soporte tecnológico – estratégico para el logro de los objetivos organizacionales. Estos procesos son:

- APO01 Gestionar el marco de gestión de TI
- APO12 Gestionar el riesgo
- APO13 Gestionar la seguridad
- BAI06 Gestionar los cambios
- DSS01 Gestionar las operaciones
- DSS03 Gestionar los problemas
- DSS04 Gestionar la continuidad
- DSS05 Gestionar los servicios de seguridad

Por otro lado, se observa que, existen 6 objetivos estratégicos de los 22, que representan el 27.3%, que requieren de la implementación del 100% de los procesos de TI alineados (ver los

objetivos que suman 15). Esto porque, en todos los niveles de la estructura organizativa que se encarga del velar por el logro de esos objetivos estratégicos, se requieren de las TI, por lo tanto, se hace imperativo la implementación y medición del rendimiento de la totalidad de los procesos alineados. Los 6 objetivos estratégicos que se alinean a la totalidad de los procesos de TI son:

- OE05 Desarrollar capacidades en investigación
- OE06 Ampliar la disponibilidad y uso de biblioteca virtual
- OE08 Lograr una planificación de la Enseñanza – Aprendizaje acorde a los estándares
- OE09 Alcanzar la excelencia en el desarrollo de las sesiones de clase
- OE19 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad
- OE20 Fidelizar a la comunidad educativa

A manera de conclusión, diremos que el propósito de esta etapa del Modelo ECP es alinear los procesos de TI propuestos por Cobit 5 a los objetivos estratégicos de la organización. En el caso de la universidad, se identificaron 15 procesos de TI alineados, de los cuales el 53.3% se alinea con la totalidad de los objetivos estratégicos. Sin embargo, el 27.3% de los objetivos estratégicos, requiere de la implementación del 100% de los procesos de TI alineados.

Tabla 20 – Resultados de la alineación de los procesos de TI con los objetivos estratégicos de la universidad

N° de procesos de TI alineados	N° de objetivos estratégicos	Procesos alineados con el 100% de los objetivos estratégicos		Objetivos estratégicos alineados con el 100% de los procesos de TI	
		N°	%	N°	%
15	22	8	**53.3%**	6	**27.3%**

ALINEAMIENTO DE LOS PROCESOS DE GOBIERNO Y GESTIÓN DE TI CON LOS OBJETIVOS ESTRATÉGICOS DE LA UNIVERSIDAD

		OBJETIVOS ESTRATÉGICOS UNIVERSIDAD PERUANA UNIÓN	PROCESOS DE GOBIERNO Y GESTIÓN ALINEADOS A LOS OBJETIVOS ESTRATÉGICOS															
			EDM04 - Asegurar la optimización de recursos	APO01 - Gestionar el Marco de Gestión de TI	APO04 - Gestionar la innovación	APO07 - Gestionar los recursos humanos	APO10 - Gestionar los proveedores	APO12 - Gestionar el riesgo	APO13 - Gestionar la seguridad	BAI04 - Gestionar la disponibilidad y la capacidad	BAI06 - Gestionar los cambios	BAI10 - Gestionar la configuración	DSS01 - Gesstionar las operaciones	DSS03 - Gestionar los problemas	DSS04 - Gestionar la continuidad	DSS05 - Gestionar los servicios de seguridad	MEA01 - Supervisar, evaluar y valorar rendimiento y conformidad	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
FINANCIERO	1	Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes	P	P	P			P	P		P		P	P	P	P		10
APRENDIZAJE	2	Contar con docentes capacitados y especializados		P	P	P	P	P	P	P	P	P	P	P	P	P	P	14
	3	Fortalecer la participación de docentes y estudiantes en eventos de investigación científica	P	P		P	P	P	P	P	P	P	P	P	P	P	P	14
	4	Incrementar los investigadores activos en redes de investigación	P	P	P	P		P	P		P	P	P	P	P	P	P	13
	5	Desarrollar capacidades en investigación	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	15
	6	Ampliar la disponibilidad y uso de biblioteca virtual	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	15
	7	Desarrollar competencias para proyectos y programas		P	P	P		P	P		P		P	P	P	P	P	11
PROCESOS	8	Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	15
	9	Alcanzar la excelencia en el desarrollo de las sesiones de clase	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	15
	10	Consolidar la atención en tutorías	P	P	P		P	P	P	P	P	P	P	P	P	P	P	14
	11	Alcanzar la efectividad de la gestión de prácticas preprofesionales	P	P	P			P	P	P	P	P	P	P	P	P	P	13
	12	Lograr la efectividad en la evaluación de la Enseñanza - Aprendizaje	P	P	P		P	P	P	P	P	P	P	P	P	P	P	14
	13	Lograr la eficacia de los procesos de investigación científica	P	P	P		P	P	P	P	P	P	P	P	P	P	P	14
	14	Fortalecer la cultura de investigación en diferentes niveles de enseñanza	P	P				P	P	P	P	P	P	P	P	P	P	12
	15	Alcanzar participación activa en proyectos según líneas de investigación	P	P				P	P	P	P	P	P	P	P	P	P	12
	16	Lograr que estudiantes y docentes registren proyectos según líneas de investigación	P	P			P	P	P	P	P	P	P	P	P	P	P	13
	17	Administrar banco de problemas y necesidades	P	P	P		P	P	P	P	P	P	P	P	P	P	P	14
	18	Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual	P	P	P			P	P		P		P	P	P	P		10
CLIENTES	19	Lograr el posicionamiento y reconocimiento en la IASD y la sociedad	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	15
	20	Fidelizar a la comunidad educativa	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	15
	21	Difundir la producción intelectual en diferentes medios		P	P	P	P	P	P	P	P	P	P	P	P	P	P	14
	22	Lograr posicionamiento por el logro de la investigación		P	P	P	P	P	P	P	P	P	P	P	P	P	P	14
			18	22	18	12	15	22	22	18	22	19	22	22	22	22	20	

Figura 36 - Cuadro de alineación de los procesos con la estrategia de la universidad

5.1.2. Etapa II: Definición del Modelo de Referencia de Procesos para el gobierno y gestión de la TI de la universidad

En esta etapa se desarrolló la Fase 2 – Referencia de Procesos del Modelo de Evaluación de la Capacidad de Procesos. Esta fase consta de tres actividades. La explicación de cómo se desarrolló cada actividad se encuentra en el Capítulo IV.

El resultado esperado de esta etapa era el Modelo de Referencia de Procesos de Gobierno y Gestión de la universidad. Además, de la adaptación de los procesos del modelo al contexto de la universidad. En la Figura 37 podemos observar que para lograr los objetivos estratégicos la universidad debe implementar un proceso de gobierno y 14 procesos de gestión. Los procesos se gestión de agrupan de la siguiente manera: 6 procesos en el dominio APO, 3 procesos en el dominio BAI, cuatro procesos en el dominio DSS y un proceso en el dominio MEA. En la figura también podemos observar que hay 8 procesos que tienen un resaltado de color crema, esto es, porque estos 8 procesos se alinean con el 100% de los objetivos estratégicos de la universidad, por lo que son considerados procesos críticos de TI. La contextualización de los procesos a la universidad está descrita en el apartado Anexos.

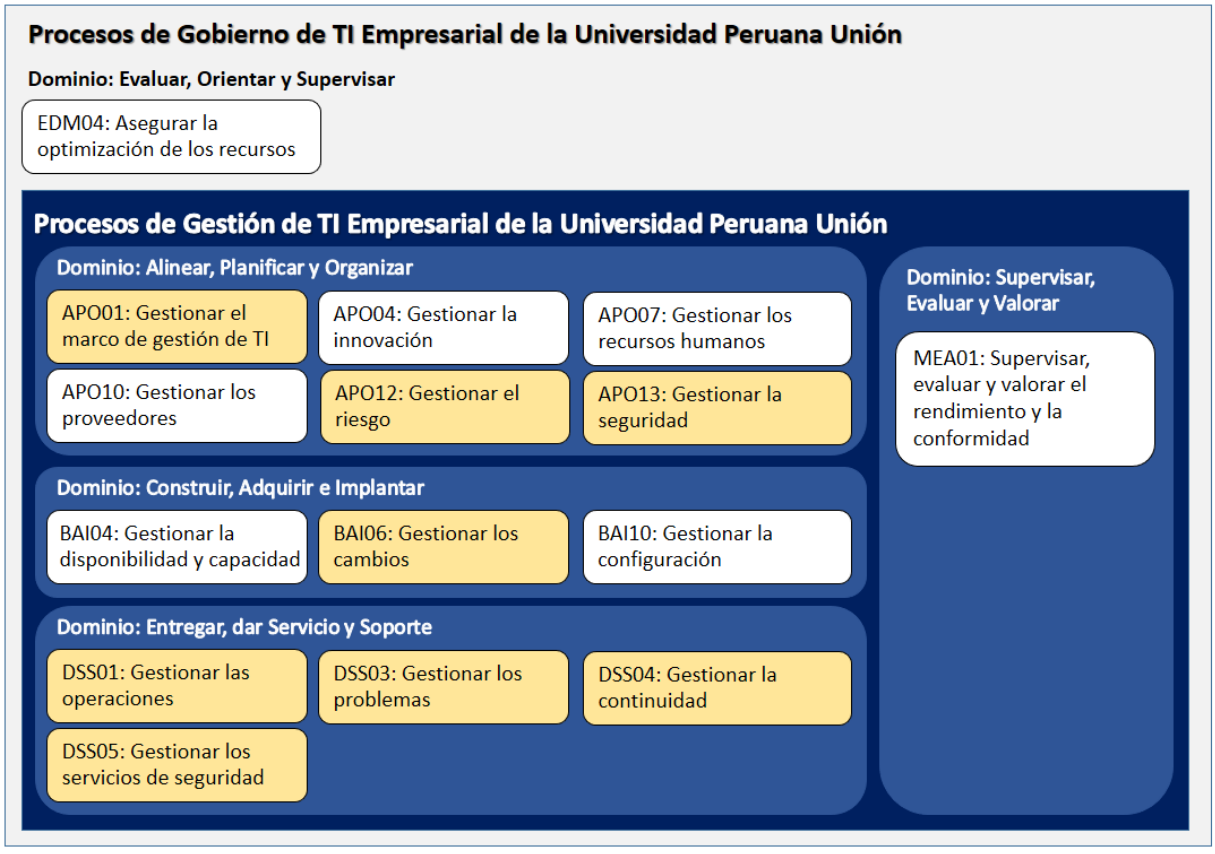


Figura 37 - Modelo de Referencia de Procesos de la universidad

5.1.3. Etapa III: Caracterización formal de la evaluación de la capacidad de procesos de la universidad

En esta etapa se desarrolló la primera parte de la Fase 3 – Evaluación de la Capacidad de Procesos del Modelo. Esta fase consta de dos actividades. La explicación de cómo se desarrolló la caracterización formal de la evaluación de la capacidad del proceso para el Nivel 1, y para los Niveles 2 al 5 se encuentra en el Capítulo IV.

El resultado esperado de esta etapa era la caracterización formal de la evaluación de la capacidad de los procesos en los niveles mencionados. En las Figuras 38 y 39 se aprecia los elementos que conforman cada nivel de evaluación y la forma como se debe aplicar. Las ecuaciones expresadas hacen referencia a la caracterización de cada uno de los elementos que conforman la evaluación de la capacidad de procesos.

Los elementos que intervienen en la evaluación de la capacidad del proceso para el Nivel 1 son: Indicador de Evaluación, Práctica Base, Criterio/Resultado de evaluación. Para la evaluación de los niveles 2 al 5 los elementos son: Indicador de Evaluación, Práctica Genérica, Producto de Trabajo Genérico, Resultado de Cumplimiento. Para ambos niveles de evaluación, el punto de partida es el Indicador de Evaluación.

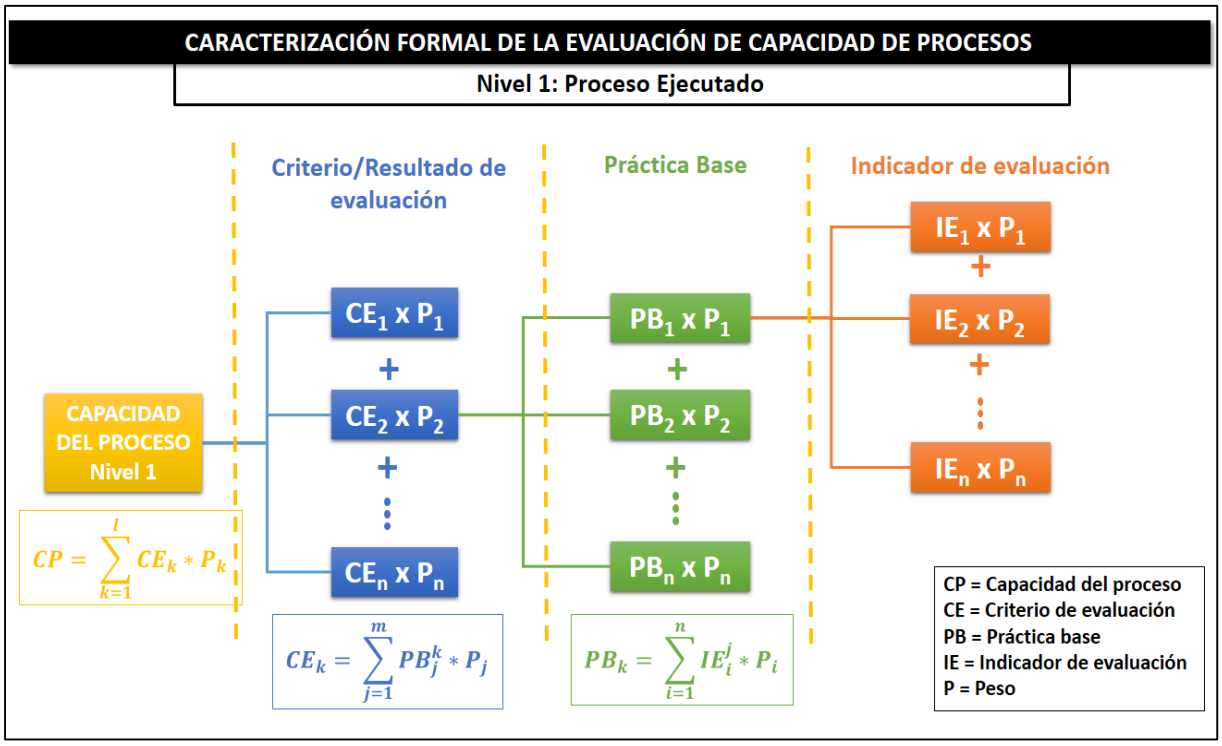


Figura 38 - Caracterización formal de la evaluación de la capacidad de procesos - Nivel 1

A continuación, describimos el significado que cada una de las ecuaciones de la Figura 38.

La ecuación $\boldsymbol{PB_k = \sum_{i=1}^{n} IE_i^j * P_i}$ hace referencia a la evaluación del nivel de cumplimiento de las Prácticas Base (PB) que se calcula con la sumatoria de los Indicadores de Evaluación (IE) que se cumplen, multiplicado por el Peso (P) asignado a cada indicador de evaluación.

La ecuación $\boldsymbol{CE_k = \sum_{j=1}^{m} PB_j^k * P_j}$ hace referencia a la evaluación del nivel de cumplimiento de los Criterios/Resultados de Evaluación (CE), que se calcula con la sumatoria de las Prácticas Base (PB) multiplicado por el Peso (P) asignado a cada práctica base.

La ecuación $\boldsymbol{CP = \sum_{k=1}^{l} CE_k * P_k}$ hace referencia a la evaluación de la Capacidad del Proceso (CP) del Nivel 1, que se calcula con la sumatoria de los Criterios/Resultados de Evaluación (CE) multiplicado por el Peso (P) asignado.

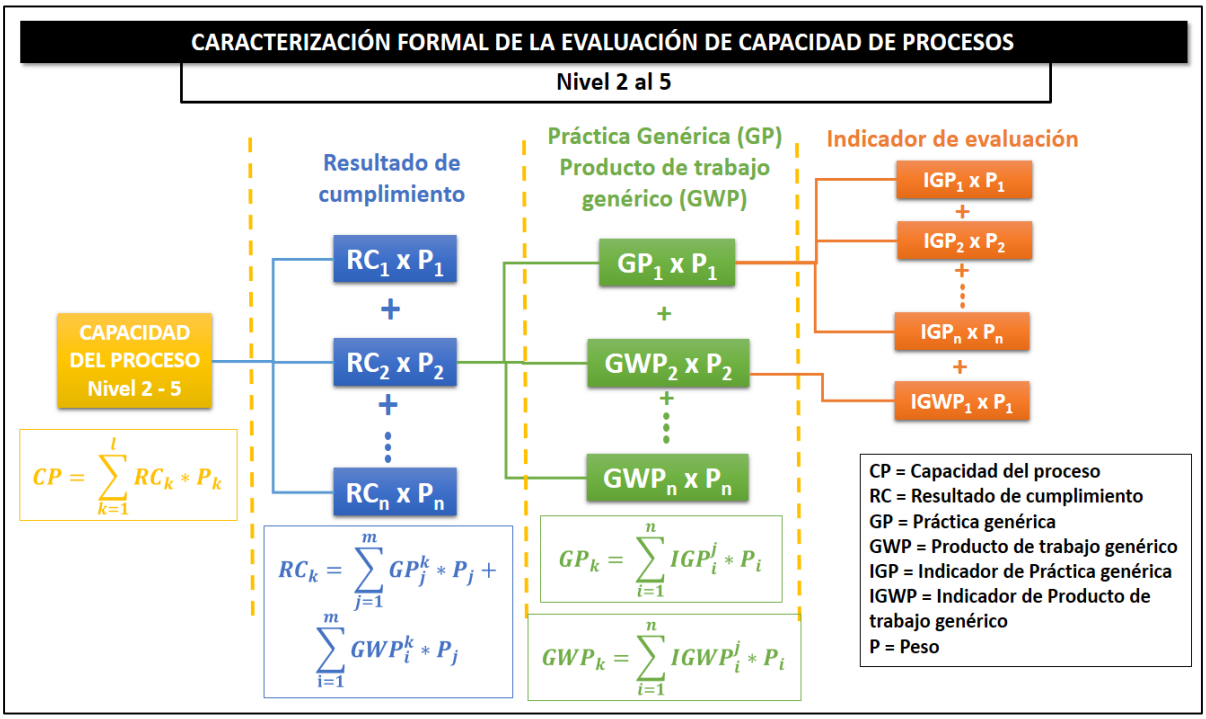


Figura 39 - Caracterización formal de la evaluación de la capacidad de procesos - Niveles 2 al 5

A continuación, se describe el significado de las ecuaciones que se ven en la Figura 39.

La ecuación $\boldsymbol{GP_k = \sum_{i=1}^{n} IGP_i^j * P_i}$ hace referencia a la evaluación del nivel de cumplimiento de las Prácticas Genéricas (GP) que se calcula con la sumatoria de los Indicadores de Evaluación de las Prácticas Genéricas que se cumplen (IGP) multiplicado por el Peso (P) asignado a cada IGP.

La ecuación $\boldsymbol{GWP_k = \sum_{i=1}^{n} IGWP_i^j * P_i}$ hace referencia a la evaluación del nivel de cumplimiento de los Productos de Trabajo Genéricos (GWP) que se calcula con la sumatoria de los Indicadores de Evaluación de los Productos de Trabajo Genéricos que se cumplen (IGWP) multiplicado por el Peso (P) asignado a cada IGWP.

La ecuación $\boldsymbol{RC_k = \sum_{j=1}^{m} GP_j^k * P_j + \sum_{i=1}^{m} GWP_i^k * P_j}$ hace referencia a la evaluación del nivel de cumplimiento de los Resultados de Cumplimiento (RC) que se calcula con la sumatoria de las Prácticas Genéricas (GP) multiplicado por el Peso (P) asignado a cada GP más la sumatoria de los Productos de Trabajo Genéricos (GWP) multiplicado por el Peso (P) asignado a cada GWP.

La ecuación $\boldsymbol{CP = \sum_{k=1}^{l} RC_k * P_k}$ hace referencia a la evaluación de la Capacidad del Proceso (CP) para los niveles 2 al 5, que se calcula con la sumatoria de los Resultados de Cumplimiento (RC) por el Peso (P) asignado a cada RC.

5.1.4. Etapa IV: Aplicación de la caracterización formal para la evaluación de la capacidad de procesos de la universidad

En esta etapa se aplicaron las caracterizaciones de evaluación desarrolladas en la Fase 3 para validar su funcionamiento. Para este fin se evaluó la capacidad del proceso DSS05 Gestionar los servicios de seguridad en la universidad. La explicación de cómo se realizó la evaluación se encuentra en el Capítulo IV.

El resultado esperado en esta etapa era la validación de los elementos de evaluación de cada nivel. La validación de la evaluación del Nivel 1, se obtuvo al determinar la capacidad del proceso evaluado en este nivel. Tal como se observa en la Figura 40, el proceso DSS05 Gestionar los servicios de seguridad está “Ampliamente alcanzado”, pues logró un 69.6% de cumplimiento de las prácticas base de acuerdo a la Escala de Calificación del PAM.

DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD								
PROPÓSITO	Minimizar el impacto en el negocio de las vulnerabilidades operacionales de seguridad de la información y de incidentes							
Calificación por criterios / resultados	69.6%							
Nivel de capacidad alcanzado	Ampliamente alcanzado							
Evaluar si los siguientes resultados son alcanzados		Criterios / Resultados	¿Criterios alcanzados? S/N	Comentario	No alcanzado (0-15%)	Parcialmente Alcanzado (>15% -50%)	Ampliamente Alcanzado (>50% - 85%)	Completamente Alcanzado (>85-100%)
Nivel 1 Proceso Ejecutado	PA 1.1 Desempeño del proceso. El proceso implementado consigue su propósito	**DSS05-O1** Satisfacer las necesidades del negocio respecto a la seguridad de redes y comunicaciones.	S				75%	
		DSS05-O2 La información procesada, almacenada y transmitida por medio de dispositivos de punto final está protegida.	S				71%	
		DSS05-O3 Todos los usuarios tienen un púnico identificador y los derechos de acceso acordes con su función en la empresa.	S				72%	
		DSS05-O4 Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias al ser procesada, almacenada o transmitida	S			45%		
		DSS05-O5 La información electrónica se ha asegurado correctamente cuando se almacena, transmite o destruye.	S				85%	

Figura 40 - Capacidad del proceso DSS05 Gestionar los servicios de seguridad de la universidad

La Figura 41 muestra los resultados de la evaluación de capacidad del proceso DSS05 Gestionar los servicios de seguridad por Prácticas de Gestión, recordemos que este proceso tiene 7 prácticas de gestión. La línea de color naranja es el logro esperado por el proceso y la línea de color azul es el logro alcanzado por cada Práctica de Gestión. Esto significa que existe una brecha de actividades que el proceso debe mejorar para alcanzar el nivel esperado.

La Práctica de Gestión que alcanzó el más alto porcentaje de cumplimiento, 85%, es la práctica DSS05.06 Gestionar documentos sensibles y dispositivos de salida, esto significa que el área de TI de la universidad cumple con las actividades propuestas por COBIT para la protección de la información que se encuentra en los documentos sensibles y dispositivos de salida.

La Práctica de Gestión que alcanzó el más bajo porcentaje de cumplimiento, 45%, es la práctica DSS05.05 Gestionar el acceso físico a los activos de TI, esto significa que el área de TI de la universidad requiere mejorar en cuanto a la protección de los activos de TI,

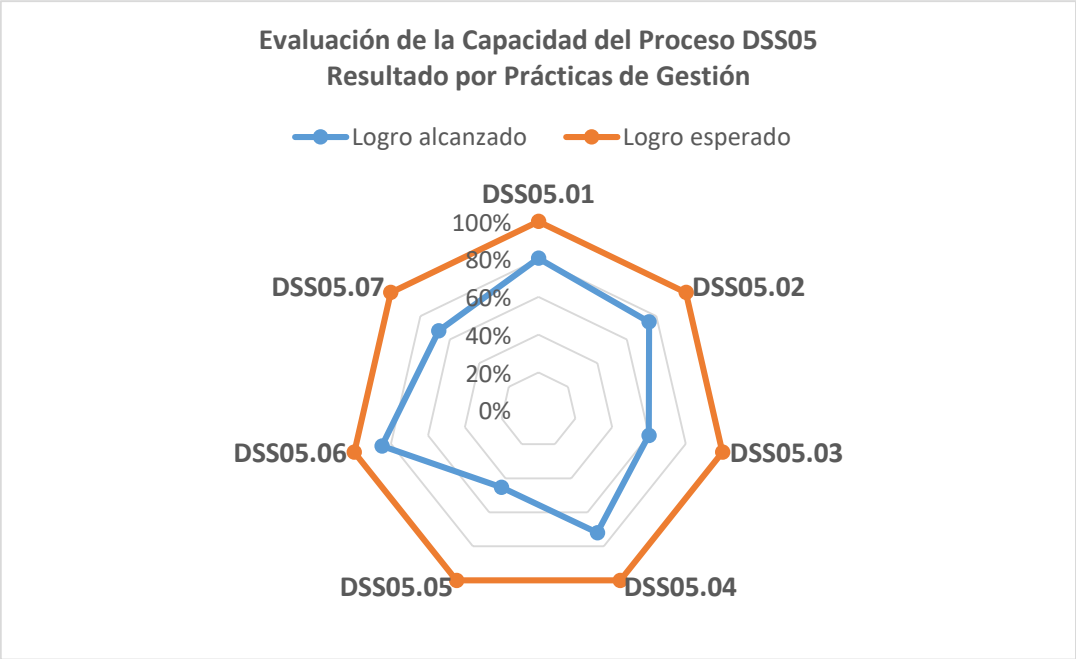


Figura 41 - Resultado de la capacidad del proceso por prácticas de gestión

La validación de los elementos de evaluación de los niveles 2 al 5 se realizó con la elaboración del Instrumento de Evaluación para el Nivel 2. Se debe aclarar que no fue posible aplicar este instrumento pues para evaluar la capacidad del proceso en el Nivel 2, es necesario que el proceso haya alcanzado un valor porcentual entre >85% al 100% en el Nivel 1. La Figura 42 muestra el instrumento de evaluación para el Nivel 2 de capacidad del proceso.

INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 2: PROCESO GESTIONADO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

Atributo: 2.1. Gestión del rendimiento

RESULTADO DE CUMPLIMIENTO			PRÁCTICA GENÉRICA (GP) PRODUCTO DE TRABAJO GENÉRICO (GWP)				N°	PREGUNTA	PESO	SI	NO
N°	DESCRIPCIÓN	PESO	N°	TIPO	DESCRIPCIÓN	PESO					
1	Los objetivos para el rendimiento del proceso están identificados.	20%	2.1.1.	GP	Identificar los objetivos para el rendimiento del proceso. Los objetivos de rendimiento, junto con los supuestos y limitaciones, están definidos y comunicados.	60%	1	Se ha definido los objetivos para el rendimiento del proceso?	25%		
							2	Se ha definido los supuestos para el rendimiento del proceso?	25%		
							3	Se ha definido las limitaciones para el rendimiento del proceso?	25%		
							4	Los objetivos, supuestos y limitaciones para el rendimiento del proceso fueron comunicados a los interesados?	25%		
			1.0	GWP	**Documentación del proceso**: debe describir el alcance del proceso.	20%	5	La documentación del proceso proporciona el alcance del proceso?	100%		
			2.0	GWP	**Plan del proceso**: debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	6	El plan del proceso proporciona los objetivos de rendimiento del proceso?	100%		
2	El rendimiento del proceso está planificado y monitorizado.	20%	2.1.2.	GP	Planificar y monitorizar el rendimiento del proceso para cumplir con los objetivos identificados. Medidas básicas de rendimiento de procesos vinculados a los objetivos de negocio están establecidas y monitorizadas. Incluyen hitos clave, actividades requeridas, estimaciones y planificaciones.	60%	7	Se ha planificado el rendimiento del proceso que permita cumplir con los objetivos?	35%		
							8	Se ha establecido medidas básicas de rendimiento (hitos, actividades, estimaciones)?	35%		
							9	Se monitorea el rendimiento del proceso para ver el cumplimiento de los objetivos?	30%		
			2.0	GWP	**Plan del proceso**: debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	10	El plan del proceso proporciona los objetivos de rendimiento del proceso?	100%		
			9.0	GWP	**Registros del desempeño del proceso**: deben proporcionar detalles de los resultados.	20%	11	Los registros de desempeño del proceso proporcionan los resultados del rendimiento del proceso?	100%		

Figura 42 - Instrumento de evaluación de la capacidad de procesos del Nivel 2

5.2. Descripción del Modelo de Evaluación de la Capacidad de Procesos (ECP) de la Universidad

Luego de aplicada la Metodología de Investigación, el resultado fue el Modelo de Evaluación de la Capacidad de Procesos de la universidad. En esta sección describiremos los elementos que conforman el modelo, aquellos que se basan en COBIT 5 y los aportes que se dieron para obtener el resultado que se consiguió. La Figura 43 muestra la Versión 1.0 del Modelo ECP de la universidad.

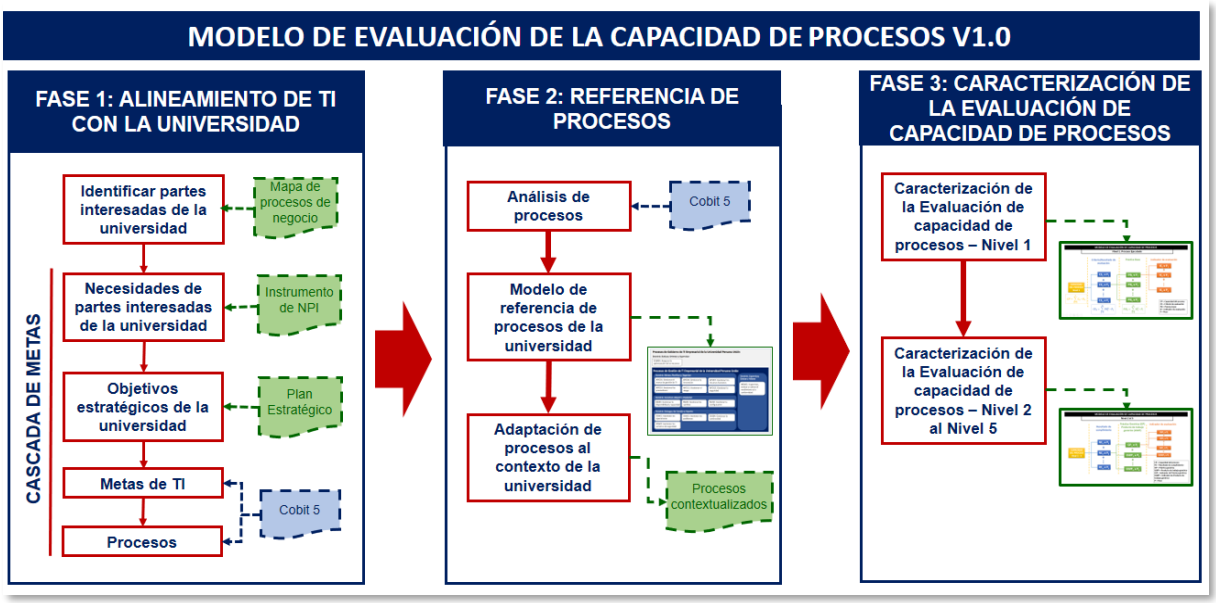


Figura 43 - Modelo ECP versión 1.0

5.2.1. Fase 1 – Alineamiento de TI con la universidad

La Tabla 21 describe, por cada actividad de la Fase 1 del Modelo ECP, lo considerado del COBIT 5, el aporte dado en la investigación y el resultado obtenido. Así, se va desarrollando cada fase del modelo.

Tabla 21 - Descripción de la Fase 1 - Alineamiento de TI con la universidad del Modelo ECP

ACTIVIDAD	COBIT 5	APORTE	RESULTADO
Identificar partes interesadas de la universidad	Definición de partes interesadas, tipos, características	Para una apropiada identificación de las partes interesadas se utilizó el mapa de procesos de la universidad y sus procedimientos.	Se identificaron 20 partes interesadas, 15 internas y 5 externas. Para una mejor evaluación de sus necesidades, se las puede agrupar en Administradores, Administrativos, Docentes, Estudiantes y Externos

Necesidades de las partes interesadas de la universidad	Apéndice D del libro Marco de negocio para el Gobierno y la Gestión de las TI en la empresa. Mecanismo de la cascada de metas	En base a la información del Apéndice D, se elaboró un instrumento para identificar las necesidades de los diferentes grupos de partes interesadas de la universidad (ver en Anexos)	Se identificó las necesidades y la percepción de las partes interesadas sobre las TI de la universidad. El resultado de esta evaluación está en la explicación de la Etapa I de la Metodología de Investigación
Objetivos estratégicos de la universidad	Mecanismo de la Cascada de metas	Se utilizaron los Objetivos Estratégicos (OE) de la universidad definidos en el Plan Estratégico 2014 – 2018 v2.	Luego de un análisis con las partes interesadas se concluyó que, de los 38 OE, 22 son los que responden a las necesidades de las partes interesadas (NPI), es decir 22 OE se alinean con las NPI. Tal como se observa en la Tabla 6.
Metas de TI	Metas de TI del Apéndice B del libro Marco de negocio para el Gobierno y la Gestión de las TI en la empresa. Mecanismo de la cascada de metas		Luego de aplicado el Mecanismo de la Cascada de Metas para este nivel, se identificaron las Mestas de TI de COBIT 5 que se alinean con los 22 OE de la universidad. Los que se observan en la Tabla 7.
Procesos	Apéndice C del libro Marco de negocio para el Gobierno y la Gestión de las TI en la empresa. Mecanismo de la cascada de metas		Luego de aplicado el Mecanismo de la Cascada de Metas para este nivel, se identificaron los procesos de COBIT 5 que se alinean con las Metas de TI, y como consecuencia con los 22 OE de la universidad. Los que se observan en la Tabla 8.

5.2.2. Fase 2 – Referencia de procesos

La Tabla 22 describe, por cada actividad de la Fase 2 del Modelo ECP, lo considerado del COBIT 5, el aporte dado en la investigación y el resultado obtenido. Así, se va desarrollando esta fase del modelo.

Tabla 22 - Descripción de la Fase 2 - Referencia de procesos del Modelo ECP

ACTIVIDAD	COBIT 5	APORTE	RESULTADO
Análisis de procesos	Descripción de los procesos de COBIT alineados obtenidos del libro Procesos Catalizadores		Identificación de los elementos que debían contextualizarse a la realidad de la universidad.

Modelo de referencia de procesos de la universidad	Modelo de referencia de procesos de COBIT 5	Organización de los 15 procesos resultantes de acuerdo a los 5 dominios del modelo de referencia de procesos de COBIT 5	Modelo de referencia de procesos de la universidad, identificando los procesos críticos que se deben implementar para alcanzar los OE de la universidad. Ver Figura 46.
Adaptación de procesos al contexto de la universidad	Descripción de los procesos de COBIT alineados obtenidos del libro Procesos Catalizadores	Para cada proceso de identificaron los siguientes elementos: dueño del proceso, partes interesadas internas y externas, OE alineados	Los 15 procesos resultantes de la cascada de metas fueron contextualizados a la universidad incorporando a su descripción los elementos mencionados.

5.2.3. Fase 3 – Caracterización de la evaluación de la capacidad de procesos

La Tabla 23 describe, por cada actividad de la Fase 3 del Modelo ECP, lo considerado del COBIT 5, el aporte dado en la investigación y el resultado obtenido. Así, se va desarrollando esta fase del modelo.

Tabla 23 - Descripción de la Fase 3 - Caracterización de la evaluación de la capacidad de procesos del Modelo ECP

ACTIVIDAD	COBIT 5	APORTE	RESULTADO
Caracterización de la evaluación de la capacidad de procesos – Nivel 1	Elementos del PAM para evaluar la capacidad de los procesos en el Nivel 1	Definición de nuevo elementos, el Indicador de Evaluación, como base para la evaluación del nivel de cumplimiento de las Prácticas Base. Desglose de los elementos: Prácticas Base y Criterios/Resultado de evaluación del PAM para una mejor evaluación del nivel de cumplimiento de cada uno. Caracterización formal de los elementos que intervienen en la evaluación de la capacidad de procesos.	Elaboración de un instrumento de evaluación de la capacidad de procesos para el Nivel 1. Aplicación del instrumento para medir la capacidad del proceso DSS05 Gestionar los servicios de seguridad. Determinación de la capacidad del proceso evaluado. Interpretación del resultado y propuestas de mejora.
Caracterización de la evaluación de la capacidad de procesos – Nivel 2 al Nivel 5	Elementos del PAM para evaluar la capacidad de los procesos en el Nivel 2 al Nivel 5	Definición de nuevo elemento, el Indicador de Evaluación, como base para la evaluación del nivel de cumplimiento de las Prácticas Genéricas y los Productos de Trabajo Genéricos. Desglose de los elementos: Prácticas Genéricas, Productos de Trabajo Genéricos, y Resultados de cumplimiento del PAM para una mejor evaluación del nivel de cumplimiento de cada uno.	Elaboración de un instrumento de evaluación de la capacidad de procesos para el Nivel 2 al Nivel 5. Aplicación del instrumento para medir la capacidad del proceso DSS05 Gestionar los servicios de seguridad. Determinación de la capacidad del proceso en el Nivel evaluado. Interpretación del resultado y propuestas de mejora.

	Caracterización formal de los elementos que intervienen en la evaluación de la capacidad de procesos.

Finalmente, mencionaremos que el Modelo ECP se desarrolla en 3 fases y 10 actividades. La realización de las actividades en cada fase conlleva a un resultado, los cuáles se describen a continuación:

- Resultado de la Fase 1: alineación de los procesos de TI con los objetivos estratégicos de la universidad, para esto se utilizó el procedimiento de la Cascada de Metas.
- Resultado de la Fase 2: modelo de referencia de procesos de la universidad y la contextualización de los procesos de TI alineado.
- Resultado de la Fase 3: Evaluación de la capacidad de los procesos, para esto se utilizó el procedimiento para la evaluación del Nivel 1 y para la evaluación de los Niveles 2 al 5.

CONCLUSIONES

Se logró el objetivo general de la investigación, diseñar el Modelo de Evaluación de la Capacidad de Procesos de TI para el gobierno y gestión de tecnologías de información basado en las buenas prácticas de COBIT 5 para una universidad. Este modelo fue validado por juicio de experto, siendo el resultado de que el modelo es aplicable.

Para el diseño de la Fase 1 del modelo, se propuso un procedimiento para la alineación de los procesos de TI con los objetivos estratégicos de la universidad, con el propósito de identificar aquellos que realmente aportan valor a la institución. El resultado de esta alineación fue de 15 procesos de TI, de los cuáles 8 se relacionan con todos los objetivos estratégicos de la universidad.

En la Fase 2 del modelo se diseñó el Modelo de Referencia de Procesos de TI para la universidad, basado en el resultado del procedimiento de alineación de la Fase 1. Se utilizó la distribución propuesta por el Marco COBIT 5. En esta distribución se puede observar que los 15 procesos se ubican dentro de las 5 dimensiones de COBIT: un proceso en la dimensión EDM, 6 procesos en la dimensión APO, 3 procesos en la dimensión BAI, 4 procesos en la dimensión DSS y un proceso en la dimensión MEA.

En la Fase 3 del modelo, se definieron los elementos necesarios para la evaluación de la capacidad de los procesos alineados. El modelo de evaluación de capacidad de procesos establece dos formas de evaluación: la evaluación del Nivel 1 que mide el Rendimiento del proceso y la evaluación de los Niveles 2 al 5 que mide la gestión, despliegue, control, medición, innovación y optimización del proceso, de acuerdo a los propuesto por el PAM de COBIT 5. Una vez identificados los elementos para las dos formas de evaluación, se realizó la caracterización formal del modelo de evaluación de capacidad de procesos en sus dos formas. Esta caracterización permite la construcción del instrumento de evaluación para cada proceso de acuerdo al nivel que se desee evaluar.

Las formas de evaluación definidas en la Fase 3, fueron aplicadas en la evaluación de la capacidad del proceso DSS05 Gestionar los niveles de seguridad. El resultado de la evaluación del Nivel 1 – Rendimiento del proceso fue de 69.6% lo que significa que el proceso está Ampliamente alcanzado. Sin embargo, no se pudo aplicar la evaluación de los Niveles 2 al 5 pues para realizar esta evaluación se debía alcanzar un puntaje entre el 85% y el 100% en el nivel anterior.

Finalmente, se concluye que con el diseño y aplicación de cada fase del modelo de evaluación de la capacidad de procesos de TI se puede establecer los tres elementos de gobierno y gestión TI para la universidad: alineación estratégica de las tecnologías de información, la entrega de valor a las partes interesadas y la medición del rendimiento de las TI.

RECOMENDACIONES

El Modelo ECP fue desarrollado para una universidad en específico, sin embargo, puede ser aplicado a cualquier otro contexto empresarial, considerando el uso de los recursos que se indican en el desarrollo de cada fase del modelo. Se recomienda tener amplio conocimiento de la organización, así como de la estrategia.

Es conveniente que las organizaciones que deseen iniciar el gobierno de TI, elijan un marco de referencia que les sirva de orientación. Recomendamos el COBIT 5, por ser un marco de referencia completo, flexible, y que permite la integración de las buenas prácticas y normas de calidad que la organización ya tenga implementado.

Esta investigación abarca tres aspectos clave de gobierno de TI: la alineación estratégica de la TI, la entrega de valor a las partes interesadas y la medición del rendimiento de las TI. En el caso de que la organización decida tomar como referencia el marco COBIT, recomendamos el uso del Modelo ECP para realizar la alineación estratégica e identificar los procesos de TI necesarios para el logro de sus objetivos.

Un aspecto muy importante para el desarrollo de toda organización es la medición de lo que hace. Conocer si lo que hace está bien hecho y sigue la dirección definida, permite tomar decisiones que aporten al desarrollo de la empresa. En este sentido, recomendamos el uso del Modelo ECP para la evaluación de la capacidad de sus procesos de TI, y así conocer que aspectos deben mejorar para que las TI realmente sean el aporte tecnológico que la estrategia requiere.

REFERENCIAS

[1] C. Juiz, "Gobernar para ti, gobernar las TI, las TI para gobernar," *BrigthTALK*, 2014. [Online]. Available: https://www.brighttalk.com/webcast/8103/107633?utm_campaign=webcasts-search-results-feed&utm_content=gobierno de ti&utm_source=brighttalk-portal&utm_medium=web. [Accessed: 08-Oct-2017].

[2] C. Juiz, "El gobierno de TI llevado a la práctica," *BrigthTALK*, 2013. [Online]. Available: https://www.brighttalk.com/webcast/8103/77877?utm_campaign=webcasts-search-results-feed&utm_content=gobierno de ti&utm_source=brighttalk-portal&utm_medium=web. [Accessed: 08-Oct-2017].

[3] M. Zambrano and L. Molina, "Diagnóstico situacional del Gobierno de las Tecnologías de Información. Caso Universidad Laica Eloy Alfaro de Manabí," *Cienc. UNEMI*, vol. 10, no. 25, pp. 111–122, 2017.

[4] ISACA, *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*, Primera Ed. Rolling Meadows, 2012.

[5] W. Rivas, "DIAGNÓSTICO Y PLAN DE ACCION PARA LA IMPLEMENTACION DEL MARCO DE NEGOCIO PARA EL GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (COBIT5.0) APLICADO A LA UNIVERSIDAD TÉCNICA DE MACHALA," Universidad de Cuenca, 2017.

[6] V. de las M. Villareal, "Modelo de Gestión y Gobierno de Tecnologías de la Información en la Universidad Estatal Amazónica," Pontificia Universidad Católica del Ecuador, 2018.

[7] A. Lozano and J. Utreras, "Diseño de un Marco Referencial de Gobierno de TI basado en Instituciones Educativas K-12 radicadas en Ecuador (Tesis de Maestría)," Universidad de las Américas, 2014.

[8] A. Páez and F. Vivas, "MODELO PARA LA DEFINICIÓN E IMPLEMENTACIÓN DE PROCESOS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN APLICADO A CENIT TRANSPORTE Y LOGÍSTICA DE HIDROCARBUROS S.A.S.," Universidad del Rosario, 2015.

[9] E. J. Mazo, "Evolución de un modelo de gobernabilidad empresarial de TI en una empresa líder del sector agroindustrial," Escuela Colombiana de Ingeniería Julio Garavito, 2015.

[10] C. Carmona Ramírez, "Modelo de Gobernabilidad basado en COBIT para la Gestión

por Procesos definida en un espacio multidimensional," Universidad de Medillín, 2013.

[11] ISACA, *Modelo de evaluación de capacidad de procesos (PAM): usando COBIT 5*, Primera Ed. Rolling Meadows, 2013.

[12] Organización para la Cooperación y el Desarrollo Económico(OCDE), *Principios de Gobierno Corporativo de la OCDE*, Primera. Paris, 2004.

[13] J. M. Flórez-Parra and M. V. López Pérez, "El gobierno corporativo de las Universidades: Estudio de las 100 primeras Universidades del ranking de Shanghái," *Rev. Educ.*, p. 17, 2014.

[14] OCDE, *Principios de Gobierno Corporativo de la OCDE y del G20*, Primera. Paris, 2016.

[15] J. M. Ballester, "Gobierno corporativo tic."

[16] A. Fernández Martinez and F. Llorens Largo, *Gobierno de las TI para universidades*, Primera Ed., vol. 1. Madrid, España, 2015.

[17] T. Nakano Osores, "Integración y gobernanza del las TIC en las Universidades: análisis situacional de la PUCP," Pontificia Universidad Católica del Perú, 2014.

[18] ISACA, *Procesos Catalizadores*, Primera Ed. Rolling Meadows, 2012.

[19] A. Vara, *7 pasos para elaborar una tesis*, Primera. Lima, Perú, 2015.

[20] R. Hernández, C. Fernández, and P. Baptista, *Metodología de la investigación*, vol. 53, no. 9. 2014.

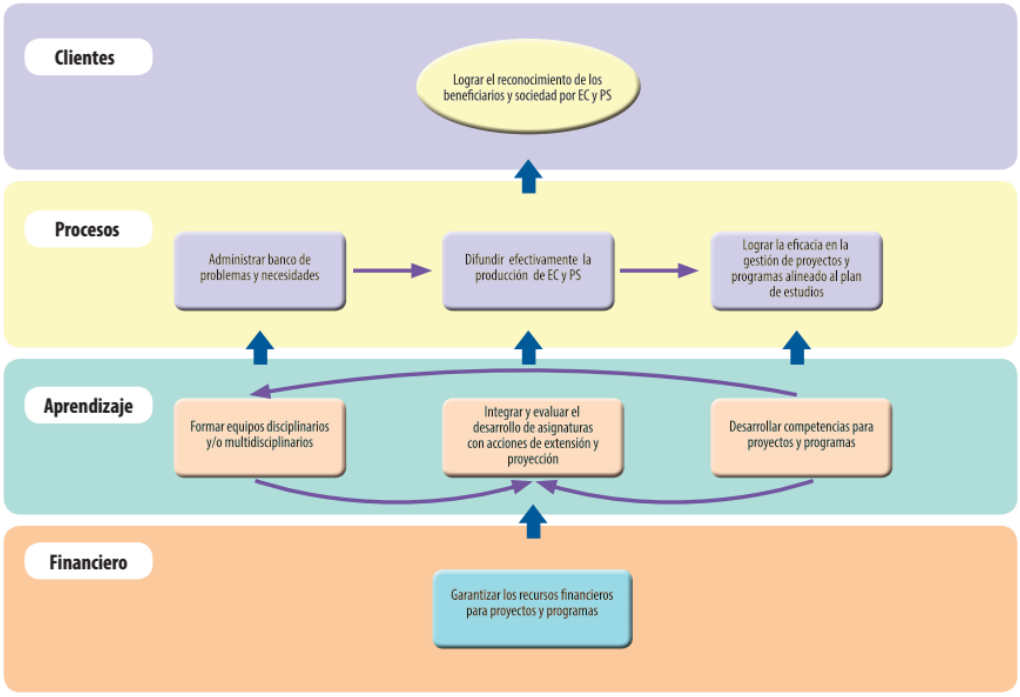
[21] Universidad, "Plan Estratégico 2014-2018 V2," 2015. .

[22] J. Escobar-Pérez, "Validez de contenido y juicio de expertos: una aproximación a su utilización," *Av. en medición*, vol. 6, no. 2, pp. 27–36, 2008.

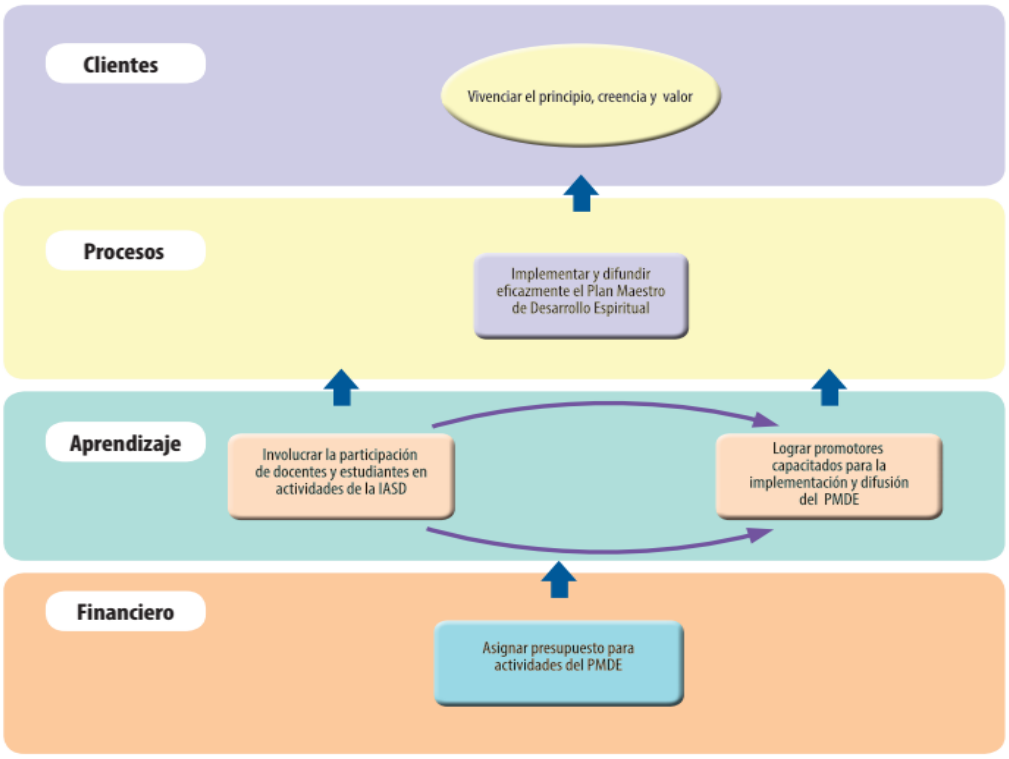
ANEXOS

1. Mapas estratégicos del Plan Estratégico 2014 – 2018 de la universidad

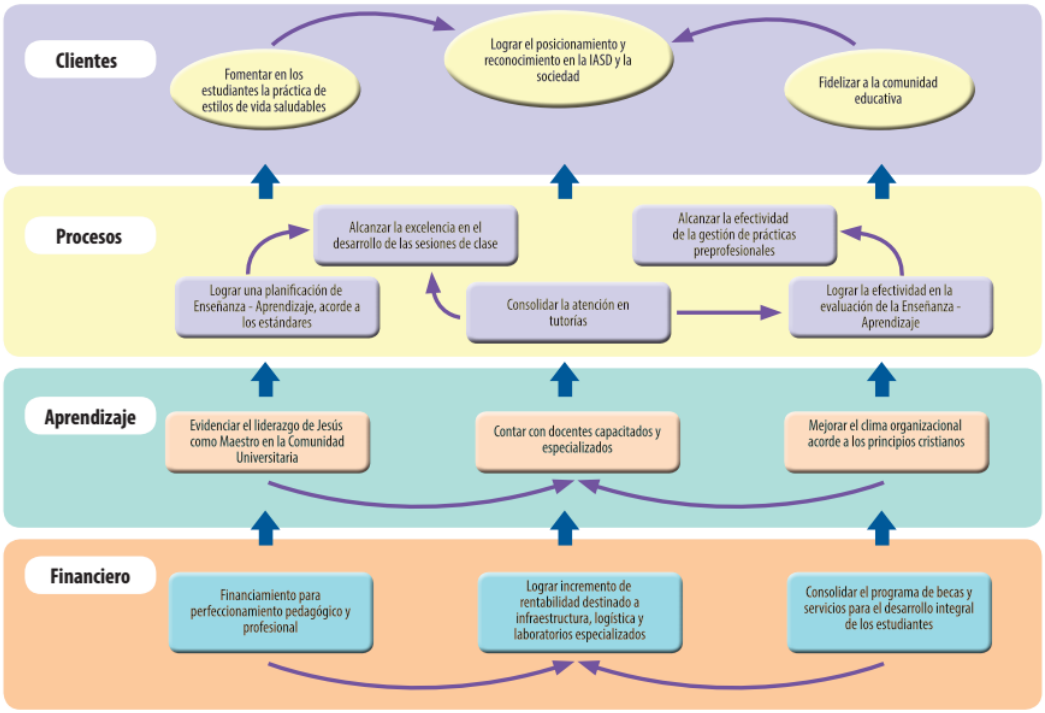
MAPA ESTRATÉGICO DE EXTENSIÓN CULTURAL Y PROYECCIÓN SOCIAL



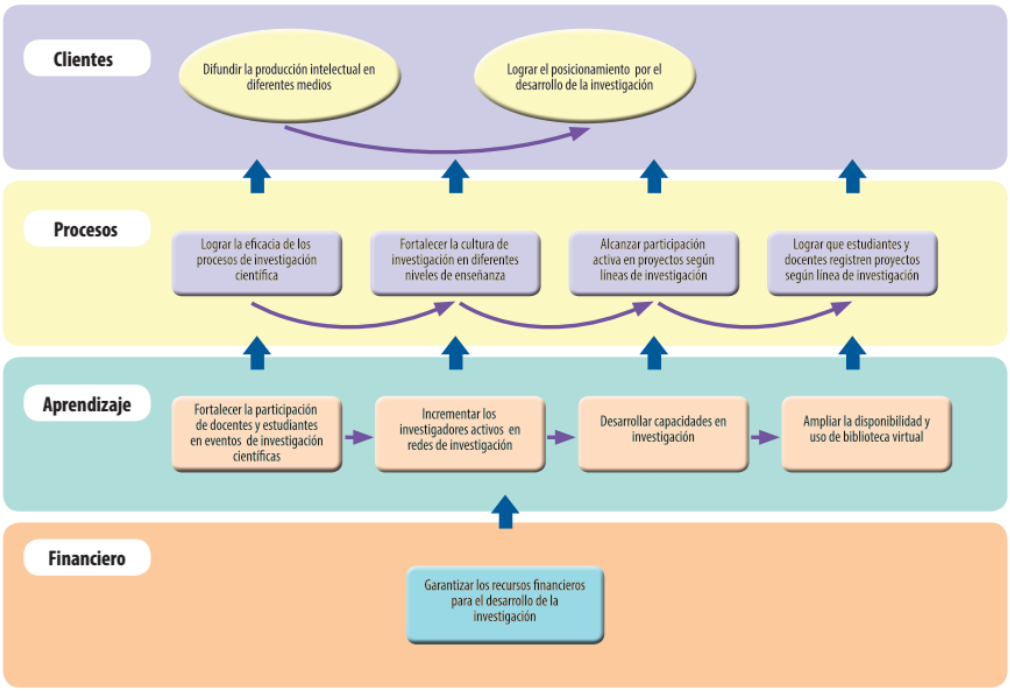
MAPA ESTRATÉGICO DE DESARROLLO ESPIRITUAL



MAPA ESTRATÉGICO DE ENSEÑANZA - APRENDIZAJE



MAPA ESTRATÉGICO DE INVESTIGACIÓN



2. Adaptación de los 14 procesos restantes que se alinean a la estrategia de la universidad

<table>
<tr><td colspan="2">EDM04: Asegurar la optimización de recursos</td><td>Área: Gobierno
Dominio: Evaluar, Orientar y Supervisar</td></tr>
<tr><td colspan="3">Descripción:
Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.</td></tr>
<tr><td colspan="3">Propósito:
Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.</td></tr>
<tr><td colspan="2">Dueño del proceso:
Director de DIGETI</td><td>Partes interesadas:
a) Rector
b) Gerente General
c) Vicerrector
d) Decanos</td></tr>
<tr><td colspan="3">Metas corporativas relacionadas:</td></tr>
<tr><td colspan="3">03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes
08 Contar con docentes capacitados y especializados
10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
11 Incrementar los investigadores activos en redes de investigación
12 Desarrollar capacidades en investigación
13 Ampliar la disponibilidad y uso de biblioteca virtual
19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares
20 Alcanzar la excelencia en el desarrollo de las sesiones de clase
21 Consolidar la atención en tutorías
22 Alcanzar la efectividad de la gestión de prácticas pre profesionales
23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
24 Lograr la eficacia de los procesos de investigación científica
25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza
26 Alcanzar participación activa en proyectos según líneas de investigación
27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación
28 Administrar banco de problemas y necesidades
31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual
33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad
34 Fidelizar a la comunidad educativa
36 Lograr posicionamiento por el logro de la investigación</td></tr>
<tr><td colspan="3">Metas de TI relacionadas:</td></tr>
<tr><td>- Agilidad de las TI</td><td colspan="2">- Nivel de satisfacción de los ejecutivos de la universidad con la capacidad de respuesta de la TI a nuevos requerimientos
- Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas</td></tr>
<tr><td>- Optimización de los activos, recursos</td><td colspan="2">- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI</td></tr>
<tr><td>16 Personal del negocio y de las TI competente y motivado</td><td colspan="2">- Porcentaje del personal cuyas habilidades de TI son suficientes para las competencias requeridas para su función
- Porcentaje del personal satisfecho con su función de TI</td></tr>
<tr><td colspan="3">Metas del proceso:</td></tr>
<tr><td>Las necesidades de recursos de la empresa son cubiertas con capacidades óptimas</td><td colspan="2">- Nivel de realimentación de las partes interesadas sobre la optimización de los recursos
- Serie de beneficios que se logran a través de la utilización óptima de los recursos</td></tr>
<tr><td>Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones</td><td colspan="2">- Porcentaje de proyectos con asignación de recursos adecuados</td></tr>
<tr><td>El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico</td><td colspan="2">- Porcentaje de proyectos y programas con un estado de riesgo medio o alto debido a los problemas en la gestión de recursos
- Número de metas de rendimiento de la gestión de recursos alcanzadas</td></tr>
<tr><td colspan="3">Prácticas de Gobierno</td></tr>
<tr><td colspan="3">EDM04.01 Evaluar la gestión de recursos
Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con la TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa.</td></tr>
<tr><td colspan="3">Iniciativas y/o Documentos E/S</td></tr>
</table>

Entrada: - Brechas y cambios necesarios para hacer realidad los objetivos de capacidad - Planes de desarrollo de competencias - Decisiones sobre los resultados de evaluación de proveedores	Salida: - Principios rectores para la asignación de recursos y capacidades - Principios rectores de la arquitectura de la empresa - Plan de recursos aprobado
Actividades: 1. Examinar y evaluar la estrategia actual y futura las opciones de aprovisionamiento de recursos de TI y desarrollar capacidades para cubrir las necesidades actuales y futuras (incluyendo alternativas de aprovisionamiento). 2. Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI puedan satisfacer las necesidades de la empresa, con la habilidad y capacidad requerida, de acuerdo a las prioridades acordadas y las limitaciones presupuestarias. 3. Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la empresa para la entrega de valor y la mitigación de riesgos con los recursos asignados. 4. Comprender los requisitos para alinear la gestión de recursos con la planificación de recursos empresariales financieros y humanos. 5. Definir los principios para la gestión y el control de la arquitectura de la empresa.	
EDM04.02 Orientar la gestión de recursos Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica	
Iniciativas y/o Documentos E/S	
Entrada:	Salida: - Comunicación de las estrategias de reasignación de recursos - Responsabilidades asignadas para la gestión de los recursos - Principios para la protección de recursos
Actividades: 1. Comunicar e impulsar la adopción de estrategias de gestión de recursos, principios y el plan de recursos y las estrategias de arquitectura de empresa acordados 2. Asignar responsabilidades para la ejecución de la gestión de recursos 3. Definir los objetivos medidas y métricas clave para la gestión de los recursos 4. Establecer los principios relacionados con la protección de recursos 5. Alinear la gestión de recursos con la planificación de RRHH y financiera de la empresa	
EDM04.03 Supervisar la gestión de recursos Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas	
Iniciativas y/o Documentos E/S	
Entrada:	Salida: - Comentarios sobre la asignación y la eficacia de los recursos y capacidades - Acciones correctivas para hacer frente a las desviaciones de gestión de recursos
Actividades: 1. Supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la empresa mediante objetivos y métricas acordados 2. Supervisar las estrategias de aprovisionamiento de TI y de arquitectura de la empresa y los recursos y capacidades de TI para garantizar que las necesidades actuales y futuras de la empresa pueden ser satisfechas 3. Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes	

APO01: Gestionar el Marco de Gestión de TI	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	
Propósito: Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** Gerente General Vicerrector Decanos

Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI.
09 Agilidad de las TI	- Nivel de satisfacción de los ejecutivos de la universidad con la capacidad de respuesta de la TI a nuevos requerimientos - Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
16 Personal del negocio y de las TI competente y motivado	- Porcentaje del personal cuyas habilidades de TI son suficientes para las competencias requeridas para su función - Porcentaje del personal satisfecho con su función de TI
Metas del proceso:	
Se ha definido y se mantiene un conjunto eficaz de políticas	- Porcentaje de políticas, estándares y otros elementos catalizadores activos documentados y actualizados - Número de exposiciones a riesgos debidas a la inadecuación del diseño del entorno de control
Todos tienen conocimiento de las políticas y de cómo deberían implementarse	- Número de empleados que asistieron a sesiones de formación o de sensibilización - Porcentaje de proveedores con contratos en los que se definen requisitos de control
Prácticas de Gestión	
APO01.01 Definir la estructura organizativa Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.	
Iniciativas y/o Documentos E/S	
Entrada: - Modelo de toma de decisiones - Modelos de arquitectura de procesos	Salida: - Definición de estructura y funciones organizativas - Directrices operativas de la organización - Reglas de comunicación
1. Definir el alcance, las funciones internas y externas, los roles internos y externos, y las capacidades y los derechos de decisión requeridos, incluidas actividades de TI realizadas por terceras partes. 2. Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la gestión y ejecución de servicios de TI. 3. Establecer la implicación de las partes interesadas críticas para la toma de decisiones (quiénes rendirán cuentas, quiénes son responsables, quiénes deben ser consultados y quiénes informados). 4. Alinear la organización relativa a TI con los modelos organizativos de arquitectura corporativa. 5. Definir el enfoque, los roles y las responsabilidades de cada función dentro de la estructura organizativa relativa a TI. 6. Definir las estructuras y relaciones de gestión para contribuir a las funciones y roles de gestión y ejecución, en consonancia con la dirección de gobierno establecida.	

7. Establecer un Comité Estratégico de TI (o equivalente) a nivel del Consejo de Administración. Este comité debería asegurarse de que el gobierno de TI, como parte del gobierno corporativo, está contemplado de forma adecuada, debe aconsejar sobre la dirección estratégica y revisar las inversiones principales, en representación del consejo de administración al completo.
8. Establecer un comité directivo de TI (o equivalente) compuesto por la dirección ejecutiva, de negocio y de TI para determinar las prioridades de los programas de inversión de TI de acuerdo con la estrategia y prioridades de negocio de la empresa; realizar un seguimiento del estado de los proyectos y resolver los conflictos de recursos; y supervisar los niveles de servicio y las mejoras en el servicio.
9. Proporcionar directrices para cada estructura de gestión (incluyendo órdenes, objetivos, asistentes a reuniones, marco temporal, seguimiento, supervisión y vigilancia), así como las entradas requeridas y las salidas esperadas en cuanto a las reuniones.
10. Definir reglas básicas de comunicación mediante la identificación de las necesidades comunicativas y la implementación de planes basados en dichas necesidades, teniendo en cuenta la comunicación de arriba hacia abajo, de abajo hacia arriba y horizontal.
11. Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre el negocio y las funciones de TI dentro de la empresa y con entidades no pertenecientes a la empresa.
12. Verificar regularmente la adecuación y la eficacia de la estructura organizativa.

APO01.02 Establecer roles y responsabilidades

Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Niveles de autoridad - Responsabilidades asignadas para la gestión de recursos - Matriz de habilidades y competencias - Roles, responsabilidades y niveles de decisión del SGC	- Definición de roles y responsabilidades relativos a TI - Definición de prácticas de supervisión

Actividades:

1. Establecer, acordar y comunicar roles y responsabilidades relativos a TI para todo el personal de la empresa, de acuerdo con las necesidades y los objetivos del negocio. Delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones.
2. Tener en cuenta los requisitos desde la empresa y la continuidad del servicio de TI a la hora de definir los roles, incluyendo el respaldo por parte de la plantilla y los requisitos de formación interdisciplinar.
3. Contribuir al proceso de continuidad del servicio de TI manteniendo actualizada la información de contacto y las descripciones de roles de la empresa.
4. Incluir en las descripciones de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales.
5. Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. El nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas.
6. Asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades.
7. Estructurar los roles y las responsabilidades para reducir las posibilidades de que un solo rol pueda comprometer un proceso crítico.

APO01.03 Mantener los elementos catalizadores del sistema de gestión

Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos).

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Problemas y factores de riesgo emergentes - Resultados del análisis de riesgos	- Políticas relativas a TI

Actividades:

1. Adquirir comprensión de la visión, la dirección y la estrategia corporativas.
2. Tener en cuenta el entorno interno de la empresa, incluyendo la cultura y la filosofía de gestión, la tolerancia al riesgo, la seguridad, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de integridad en la gestión.
3. Inferir e integrar los principios de TI con los principios de negocio.
4. Alinear el entorno de control de TI con el entorno de políticas de TI, con los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control. Evaluar las buenas prácticas o los requisitos específicos del sector (p. ej.,normativa específica del sector) e integrarlos donde corresponda.

5. Alinearse con todos los estándares y códigos de práctica de gobierno y gestión aplicables a nivel nacional e internacional y evaluar buenas prácticas disponibles, como el Marco de Trabajo Integrado para Control Interno de COSO y el Marco de Trabajo Integrado para Gestión Empresarial del Riesgo de COSO.
6. Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
7. Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativo o de negocio.
8. Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.
9. Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.

APO01.04 Comunicar los objetivos y la dirección de gestión

Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Principios de protección de recursos - Comunicación de impacto de riesgos - Comunicación sobre el valor del conocimiento - Política de prevención de software malicioso - Política de seguridad de la conectividad - Políticas de seguridad sobre terminales	- Comunicación de objetivos de TI

Actividades

1. Comunicar continuamente los objetivos y la dirección de TI. Asegurar que las comunicaciones reciban apoyo de la dirección ejecutiva, tanto de palabra como mediante acciones, empleando todos los canales disponibles.
2. Garantizar que la información comunicada engloba una clara articulación de la misión, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código ético/de conducta, las políticas y procedimientos, los roles y las responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado para cada respectiva audiencia dentro de la empresa.
3. Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo.

APO01.05 Optimizar la ubicación de la función de TI

Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte del CIO debe ser proporcional a la importancia de las TI en la empresa.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Modelo operativo empresarial - Estrategia del negocio	- Definir la función operacional de las funciones de TI

Actividades

1. Entender el contexto de la función de TI, incluyendo una evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, híbrido), importancia de TI, la situación y opciones para la provisión.
2. Identificar, evaluar y priorizar las opciones para la ubicación en la organización, los modelos operativos y de aprovisionamiento.
3. Definir la ubicación de las función de TI y obtener aprobación.

APO01.06 Definir la propiedad de la información y del sistema

Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
	- Directrices para la clasificación de los datos - Directrices para el control y seguridad de los datos - Procedimientos de integridad de los datos

Actividades

1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa.
2. Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario.
3. Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.
4. Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (*data warehouses*) y archivos de datos.

APO01.07 Gestionar la mejora continua de los procesos

Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Actualización de políticas, principios, procedimientos y estándares	- Evaluaciones de la capacidad de los procesos - Oportunidades de mejora de proceso - Objetivos y métricas de rendimiento para el seguimiento de la mejora de procesos

Actividades

1. Identificar los procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora. Analizar las diferencias en la capacidad y control del proceso. Identificar las opciones de mejora y rediseño de procesos. Priorizar iniciativas para la mejora de procesos basadas en el potencial coste-beneficio.
2. Implementar las mejoras acordadas, funcionando como una práctica normal del negocio y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.
3. Considerar las maneras de mejorar la eficiencia y eficacia (p. ej., mediante formación, documentación, estandarización y automatización de procesos).
4. Aplicar prácticas de gestión de calidad para la actualización de procesos.
5. Retirar procesos, componentes o catalizadores desactualizados.

APO01.08 Mantener el cumplimiento con las políticas y procedimientos

Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Actualización de políticas, principios, procedimientos y estándares	- Acciones de remediación por no cumplimiento

Actividades

1. Hacer un seguimiento del cumplimiento con políticas y procedimientos.
2. Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir el cambio de requerimientos).
3. Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.
4. Evaluar periódicamente el desempeño de los catalizadores del marco de referencia y adoptar las acciones necesarias.
5. Analizar las tendencias en el funcionamiento y cumplimiento y adoptar las acciones apropiadas.

APO04: Gestionar la Innovación	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**

Descripción:

Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.

Propósito:

Lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.

Dueño del proceso:	**Partes interesadas:**
Director de DIGETI	- Rector - Gerente General - Vicerrector - IASD - Comunidad

Metas corporativas relacionadas:

03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes
08 Contar con docentes capacitados y especializados
10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
11 Incrementar los investigadores activos en redes de investigación
12 Desarrollar capacidades en investigación
13 Ampliar la disponibilidad y uso de biblioteca virtual
16 Desarrollar competencias para proyectos y programas
19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares
20 Alcanzar la excelencia en el desarrollo de las sesiones de clase

21 Consolidar la atención en tutorías
22 Alcanzar la efectividad de la gestión de prácticas pre profesionales
23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
24 Lograr la eficacia de los procesos de investigación científica
25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza
26 Alcanzar participación activa en proyectos según líneas de investigación
27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación
28 Administrar banco de problemas y necesidades
31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual
33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad
34 Fidelizar a la comunidad educativa
35 Difundir la producción intelectual en diferentes medios
36 Lograr posicionamiento por el logro de la investigación

Metas de TI relacionadas:	
08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	- Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios TI que dan soporte a estos procesos - Nivel de comprensión de los usuarios de negocio sobre cómo las soluciones tecnológicas soportan sus procesos - Nivel de satisfacción de los usuarios de negocio con la formación y manuales de usuario
09 Agilidad de las TI	- Nivel de satisfacción de los ejecutivos de la universidad con la capacidad de respuesta de la TI a nuevos requerimientos - Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
Metas del proceso:	
1 El valor de empresa es creado mediante la cualificación y puesta en escena de los avances e innovaciones tecnológicas más apropiadas, los métodos y las soluciones TI utilizadas.	- Percepciones de las partes interesadas y realimentación sobre la innovación en TI
2 Los objetivos de la empresa se cumplen por la mejora de los beneficios de la calidad y/o la reducción de costes como resultado de la identificación e implementación de soluciones innovadoras.	- Porcentaje de las iniciativas implementadas que dieron los beneficios previstos - Porcentaje de las iniciativas implementadas con un vínculo claro a los objetivos de la empresa
3 La innovación se permite y se promueve y forma parte de la cultura de la empresa.	- Opinión y encuestas de las partes interesadas

Prácticas de Gestión

APO04.01 Crear un entorno favorable para la innovación
Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados.

Iniciativas y/o Documentos E/S

Entrada:	Salida: - Plan de innovación - Programa de reconocimiento y recompensa

Actividades
1. Crear un plan de innovación que incluya el apetito por el riesgo, el presupuesto previsto para invertir en la innovación y los objetivos de la innovación.
2. Proveer de una infraestructura que pueda permitir innovar, tales como herramientas de colaboración para mejorar el trabajo entre diferentes ubicaciones geográficas y divisiones de la empresa.
3. Crear un entorno que fomente la innovación manteniendo iniciativas de recursos humanos relevantes, tales como el reconocimiento de la innovación y programas de reconocimiento, una rotación apropiada en los puestos de trabajo y tiempo prudencial para la experimentación.
4. Mantener un programa que permita a los empleados presentar ideas innovadoras y crear una estructura adecuada de toma de decisiones para evaluar y aplicar estas ideas.
5. Animar a innovar a los clientes, proveedores y socios comerciales.

APO04.02 Mantener un entendimiento del entorno de la empresa
Trabajar junto a las partes interesadas para entender sus retos. Mantener un entendimiento adecuado de la estrategia corporativa y del entorno competitivo, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.

Iniciativas y/o Documentos E/S

Entrada: - Estrategia corporativa	**Salida**:

- Análisis FODA de la empresa	- Oportunidades de innovación vinculadas a los motivadores del negocio

Actividades:

1. Mantener una comprensión de los motores del negocio y de la industria, de la estrategia corporativa, operaciones corporativas y otras incidencias de modo que los potenciales valores añadidos tecnológicos o innovaciones TI puedan ser identificadas.
2. Realizar reuniones periódicas con las unidades de negocio, divisiones y/o otras entidades interesadas para entender los problemas actuales del negocio, cuellos de botella de los procesos u otras limitaciones donde las tecnologías emergentes o la innovación TI puede crear oportunidades.
3. Entender los parámetros de inversiones corporativas para la innovación y las nuevas tecnologías, de modo que se desarrollen las estrategias adecuadas.

APO04.03 Supervisar y explorar el entorno tecnológico

Realizar una supervisión sistemática y un escaneo del entorno externo a la empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, realizando la estrategia corporativa, optimizando costes, evitando la obsolescencia y catalizando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias que permitan analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial.

Iniciativas y/o Documentos E/S

Entrada: - Tecnologías emergentes	Salida: - Análisis de investigación de las posibilidades de investigación

Actividades

1. Comprender el interés de la empresa y su potencial para adoptar nuevas innovaciones tecnológicas canalizando los esfuerzos de concienciación en las innovaciones tecnológicas más oportunas.
2. Realizar estudios y analizar el entorno exterior, incluyendo sitios web apropiados, diarios y conferencias para identificar tecnologías emergentes.
3. Consultar con terceras personas expertas cuando se necesite confirmar los resultados de la investigación o como fuente de información en tecnologías emergentes.
4. Recopilar las ideas innovadoras del personal de TI y analizarlas para su posible implementación.

APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras

Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de las nuevas tecnologías y la innovación.

Iniciativas y/o Documentos E/S

Entrada	**Salida** - Evaluación de las ideas de innovación - Pruebas de concepto y descripción de los casos de negocio - Resultados de las pruebas de concepto

Actividades

1. Evaluar las tecnologías identificadas, considerando aspectos tales como tiempo para alcanzar la madurez, riesgo inherente de la nueva tecnología (incluyendo posibles implicaciones legales), ajuste con la arquitectura empresarial y potencial para proporcionar valor añadido.
2. Identificar cualquier problema que pueda necesitar ser resuelto o probado a través de una iniciativa de prueba de concepto.
3. Alcance de la iniciativa de prueba de concepto, incluyendo resultados deseados, presupuesto necesario, plazos de tiempo y responsabilidades.
4. Obtener autorización para realizar la prueba de concepto.
5. Realizar pruebas de concepto para evaluar las tecnologías emergentes u otras ideas innovadoras, identificar cualquier problema y determinar si más implementaciones deberían ser tenidas en cuenta, basándose en la viabilidad y el potencial retorno de la inversión (ROI).

APO04.05 Recomendar iniciativas apropiadas adicionales

Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas.

Iniciativas y/o Documentos E/S

Entrada	**Salida** - Resultados de las pruebas de concepto - Análisis de las iniciativas rechazadas

Actividades

1. Documentar los resultados de las pruebas de concepto, incluyendo guía y recomendaciones para programas de innovación y tendencias.
2. Comunicar las oportunidades de innovación viables en la estrategia TI y en los procesos de arquitectura empresarial.
3. Realizar un seguimiento de las pruebas de concepto para medir el grado en que las mismas han influenciado en las inversiones reales.
4. Analizar y comunicar las razones por las que se ha rechazado una prueba de concepto.

APO04.06 Supervisar la implementación y el uso de la innovación

Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas.

Iniciativas y/o Documentos E/S	
Entrada	**Salida** - Evaluación de los beneficios de la innovación - Planes de innovación ajustados
Actividades 1. Valorar la implementación de nuevas tecnologías o innovaciones TI adoptadas como parte de la estrategia TI y desarrollos de la arquitectura empresarial y su realización durante programas de gestión de iniciativas. 2. Capturar lecciones aprendidas y oportunidades de mejora. 3. Ajustar el plan de innovación, si fuese necesario. 4. Identificar y evaluar el posible valor obtenido como fruto del uso de la innovación.	

APO07: Gestionar los Recursos Humanos	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción: Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	
Propósito: Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Gerente General - Vicerrector - Decanos - Director PROESAD - Director EPG
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa	
Metas de TI relacionadas:	
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
13 Entrega de programas que proporcionan beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	- Número de programas/proyectos ejecutados en plazo y en presupuesto - Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
16 Personal del negocio y de las TI competente y motivado	- Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función - Porcentaje del personal satisfecho con su función TI
Metas del proceso:	
1 La estructura organizacional y las relaciones de TI son flexibles y respuesta ágil	- Número de definiciones de servicio y catálogos de servicio - Nivel de satisfacción de los ejecutivos con la toma de decisiones de la gerencia
2 Los recursos humanos son gestionados eficaz y eficientemente	- Porcentaje de rotación del personal - Duración media de las vacantes - Porcentaje de puestos de TI vacantes
Prácticas de Gestión	

APO07.01 Mantener la dotación de personal suficiente y adecuada

Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Principios para la asignación de recursos y capacidades - Definición de las prácticas de supervisión - Políticas empresariales y procedimientos de RRHH	- Evaluaciones de requisitos de personal - Planes de desarrollo de carrera y de competencias - Planes de aprovisionamiento de personal

Actividades:

1. Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar que:
   - La función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos empresariales.
   - La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI.
2. Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa.
3. Incluir controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores. El alcance y la frecuencia de estos controles depende de la sensibilidad y/o criticidad de la función.
4. Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias, contratistas externos y acuerdos de servicio con terceras partes.
5. Asegurarse de que el entrenamiento cruzado se lleva a cabo y que hay respaldo para el personal clave para reducir la dependencia de una sola persona.

APO07.02 Identificar personal clave de TI

Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (*backup*) del personal.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
-	-

Actividades:

1. Minimizar la dependencia en una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión, el respaldo (*backup*) del personal, el entrenamiento cruzado e iniciativas de rotación de puestos.
2. Como medida de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que deben tomar los individuos clave.
3. Tomar acciones expeditivas con respecto a cambios laborales, especialmente despidos.
4. Probar regularmente los planes de respaldo (*backup*) del personal.

APO07.03 Mantener las actividades y competencias del personal

Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Concienciación del conocimiento y esquemas de formación - Seguimiento de resultados en habilidades y competencias - Requisitos de formación - Metas y objetivos de la empresa	- Matriz de habilidades y competencias - Planes de desarrollo de habilidades

Actividades

1. Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos.
2. Proporcionar una planificación formal de la carrera y desarrollo profesional para fomentar el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave.
3. Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias.
4. Identificar las diferencias entre las habilidades necesarias y las disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva, tales como formación (técnica y en habilidades de comportamiento), contratación, redistribución y cambios en las estrategias de contratación.
5. Desarrollar y ejecutar programas de formación basados en los requisitos organizativos y de procesos, incluidos los requisitos sobre conocimiento empresarial, control interno, conducta ética y seguridad.
6. Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Revisar la planificación de la sucesión.

7. Revisar los materiales y programas de formación de manera regular para asegurarse su adecuación a los requisitos empresariales cambiantes y su impacto en los conocimientos, aptitudes y habilidades necesarias.

APO07.04 Evaluar el desempeño laboral de los empleados

Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Objetivos de desempeño de RRHH alineados - Resultados de la revisión de desempeño de los RRHH - Derechos de acceso asignados - Metas y objetivos empresariales	- Metas personales - Evaluaciones de desempeño - Planes de mejora

Actividades

1. Considerar los objetivos funcionales/de empresa como el contexto para establecer las metas individuales.
2. Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales. Basar las metas en objetivos SMART (específicos, medibles, realizables, pertinentes y de duración determinada) que reflejen las competencias básicas, los valores empresariales y las habilidades necesarias para la(s) función(es).
3. Recopilar los resultados de la evaluación de desempeño de 360 grados.
4. Implementar y comunicar un proceso disciplinario.
5. Proporcionar instrucciones específicas para el uso y almacenamiento de información personal en el proceso de evaluación, de conformidad con la legislación laboral y sobre datos personales aplicables
6. Proporcionar retroalimentación oportuna sobre el desempeño frente a las metas del individuo.
7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, el desarrollo de competencias y el logro exitoso de los objetivos de desempeño. Asegurar que el proceso se aplica de forma coherente y en consonancia con las políticas de la organización.
8. Desarrollar planes de mejora del desempeño basados en los resultados del proceso de evaluación y los requisitos de capacitación y desarrollo de competencias identificados.

APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio

Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Requisitos y funciones de recursos - Requisitos de recursos de proyectos - Carteras actuales y futuras - Estructura organizativa de la empresa	- Inventario de recursos humanos del negocio y de TI - Registros de utilización de recursos

Actividades

1. Crear y mantener un inventario de recursos humanos de negocio y TI.
2. Entender la demanda actual y futura de recursos humanos para apoyar el logro de los objetivos de TI y ofrecer servicios y soluciones basados en la cartera de las iniciativas actuales relacionadas con las TI, la cartera de inversiones futuras y las necesidades operativas del día a día.
3. Identificar las carencias y proporcionar datos de entrada a planes de aprovisionamiento, así como a los procesos de contratación de la empresa y de TI. Crear y revisar el plan de personal, haciendo seguimiento del uso real.
4. Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos.

APO07.06 Gestionar el personal contratado

Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización, así como los requisitos contractuales previamente acordados.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Requisitos y funciones de recursos - Requisitos de recursos de proyectos - Comunicación del retiro del programa y responsabilidades en curso	- Políticas de contratación del personal - Acuerdos contractuales

Actividades

1. Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización y el marco de control de TI.
2. Obtener un acuerdo formal por parte de los contratistas en el inicio del contrato en cuanto a que están obligados a cumplir con el marco de control de TI de la empresa, tal como políticas de control de seguridad, control de acceso físico y lógico, uso de las instalaciones, requisitos de confidencialidad de la información y los acuerdos de confidencialidad.
3. Advertir a los contratistas de que la gerencia se reserva el derecho de supervisar e inspeccionar todo uso de los recursos de TI, incluyendo correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.

4. Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades como parte de sus contratos, incluidos requisitos explícitos para documentar su trabajo en base a normas y formatos previamente acordados. 5. Revisar el trabajo de los contratistas y basar la aprobación de los pagos en los resultados. 6. Definir todo el trabajo a realizar por terceras partes en contratos formales y sin ambigüedades. 7. Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios. 8. Llevar a cabo revisiones periódicas para asegurarse de que las funciones de los contratistas y sus derechos de acceso son adecuados y en línea con los acuerdos.

APO10: Gestionar los Proveedores	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción: Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.	
Propósito: Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Gerente General - Gerente Financiero - Proveedores
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
09 Agilidad de las TI	- Nivel de satisfacción de los ejecutivos de la universidad con la capacidad de respuesta de la TI a nuevos requerimientos - Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas
Metas del proceso:	
1 Los proveedores rinden según lo acordado	- Porcentaje de proveedores que cumplen con los requisitos acordados
2 El riesgo de los proveedores se evalúa y trata adecuadamente	- Número de eventos de riesgo que conducen a incidentes del servicio - Frecuencia de las reuniones con suministradores sobre la gestión de riesgos

	- Porcentaje de los incidentes relacionados con el riesgo resueltos adecuadamente (en tiempo y coste)
3 Las relaciones con los proveedores son eficaces	- Numero de reuniones de revisión con proveedores - Número de disputas formales con proveedores - Porcentaje de disputas con proveedores resueltas adecuadamente y en un tiempo razonable

Prácticas de Gestión

APO10.01 Identificar y evaluar las relaciones y contratos con los proveedores

Identificar proveedores y contratos asociados y categorizarlos por tipo, relevancia y criticidad. Establecer un criterio de evaluación de contratos y proveedores y evaluar la cartera general de proveedores y contratos actuales y alternativos.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Contratos con los proveedores	- Catálogo de proveedores - Criterios de evaluación - Revisiones potenciales de los contratos con los proveedores

Actividades:

1. Establecer y mantener criterios relativo al tipo, relevancia y criticidad de los contratos y proveedores, focalizándose en aquellos de mayor importancia.
2. Establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente.
3. Identificar, registrar y categorizar los proveedores y contratos existentes de acuerdo al criterio definido para mantener un registro detallado de los proveedores que deben ser gestionados cuidadosamente.
4. Evaluar y comparar periódicamente el rendimiento de los proveedores actuales y alternativos para identificar oportunidades de mejora o la necesidad forzosa de reconsiderar los contratos con los proveedores actuales.

APO10.02 Seleccionar proveedores

Seleccionar proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos. Los requisitos deberían estar optimizados con las aportaciones de nuevos proveedores potenciales

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Plan de adquisiciones	- Solicitudes de información y peticiones de propuestas a proveedores - Evaluación de solicitudes y peticiones - Resultados de las evaluaciones

Actividades:

1. Revisar todas las RFIs y RFPs para asegurar que:
   - Definen claramente los requisitos.
   - Incluyen un procedimiento para clarificar los requisitos.
   - Dan a los proveedores tiempo suficiente para elaborar sus propuestas.
   - Definen claramente los criterios y el proceso de decisión.
2. Evaluar RFIs y RFPs de acuerdo al proceso y criterios aprobados y mantener evidencia documental de las evaluaciones. Verificar las referencias de los proveedores candidatos.
3. Seleccionar el proveedor que mejor cumpla la RFP. Documentar y comunicar la decisión alcanzada y firmar el contrato.
4. En el caso específico de la adquisición de software, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir la propiedad y el licenciamiento de la propiedad intelectual, el mantenimiento, las garantías, los procesos de arbitraje, las condiciones de actualización y la aptitud para el propósito definido, incluyendo seguridad, depósito de garantía y derechos de acceso.
5. En el caso específico de la adquisición de desarrollos, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir la propiedad y el licenciamiento de la propiedad intelectual; aptitud para el propósito definido, incluyendo metodologías, pruebas, procesos de gestión de la calidad, incluyendo los criterios de evaluación del rendimiento, formas de pago, garantías, los procesos de arbitraje, gestión de recursos humanos y cumplimiento con las políticas corporativas.
6. Obtener asesoramiento legal sobre los acuerdos de adquisición de desarrollos en relación a la propiedad y el licenciamiento de propiedad intelectual.
7. En el caso específico de la adquisición de infraestructuras, instalaciones y servicios relacionados, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir niveles de servicio, procedimientos de mantenimiento, controles de acceso, seguridad, revisiones de rendimiento, formas de pago y procesos de arbitraje.

APO10.03 Gestionar contratos y relaciones con proveedores

Formalizar y gestionar las relaciones con cada proveedor. Gestionar, mantener y supervisar los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, las leyes y las regulaciones. Gestionar los conflictos contractuales.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Planes de adquisiciones aprobados	- Roles y responsabilidades de proveedores

	- Procesos de revisión y comunicación - Resultados y sugerencia de mejora

Actividades

1. Asignar propietarios de las relaciones para cada proveedor y hacerles responsables de la calidad del servicio proporcionado.
2. Especificar un proceso de comunicación formal y de revisión, que incluyan las interacciones con el proveedor y la planificación.
3. Acordar, gestionar, mantener y renovar los contratos con los proveedores. Asegurar que los contratos son conformes con las normas corporativas y con los requisitos legales y regulatorios.
4. Incluir en los contratos con los proveedores de servicios clave disposiciones para revisar los lugares de trabajo y las prácticas y controles de la dirección o de terceras partes.
5. Evaluar la eficiencia de la relación con los proveedores e identificar las mejoras necesarias.
6. Definir, comunicar y acordar las maneras de implementar las mejoras requeridas en las relaciones.
7. Hacer uso de los procedimientos establecidos para tratar los conflictos contractuales haciendo uso primero, siempre que sea posible, de relaciones y mecanismos de comunicación eficaces que permitan superar los problemas de servicio.
8. Definir y formalizar los roles y responsabilidades de cada proveedor. Cuando varios proveedores se combinan para proporcionar un servicio, considerar asignar un rol de proveedor líder a uno de los proveedores para que asuma la responsabilidad global del contrato.

APO10.04 Gestionar el riesgo en la capacidad de los proveedores

Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Análisis de riesgos e informes de perfil de riesgos para las partes interesadas	- Identificar el riesgo de entrega del proveedor - Requisitos contractuales para minimizar el riesgo

Actividades

1. Identificar, supervisar y, cuando sea apropiado, gestionar los riesgos relacionados con la capacidad del proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua.
2. A la hora de definir el contrato, para los riesgos potenciales, incluir una descripción clara de todos los requisitos de servicio, incluyendo depósitos de garantía, proveedores alternativos o acuerdos en suspenso para mitigar el riesgo de un posible fallo del proveedor; los aspectos de seguridad, la propiedad intelectual y los requisitos legales y regulatorios.

APO10.05 Supervisar el cumplimiento y rendimiento del proveedor

Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y el valor de lo pagado y tratar las incidencias identificadas.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Criterios de supervisión del cumplimiento de los proveedores - Resultados de las revisiones de la supervisión del cumplimiento de los proveedores

Actividades

1. Definir y documentar los criterios para supervisar el rendimiento de los proveedores alineado con los acuerdos de nivel de servicio y asegurando que el proveedor informa según estos criterios de forma regular y transparente.
2. Supervisar y revisar la entrega de servicios para asegurar que el proveedor está proporcionando una calidad del servicio adecuada, cumpliendo los requisitos y las condiciones de los contratos.
3. Revisar el rendimiento y el coste de los proveedores para asegurar que son competitivos y fiables, en comparación con proveedores alternativos y condiciones de mercado.
4. Solicitar revisiones independientes de las prácticas internas y los controles, si se considera necesario.
5. Registrar y evaluar los resultados de la revisión periódica y discutirlos con el proveedor para identificar las necesidades y oportunidades de mejora.
6. Supervisar y evaluar la información externa disponible sobre el proveedor.

APO12: Gestionar el riesgo	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Propósito: Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Decanos - Director PROESAD - Director EPG - Estudiantes de pregrado - Estudiantes de posgrado

	- Docentes - Personal administrativo
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI.
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
10 Seguridad de la información, infraestructura y aplicaciones	- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública - Número de servicios de TI con los requisitos de seguridad pendientes - Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados
13 Entrega de programas que proporcionan beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	- Número de programas/proyectos ejecutados en plazo y en presupuesto - Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
Metas del proceso:	
1 Es riesgo relacionado con TI está identificado, analizado, gestionado y reportado	- Número de eventos de pérdida con características clave, capturados en repositorios - Porcentaje de auditorías, eventos y tendencias capturados en - repositorios
2 Existe un perfil de riesgo actual y completo	- Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo - Completitud de atributos y valores en el perfil de riesgo
3 Todas las acciones de gestión para los riesgos significativos están gestionados	- Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado - Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos
4 Las acciones de gestión de riesgos están efectivamente implementadas	- Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados - Número de medidas que no reducen el riesgo residual
Prácticas de Gestión	
APO12.01 Recopilar datos Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	
Iniciativas y/o Documentos E/S	
Entrada: - Evaluaciones de actividades de gestión de riesgos - Procesos para medir la gestión de riesgos - Políticas de gestión de riesgos - Evaluaciones del riesgo	Salida: - Datos en el entorno de operación relacionados con el riesgo - Datos de eventos de riesgo - Elementos y factores de riesgo emergentes

- Estado de incidentes e informe de tendencias	

Actividades:
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.
3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.
4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.
5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.
6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.
7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

APO12.02 Analizar el riesgo
Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Análisis de impacto en el negocio - Evaluaciones de amenazas potenciales	- Escenarios de riesgo de TI - Resultados de análisis de riesgos

Actividades:
1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.
2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.
3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.
5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.
6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.
7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.

APO12.03 Mantener un perfil de riesgo
Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Niveles de tolerancia al riesgo aprobado - Riesgo de entrega de proveedores - Evaluaciones de amenazas potenciales	- Escenarios de riesgos documentados - Perfil de riesgo, con las acciones de gestión de riesgo

Actividades
1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.
2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.
5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.

6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.
7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.

APO12.04 Expresar el riesgo
Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Análisis de riesgos - Informes de perfil de riesgos para las partes interesadas

Actividades
1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.
2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.
3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.
4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.
5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.

APO12.05 Definir un portafolio de acciones para la gestión de riesgos
Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Propuestas de proyectos para reducir el riesgo

Actividades
1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.
2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.
3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.

APO12.06 Responder al riesgo
Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Acciones correctoras para tratar las desviaciones de gestión de riesgos	- Planes de respuesta para incidentes relacionados con riesgos - Comunicaciones del impacto del riesgo - Causa raíz relacionadas con el riesgos

Actividades
1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.

APO13: Gestionar la seguridad	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información	
Propósito:	

Mantener el impacto y la ocurrencia de los incidentes de la seguridad de la información dentro de los niveles del apetito de riesgo de la empresa	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Rectos - Vicerrector - Gerente General - Director de Bienestar Universitario
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI.
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
10 Seguridad de la información, infraestructura y aplicaciones	- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública - Número de servicios de TI con los requisitos de seguridad pendientes - Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados
14 Disponibilidad de información útil y relevante para la toma de decisiones	- Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión - Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información
Metas del proceso:	
1 Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	- Número de roles de seguridad claves claramente definidos - Número de incidentes relacionados con la seguridad
2 Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	- Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa - Número de soluciones de seguridad que se desvían del plan
3 Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	- Número de incidentes de seguridad causados por la no observancia del plan de seguridad - Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad
Prácticas de Gestión	
APO13.01 Establecer y mantener un SGSI Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	
Iniciativas y/o Documentos E/S	

Entrada:	Salida:
- Enfoque de seguridad de la empresa	- Política del SGSI - Alcance del SGSI

Actividades:

1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
7. Comunicar el enfoque de SGSI

APO13.02 Definir y gestionar un plan de tratamiento del riesgo

Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Análisis y evaluación de riesgos - Descripción de la arquitectura empresarial - Propuestas de proyectos para reducir el riesgo	- Plan de tratamiento de riesgos de seguridad de la información - Casos de negocio de seguridad de información

Actividades:

1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.
6. Recomendar programas de formación y concienciación en seguridad de la información.
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.

APO13.03 Supervisar y revisar el SGSI

Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Niveles de tolerancia al riesgo aprobado - Riesgo de entrega de proveedores - Evaluaciones de amenazas potenciales	- Escenarios de riesgos documentados - Perfil de riesgo, con las acciones de gestión de riesgo

Actividades

1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.
2. Realizar auditorías internas al SGSI a intervalos planificados.
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.

BAI04: Gestionar la disponibilidad y la capacidad	**Área: Gestión** **Dominio: Construir, Adquirir e Implantar**

Descripción: Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.	
Propósito: Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Decanos - Director PROESAD - Director EPG - Estudiantes de pregrado - Estudiantes de posgrado - Docentes - Personal administrativo - Padres de familia
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
14 Disponibilidad de información útil y relevante para la toma de decisiones	- Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión - Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información
Metas del proceso:	
1 El plan de disponibilidad anticipa la expectativa del negocio en cuanto a requerimientos críticos de capacidad	- Número de actualizaciones de capacidad, rendimiento o disponibilidad no planificada.
2 Cumplimiento de requerimiento de capacidad, rendimiento y disponibilidad	- Número de incidentes de disponibilidad - Número de eventos donde la capacidad ha excedido los límites planificados
3 Cuestiones de disponibilidad, rendimiento y capacidad identificados y resueltos de manera rutinaria	- Número y porcentaje de cuestiones de disponibilidad, rendimiento y capacidad no resueltos
Prácticas de Gestión	
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia	

Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los ANSs. Crear líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Registro de definiciones de requisitos - Registro de requisitos de riesgo	- Líneas de referencia de disponibilidad, rendimiento y capacidad - Evaluaciones respecto a los SLA

Actividades:

1. Considerar en la evaluación (actual o prevista) de disponibilidad, rendimiento y capacidad de servicios y recursos lo siguiente: Requisitos del cliente, prioridades de negocio, objetivos de negocio, impacto en el presupuesto, utilización de recursos, capacidades de TI y tendencias de la industria.
2. Supervisar el rendimiento y la utilización de la capacidad reales frente a los umbrales definidos, con el apoyo cuando sea necesario de software automatizado.
3. Identificar y dar seguimiento a todos los incidentes causados por un rendimiento o una capacidad inadecuados.
4. Evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento (la demanda del negocio, capacidad de servicio y capacidad de los recursos) mediante la comparación con las tendencias y los ANSs, teniendo en cuenta los cambios en el entorno.

BAI04.02 Evaluar el impacto en el negocio

Identificar los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias del negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- SLA internos y externos	- Escenarios de disponibilidad, rendimiento y capacidad - Evaluaciones de impacto en el negocio de disponibilidad, rendimiento y capacidad

Actividades:

1. Identificar solamente aquellas soluciones o servicios que son críticas para los procesos de gestión de la disponibilidad y la capacidad.
2. Realizar un mapa de las soluciones o servicios seleccionados con la(s) aplicación(es) e infraestructura (TI y de instalaciones) de los que dependen, para permitir un enfoque en los recursos críticos para la planificación de la disponibilidad.
3. Recolectar datos de patrones de disponibilidad de los registros de fallos pasados y de la monitorización del rendimiento. Utilizar herramientas de modelado que ayuden a predecir fallos basados en tendencias de utilización en el pasado y expectativas de la dirección sobre nuevos entornos o condiciones de los usuarios.
4. Crear escenarios basados en datos recolectados, describiendo situaciones de disponibilidad futura para ilustrar varios niveles de capacidad potenciales necesarios para alcanzar el objetivo de rendimiento de la disponibilidad.
5. Determinar la probabilidad de que el objetivo del rendimiento de la disponibilidad no será alcanzado basado en los escenarios.
6. Determinar el impacto de los escenarios en las medidas de rendimiento del negocio (ej. Ingresos, beneficios, servicios a clientes). Involucrar a la línea de negocio, líderes funcionales (especialmente finanzas) y regionales para comprender su evaluación de impacto.
7. Asegurar que los propietarios de procesos de negocio comprenden completamente y están de acuerdo con los resultados del análisis. Obtener una lista de escenarios de riesgo inaceptables de los propietarios de negocio que requieran una respuesta para reducir el riesgo a niveles aceptables.

BAI04.03 Planificar requisitos de servicios nuevos o modificados

Planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Especificaciones de diseño aprobados - Componentes de la solución documentados	- Planes de capacidad y rendimiento

Actividades

1. Revisar las implicaciones en la disponibilidad y la capacidad del análisis de tendencias del servicio.
2. Identificar las implicaciones en la disponibilidad y la capacidad de cambios en las necesidades del negocio y oportunidades de mejora. Utilizar técnicas de modelado para validar los planes de disponibilidad, rendimiento y capacidad.
3. Priorizar las necesidades de mejora y crear planes de disponibilidad y capacidad justificables en costes.
4. Ajustar los planes de rendimiento y capacidad y los ANSs sobre la base de los procesos de negocio y servicios que los soportan realistas, nuevos, propuestos o proyectados, sobre cambios a las aplicaciones y la infraestructura, así como revisiones del rendimiento y uso de la capacidad actual, incluyendo niveles de carga de trabajo.
5. Asegurar que la dirección lleva a cabo comparaciones de la demanda actual de recursos con la demanda y suministro previstos para evaluar las técnicas de previsión actuales y realizar mejoras donde sea posible.

BAI04.04 Supervisar y revisar la disponibilidad y la capacidad

Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a las líneas de referencia establecidas. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Informes de disponibilidad y rendimiento

Actividades

1. Establecer un proceso de recolección de datos para proporcionar a la dirección información de seguimiento e informes de la carga de trabajo de disponibilidad, rendimiento y capacidad de todos los recursos relacionados con la información.
2. Proporcionar información periódica de los resultados en una forma apropiada para su revisión por las TI y la gestión del negocio y comunicar a la dirección empresarial.
3. Integrar las actividades de supervisión e información en las actividades iterativas de gestión de la capacidad supervisión, análisis, ajuste e implementaciones).
4. Proveer informes de capacidad para los procesos de presupuesto.

BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad

Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Brechas de rendimiento y capacidad - Acciones correctivas

Actividades

1. Obtener la orientación de manuales de productos de proveedores para garantizar un nivel adecuado de rendimiento de disponibilidad para picos de procesamiento y cargas de trabajo.
2. Identificar brechas de rendimiento y capacidad sobre la base de la monitorización del rendimiento actual y previsto. Utilizar las especificaciones de disponibilidad, continuidad y recuperación conocidas para clasificar los recursos y permitir la priorización.
3. Definir acciones correctivas (ej. cambiando la carga de trabajo, dando prioridad a las tareas o la adición de recursos, cuando se identifican los problemas de rendimiento y capacidad).
4. Integrar las acciones correctivas requeridas dentro de los procesos apropiados de planificación y gestión de cambios.
5. Definir un procedimiento de escalado para la resolución rápida en emergencias en caso de problemas de capacidad y rendimiento.

BAI06: Gestionar los cambios	**Área: Gestión** **Dominio: Construir, Adquirir e Implantar**

Descripción:

Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

Propósito:

Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.

Dueño del proceso:	**Partes interesadas:**
Mesa de ayuda	- Gerente General - Vicerrector - Director de Bienestar Universitario

Metas corporativas relacionadas:

03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes
08 Contar con docentes capacitados y especializados
10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
11 Incrementar los investigadores activos en redes de investigación
12 Desarrollar capacidades en investigación
13 Ampliar la disponibilidad y uso de biblioteca virtual
16 Desarrollar competencias para proyectos y programas
19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares
20 Alcanzar la excelencia en el desarrollo de las sesiones de clase
21 Consolidar la atención en tutorías
22 Alcanzar la efectividad de la gestión de prácticas pre profesionales
23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
24 Lograr la eficacia de los procesos de investigación científica
25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza
26 Alcanzar participación activa en proyectos según líneas de investigación

27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
10 Seguridad de la información, infraestructura y aplicaciones	- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública - Número de servicios de TI con los requisitos de seguridad pendientes - Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados
Metas del proceso:	
1 Los cambios autorizados son realizados de acuerdo al cronograma y con errores mínimos	- Cantidad de trabajo rehecho debido a cambios fallidos - Reducción en el tiempo y esfuerzo necesarios para aplicar los cambios - Número y antigüedad de peticiones de cambio en cartera
2 Las evaluaciones de impacto revelen el efecto de los cambios sobre todos los componentes afectados	- Porcentaje de cambios sin éxito debidos a evaluaciones de impacto inadecuadas
3 Todos los cambios de emergencia son revisados y autorizados una vez hecho el cambio	- Porcentaje sobre el total de cambios que corresponde a cambios de emergencia - Número de cambios de emergencia no autorizados una vez hecho el cambio
4 Las principales partes interesadas están informadas sobre todos los aspectos del cambio	- Ratios de satisfacción de las partes interesadas con las comunicaciones de los cambios
Prácticas de Gestión	
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.	
Iniciativas y/o Documentos E/S	
Entrada: - Componentes de la soluciones integrados y configurados - Peticiones de servicio aprobadas - Soluciones sostenibles identificadas - Cambios aprobados a los planes - Análisis de causa raíz y recomendaciones	Salida: - Evaluaciones de impacto - Peticiones de cambio aprobadas - Plan de cambio y cronograma
Actividades: 1. Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio. 2. Categorizar todas las peticiones de cambio (ej. procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software externo adquirido) y relacionarlas con los elementos de configuración afectados. 3. Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio. 4. Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados. Evaluar la probabilidad de que afecten negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, legales, contractuales, y de cumplimiento normativo del cambio solicitado. Considerar además todas las inter-dependencias entre cambios. Involucrar a los propietarios de procesos de negocio en el proceso de evaluación, de forma apropiada.	

5. Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
6. Planificar y programar todos los cambios aprobados.
7. Considerar el impacto en los proveedores de servicios contratados (ej. procesamiento de negocio externalizado, infraestructuras, desarrollo de aplicaciones y servicios compartidos) en el proceso de gestión del cambio, incluyendo la integración de la gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y ANSs.

BAI06.02 Gestionar cambios de emergencia

Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- SLA internos y externos	- Revisión de cambios de emergencia tras su implementación

Actividades:

1. Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
2. Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.
3. Supervisar todos los cambios de emergencia y realizar revisiones post-implantación involucrando a todas las partes interesadas. La revisión debería considerar e iniciar acciones correctivas basadas en causas raíz tales como problemas en los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales e integridad de datos.
4. Definir qué constituye un cambio de emergencia.

BAI06.03 Hacer seguimiento en informar de cambios de estado

Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Registro de peticiones de cambio aprobadas	- Reporte del estado de cambio de una petición

Actividades

1. Categorizar las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados, pero aún no iniciados, aprobados y en proceso y cerrados).
2. Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.
3. Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.
4. Mantener un sistema de seguimiento e informe para todas las peticiones de cambio.

BAI06.04 Cerrar y documentar los cambios

Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Documentación del cambio

Actividades

1. Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio como parte integral del cambio.
2. Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación de usuario.
3. Someter a la documentación a la misma revisión que al cambio en sí mismo.

BAI10: Gestionar la configuración	**Área: Gestión** **Dominio: Construir, Adquirir e Implantar**

Descripción:

Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

Propósito:

Proporcionar suficiente información sobre los activos del servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Decanos - Director PROESAD - Director EPG - Estudiantes de pregrado - Estudiantes de posgrado - Docentes - Personal administrativo - Padres de familia
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI.
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
14 Disponibilidad de información útil y relevante para la toma de decisiones	- Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión - Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información
Metas del proceso:	
1 El repositorio de configuración es correcto, completo y está actualizado	- Número de desviaciones ente el repositorio de configuración y la configuración real. - Número de discrepancias relativas a información de configuración incompleta o inexistente.
Prácticas de Gestión	
BAI10.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia Establecer y mantener un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, configuration items) y las relaciones entre ellos. Incluyendo los CIs considerados necesarios para gestionar eficazmente los servicios y proporcionar una sola descripción fiable de los activos en un servicio.	
Iniciativas y/o Documentos E/S	
Entrada: - Plan de lanzamiento	Salida: - Ámbito de aplicación del modelo de gestión de la configuración - Modelo de configuración lógica
Actividades: 1. Definir y acordar el alcance y nivel de detalle para la gestión de la configuración (p.ej., qué servicios, activos y elementos configurables de la infraestructura se incluyen). 2. Establecer y mantener un modelo lógico para la gestión de la configuración, incluyendo información sobre los tipos de elementos de configuración, atributos de los elementos de configuración, tipos de relaciones, atributos de relación y códigos de estado.	

BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia
Establecer y mantener un repositorio de gestión de la configuración y crear unas bases de referencia de configuración controladas.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Registro de licencias de software	- Repositorio de configuración - Base de referencia de configuración

Actividades:
1. Identificar y clasificar los elementos de configuración y rellenar el repositorio.
2. Crear, revisar y formalizar un acuerdo sobre las bases de referencia de configuración de un servicio, aplicación o infraestructura.

BAI10.03 Mantener y controlar los elementos de configuración
Mantener un repositorio actualizado de elementos de configuración rellenado con los cambios.

Iniciativas y/o Documentos E/S

Entrada:	
- Informes de estado de solicitudes de cambio - Resultados de los controles físicos de inventario - Registro de activos - Retirada autorizada de activos	Salida: - Repositorio actualizado con los elementos de configuración - Cambios aprobados a la base de referencia

Actividades
1. Identificar regularmente todos los cambios en los elementos de configuración.
2. Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.
3. Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.
4. Crear, revisar y formalizar acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.

BAI10.04 Generar informes de estado y configuración
Definir y elaborar informes de configuración sobre cambios en el estado de los elementos de configuración.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Resultados de controles físicos de inventario	- Informes de estado de configuración

Actividades
1. Identificar cambios en el estado de los elementos de configuración y contrastarlo con la base de referencia.
2. Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.
3. Identificar requisitos de información de todas las partes interesadas, incluyendo contenido, frecuencia y medios. Generar informes según las necesidades identificadas.

BAI10.05 Verificar y revisar la integridad del repositorio de configuración
Revisar periódicamente el repositorio de configuración y verificar la integridad y exactitud con respecto al objetivo deseado.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Resultados de la verificación física de elementos de configuración - Resultados de exámenes de completitud del repositorio

Actividades
1. Verificar periódicamente los elementos de configuración en activo contra el repositorio de configuración comparando configuraciones físicas y lógicas, usando las herramientas apropiadas de descubrimiento, según sea necesario.
2. Informar y revisar todas las desviaciones de las correcciones o acciones aprobadas para eliminar los activos no autorizados.
3. Verificar periódicamente que todos los elementos físicos de configuración, tal como se definen en el repositorio, existen físicamente. Informar de cualquier desviación a la Dirección.
4. Establecer y revisar periódicamente el objetivo de completitud del repositorio de configuración basado en las necesidades del negocio.
5. Periódicamente comparar el grado de completitud y precisión respecto a los objetivos y tomar medidas correctivas, según sea necesario, para mejorar la calidad de los datos del repositorio.

DSS01: Gestionar las operaciones	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
Descripción: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	
Propósito: Entregar los resultados del servicio operativo de TI, según lo planificado.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Decanos

	- Director PROESAD - Director EPG - Estudiantes de pregrado - Estudiantes de posgrado - Docentes - Personal administrativo
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
Metas del proceso:	
1 Las actividades operativas se realizan según lo requerido y programado	- Número de procedimientos operativos no estándar ejecutados - Número de incidentes causados por problemas operativos
2 Las operaciones son monitorizadas, medidas, reportadas y remediadas	- Tasa de eventos comparada con el número de incidentes - Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática
Prácticas de Gestión	
DSS01.01 Ejecutar procedimientos operativos Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	
Iniciativas y/o Documentos E/S	
Entrada: - Plan de operación y uso	Salida: - Programación operativa - Registro de copia de respaldo
Actividades: 1. Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados. 2. Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas. 3. Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	

4. Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.
5. Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.

DSS01.02 Gestionar servicios externalizados de TI

Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Plan de operación y uso - SLA, OLA	- Planes de aseguramiento independientes

Actividades:

1. Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs con terceros que alojan o proveen servicios.
2. Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios.
3. Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos.
4. Planificar la realización de auditorías y aseguramientos independiente de los entonos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.

DSS01.03 Supervisar la infraestructura de TI

Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Definiciones de servicio	- Reglas de monitorización de activos - Registro de eventos - Tickets de incidentes

Actividades

1. Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.
2. Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.
3. Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no estén sobrecargados con información innecesaria.
4. Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.
5. Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.
6. Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.

DSS01.04 Gestionar el entorno

Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Políticas de entorno - Informes de pólizas de seguro

Actividades

1. Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.
2. Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, está protegido contra las amenazas del entorno. Asegurar que la política limite o impida comer, beber y fumar en áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio en los centros de procesamiento de datos.
3. Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.
4. Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad).
5. Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas y el contacto con las autoridades locales de respuesta ante emergencias y entrenar al personal en estos procedimientos.
6. Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados. Atender a los puntos de no-conformidad de manera oportuna.

7. Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p.ej. robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servidores de producción y de desarrollo alejados entre sí).
8. Mantener en todo momento a los sitios de TI y las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).

DSS01.05 Verificar y revisar la integridad del repositorio de configuración
Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Informes de evaluación de instalaciones - Concienciación en salud y seguridad en el trabajo

Actividades
1. Examinar los requerimientos de las instalaciones de TI respecto de la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación ininterrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad del negocio.
2. Probar periódicamente los mecanismos del sistema de alimentación ininterrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio
3. Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.
4. Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en conductos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado. Proteger adecuadamente al cableado contra el daño causado por fuego, humo, agua, interceptación e interferencia.
5. Asegurar que el cableado y el *patching* físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p.ej. plano del edificio y diagramas de cableado).
6. Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.
7. Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.
8. Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo. Capacitar al personal en simulacros de incendio y rescate para asegurar el adecuado conocimiento y las acciones apropiadas a tomar en caso de incendio o incidentes similares.
9. Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición informes sobre incidentes en instalaciones donde la legislación y las regulaciones requieran su divulgación.
10. Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.
11. Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p.ej. daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de continuidad de negocio y de gestión de edificios.

DSS03: Gestionar problemas	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**

Descripción:
Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

Propósito:
Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.

Dueño del proceso:	**Partes interesadas:**
Director de DIGETI	- Decanos - Director PROESAD - Director EPG - Estudiantes de pregrado - Estudiantes de posgrado - Docentes - Personal administrativo

Metas corporativas relacionadas:
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes
08 Contar con docentes capacitados y especializados
10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
11 Incrementar los investigadores activos en redes de investigación

12 Desarrollar capacidades en investigación
13 Ampliar la disponibilidad y uso de biblioteca virtual
16 Desarrollar competencias para proyectos y programas
19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares
20 Alcanzar la excelencia en el desarrollo de las sesiones de clase
21 Consolidar la atención en tutorías
22 Alcanzar la efectividad de la gestión de prácticas pre profesionales
23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
24 Lograr la eficacia de los procesos de investigación científica
25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza
26 Alcanzar participación activa en proyectos según líneas de investigación
27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación
28 Administrar banco de problemas y necesidades
33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad
34 Fidelizar a la comunidad educativa
35 Difundir la producción intelectual en diferentes medios
36 Lograr posicionamiento por el logro de la investigación

Metas de TI relacionadas:	
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
14 Disponibilidad de información útil y relevante para la toma de decisiones	- Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión - Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información
Metas del proceso:	
Garantizar que los problemas relativos a TI son resueltos de forma que no vuelven a suceder	- Número de problemas para los que se ha encontrado una solución satisfactoria que apunta a la causa raíz - Porcentaje de incidentes graves para lo que se han registrado problemas - Porcentaje de soluciones temporales definidos para problemas abiertos - Porcentaje de problemas registrados como parte de una gestión de problemas proactiva

Prácticas de Gestión

DSS03.01 Identificar y clasificar problemas
Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Causa raíz relacionadas con riesgos - Criterios para el registro de problemas - Registro de problemas	- Esquema de clasificación de problemas - Informes de estado de problemas - Registro de problemas

Actividades:
1. Identificar problemas a través de la correlación de informes de incidentes, registros de error y otros recursos de identificación de problemas. Determinar niveles de prioridad y categorización para dedicarse a la resolución de problemas en tiempo basándose en los riesgos de negocio y en la definición del servicio.
2. Manejar formalmente todos los problemas con acceso a todos los datos relevantes, incluyendo información sobre el sistema de gestión de cambios y los detalles de incidentes sobre configuración/activos TI.
3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, en el análisis de la causa raíz, y en la determinación de la solución, para respaldar la gestión de problemas. Determinar grupos de soporte basados en categorías predefinidas, tales como hardware, redes, software, aplicaciones y software de soporte.
4. Definir niveles de prioridad mediante consultas con el negocio para asegurar que la identificación de problemas y el análisis de la causa raíz se llevan a cabo a tiempo de acuerdo con los ANSs acordados. Basar los niveles de prioridad en el impacto en el negocio y en la urgencia.
5. Informar del estado de problemas identificados al centro de servicios de forma que los clientes y la gestión de TI pueden mantenerse informados.

6. Mantener un catálogo de gestión de problemas único para registrar e informar sobre problemas identificados y para establecer pistas de auditoría sobre los procesos de gestión de problemas, incluyendo el estado de cada problema (p. ej., abierto, reabierto, en progreso o cerrado).

DSS03.02 Investigar y diagnosticar problemas

Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Causa raíz relacionadas con riesgos	- Causa raíz de los problemas - Informes de resolución de problemas

Actividades:

1. Identificar problemas que pueden ser errores conocidos comparando datos de incidentes con la base de datos de errores conocidos y posibles (p. ej., los comunicados por los proveedores externo) y clasificar problemas como errores conocidos.
2. Asociar los elementos de configuración afectados con el error conocido/establecido.
3. Producir informes para comunicar el progreso de la resolución de problemas y para supervisar el impacto continuado de los problemas no resueltos. Supervisar el estado del proceso de gestión de problemas a través de su ciclo de vida, incluyendo aportaciones de la gestión de cambios y de configuración.

DSS03.03 Levantar errores conocidos

Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
-	- Registro de errores conocidos - Soluciones propuestas para errores conocidos

Actividades

1. Tan pronto como las causas raíz de los problemas se han identificado, crear registros de errores conocidos y desarrollar una solución temporal adecuada.
2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambios) soluciones a los errores conocidos basándose en un caso de negocio coste beneficio y en el impacto de negocio y la urgencia.

DSS03.04 Resolver y cerrar problemas

Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Resoluciones de incidentes - Incidentes y peticiones de servicios cerrados	- Registro de problemas cerrados - Comunicación del conocimiento aprendido

Actividades

1. Cerrar registros de problemas, bien después de la confirmación de la eliminación satisfactoria del error conocido, bien tras acordar con el negocio cómo gestionar el problema de una manera alternativa.
2. Informar al centro de servicio del calendario de cierre del problema, p. ej., del calendario para solucionar los errores conocidos, la posible solución alternativa o el hecho de que el problema permanecerá hasta que el cambio se haya implementado, y las consecuencias de la solución escogida.
3. Mantener adecuadamente informados a los usuarios y a los clientes afectados.
4. A través del proceso de resolución, obtener informes periódicos de gestión de cambios acerca del progreso en la resolución de problemas y errores.
5. Supervisar el continuo impacto de los problemas y errores conocidos en los servicios.
6. Revisar y confirmar la resolución satisfactoria de problemas graves.
7. Asegurar que el conocimiento aprendido de esta revisión se incorpora en una reunión de revisión del servicio con el cliente de negocio.

DSS03.05 Realizar una gestión de problemas proactiva

Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Registro de monitorización de resolución de problemas - Identificar soluciones sostenibles

Actividades

1. Capturar información de problemas relacionada con cambios e incidentes TI y comunicarla a las partes interesadas clave. Esta comunicación podría tomar la forma de informes y reuniones periódicas entre los responsables de los procesos de gestión de incidentes, problemas, cambios y configuración para considerar problemas recientes y acciones correctivas potenciales.
2. Asegurar que los responsables de los procesos y los responsables de gestión de incidentes, problemas, cambios y configuración se reúnen regularmente para discutir problemas conocidos y cambios futuros planificados.
3. Permitir a la empresa supervisar los costes totales de problemas, capturar esfuerzos de cambio resultantes de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar de ellos.

4. Producir informes para supervisar la resolución de problemas respecto a los requisitos de negocio y ANSs. Asegurar el adecuado escalado de problemas, p. ej., escalado a un nivel de gestión superior de acuerdo con los criterios acordados, contactando proveedores externos, o enviando al comité de gestión de cambios para incrementar la prioridad de una petición de cambio urgente para implementar una solución temporal.
5. Optimizar el uso de recursos y reducir las soluciones temporales y hacer seguimiento de las tendencias de problemas.
6. Identificar e iniciar soluciones sostenibles (soluciones permanentes) identificando la causa raíz, y levantar peticiones de cambio a través de los procesos de gestión de cambios establecidos.

DSS04: Gestionar la continuidad	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
Descripción: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	
Propósito: Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.	
Dueño del proceso: Director de DIGETI	**Partes interesadas:** - Decanos - Director PROESAD - Director EPG - Estudiantes de pregrado - Estudiantes de posgrado - Docentes - Personal administrativo
Metas corporativas relacionadas:	
03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes 08 Contar con docentes capacitados y especializados 10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica 11 Incrementar los investigadores activos en redes de investigación 12 Desarrollar capacidades en investigación 13 Ampliar la disponibilidad y uso de biblioteca virtual 16 Desarrollar competencias para proyectos y programas 19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares 20 Alcanzar la excelencia en el desarrollo de las sesiones de clase 21 Consolidar la atención en tutorías 22 Alcanzar la efectividad de la gestión de prácticas pre profesionales 23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje 24 Lograr la eficacia de los procesos de investigación científica 25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza 26 Alcanzar participación activa en proyectos según líneas de investigación 27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación 28 Administrar banco de problemas y necesidades 31 Implementar y difundir eficazmente el Plan Maestro de Desarrollo Espiritual 33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad 34 Fidelizar a la comunidad educativa 35 Difundir la producción intelectual en diferentes medios 36 Lograr posicionamiento por el logro de la investigación	
Metas de TI relacionadas:	
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
14 Disponibilidad de información útil y relevante para la toma de decisiones	- Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión - Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información
Metas del proceso:	

La información crítica para el negocio está disponible en línea con los niveles de servicio mínimo requeridos	- Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento - Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo
Los servicios críticos tienen suficiente resiliencia	- Número de sistemas críticos para el negocio no cubiertos por el plan
Las pruebas de continuidad del servicio han verificado la efectividad del plan	- Número de ejercicios y pruebas que han conseguido los objetivos de recuperación - Frecuencia de las pruebas
Un plan de continuidad actualizado refleja los requisitos de negocio	- Porcentaje de mejoras acordadas que han sido reflejadas en el plan - Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan
Las partes interesadas internas y externas han sido formadas en el plan de continuidad	- Porcentaje de interesados internos y externos que han recibido formación - Porcentaje de asuntos identificados que se han tratado subsecuentemente en los materiales de formación

Prácticas de Gestión

DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance
Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.

Iniciativas y/o Documentos E/S

Entrada: - SLA	Salida: - Política y objetivo de continuidad de negocio - Escenarios de incidentes - Valoración de las capacidades actuales

1. Identificar procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.
2. Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.
3. Definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial.
4. Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.

DSS04.02 Mantener una estrategia de continuidad
Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.

Iniciativas y/o Documentos E/S

Entrada: - Causas raíz relacionadas con riesgos - Comunicaciones del impacto de los riesgos	Salida: - Análisis del impacto en el negocio - Requerimientos de continuidad

Actividades:
1. Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes.
2. Realizar un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas.
3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.
4. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.
5. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.
6. Determinar las condiciones y los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad.
7. Identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.
8. Obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas.

DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio
Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas

Iniciativas y/o Documentos E/S

Entrada: - OLA	Salida: - Acciones y comunicaciones de respuesta a incidentes - Plan de continuidad de negocio (BCP)

Actividades:
1. Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción. Definir los roles y responsabilidades relacionados, incluyendo la responsabilidad para la política y la implementación.

2. Desarrollar y mantener planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizados.
3. Asegurar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.
4. Definir las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.
5. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.
6. Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel, así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.
7. Determinar las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos.
8. Distribuir los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre.

DSS04.04 Ejercitar, probar y revisar el BCP

Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Pruebas de objetivos - Pruebas de ejercicios - Pruebas de resultados y recomendaciones

Actividades

1. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.
2. Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.
3. Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.
4. Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.
5. Realizar un análisis y revisión post-ejercicio para considerar el logro.
6. Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.

DSS04.05 Revisar, mantener y mejorar el plan de continuidad

Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Resultados de las revisiones del plan - Cambios recomendados al plan

Actividades

1. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégico como operativos.
2. Considerar si es necesario una revisión del análisis de impacto en el negocio, dependiendo en la naturaleza de los cambios.
3. Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la dirección y su realización mediante el proceso de gestión de cambios.
4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones.

DSS04.06 Proporcionar formación en el plan de continuidad

Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Lista del personal que requiere formación	- Requerimientos de formación - Resultados de la supervisión de habilidades y competencias

Actividades

1. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.
2. Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.
3. Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.

DSS04.07 Gestionar acuerdos de respaldo
Mantener la disponibilidad de la información crítica del negocio.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Probar los resultados de las copias de seguridad de los datos

Actividades

1. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando:
   - Frecuencia (mensual, semanal, diaria, etc.)
   - Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración)
   - Tipo de copias de seguridad (por ejemplo, completa frente a incremental)
   - Tipo se soporte
   - Copias de seguridad automatizadas en línea
   - Tipos de datos (por ejemplo, voz, óptica)
   - Creación de registros
   - Datos de cálculos críticos de usuario final (por ejemplo, hojas de cálculo)
   - Localización física y lógica de las fuentes de los datos
   - Seguridad y derechos de acceso
   - Cifrado
2. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito (escrow).
3. Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.
4. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).
5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.

DSS04.08 Ejecutar revisiones post reanudación
Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Informe de revisión post reanudación

Actividades

1. Evaluar la observancia del Plan de Continuidad de Negocio (BCP) documentado.
2. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.
3. Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.
4. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.

MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad	**Área: Gestión** **Dominio: Supervisar, Evaluar y Valorar**

Descripción:
Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

Propósito:
Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.

Dueño del proceso:	**Partes interesadas:**
Director de DIGETI	- Decanos - Director PROESAD - Director EPG - Personal administrativo

Metas corporativas relacionadas:

03 Consolidar el programa de becas y servicios para el desarrollo integral de los estudiantes
08 Contar con docentes capacitados y especializados
10 Fortalecer la participación de docentes y estudiantes en eventos de investigación científica
11 Incrementar los investigadores activos en redes de investigación
12 Desarrollar capacidades en investigación
13 Ampliar la disponibilidad y uso de biblioteca virtual
16 Desarrollar competencias para proyectos y programas
19 Lograr una planificación de Enseñanza - Aprendizaje, acorde a los estándares

20 Alcanzar la excelencia en el desarrollo de las sesiones de clase
21 Consolidar la atención en tutorías
22 Alcanzar la efectividad de la gestión de prácticas pre profesionales
23 Lograr la efectividad en la evaluación de la Enseñanza – Aprendizaje
24 Lograr la eficacia de los procesos de investigación científica
25 Fortalecer la cultura de investigación en diferentes niveles de enseñanza
26 Alcanzar participación activa en proyectos según líneas de investigación
27 Lograr que estudiantes y docentes registren proyectos según líneas de investigación
28 Administrar banco de problemas y necesidades
33 Lograr el posicionamiento y reconocimiento en la IASD y la sociedad
34 Fidelizar a la comunidad educativa
35 Difundir la producción intelectual en diferentes medios
36 Lograr posicionamiento por el logro de la investigación

Metas de TI relacionadas:	
04 Riesgos de negocio relacionados con las TI gestionados	- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos - Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones del negocio debidas a incidentes en el servicio de TI - Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
11 Optimización de activos, recursos y capacidades de las TI	- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades de TI.
Metas del proceso:	
Objetivos y métricas aprobadas por las partes interesadas	- Porcentaje de informes de rendimiento entregados en plazo - Porcentaje de objetivos y métricas aprobadas por las partes interesadas
Procesos medidos acorde a las métricas y objetivos acordados	- Porcentaje de procesos con objetivos y métricas definidas
La monitorización, evaluación y generación de información es efectiva y operativa	- Porcentaje de procesos con efectividad de objetivos y métricas revisadas y mejoradas - Porcentaje de procesos críticos supervisados
Objetivos y métricas integradas dentro de los sistemas de supervisión de la empresa	- Porcentaje de objetivos y métricas alineadas al sistema de supervisión de la empresa
Los informes acerca del rendimiento y conformidad de los procesos es útil y a tiempo	- Porcentaje de informes de rendimiento entregados en plazo

Prácticas de Gestión

MEA01.01 Establecer un enfoque de la supervisión

Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Principios de comunicación e informes - Reglas de validación y aprobación de los informes	- Requisitos de supervisión - Métricas y objetivos de supervisión aprobados

1. Identificar las partes interesadas (p. ej. dirección, propietarios de procesos o usuarios).
2. Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes (p. ej. glosario corporativo, metadatos y taxonomías), líneas de referencia y estudios comparativos (benchmarking).
3. Mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía así como las herramientas utilizadas para la obtención de datos y presentación de informes corporativos (p. ej. aplicaciones de inteligencia de negocio).
4. Acordar los objetivos y métricas (p. ej., cumplimiento, rendimiento, valor, riesgo), taxonomía (clasificación y relación entre objetivos y métricas) y la retención de datos (evidencias).
5. Acordar un proceso de control de cambios y de gestión del ciclo de vida de la supervisión y la presentación de informes. Incluir oportunidades de mejora para la presentación de la información, métricas, enfoque, líneas de referencia y estudios comparativos.
6. Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).
7. Validar periódicamente el enfoque utilizado e identificar los nuevos o cambiantes grupos de interés, requisitos y recursos.

MEA01.02 Establecer los objetivos de cumplimiento y rendimiento

Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Métricas y objetivos de rendimiento - Métricas para el seguimiento de la mejora de los procesos	- Objetos de supervisión

Actividades:

1. Definir y revisar periódicamente los objetivos y métricas con las partes interesadas para identificar cualquier detalle significativo omitido y definir la razonabilidad de metas y tolerancias.
2. Comunicar los cambios propuestos en las metas y tolerancias de rendimiento y cumplimiento (referidos a las métricas) con las partes interesadas clave con la debida diligencia (p. ej., legal, auditoría, RR.HH., ética, cumplimiento y financiero).
3. Hacer público a los usuarios de la información los cambios en metas y tolerancias.
4. Evaluar si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).

MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento

Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.

Iniciativas y/o Documentos E/S

Entrada:	Salida:
- Evaluación de la capacidad de los procesos - Resultados de la supervisión al cumplimiento de los proveedores - Informes de la revisión de la capacidad, rendimiento y disponibilidad - Informes de evaluación de instalaciones	- Datos de supervisión y revisión procesados

Actividades:

1. Recopilar datos de los procesos definidos, de forma automatizada, cuando sea posible.
2. Evaluar la eficiencia (esfuerzo en relación con la comprensión detallada proporcionada) y oportunidad (utilidad y significado) y validar la integridad (precisión y completitud) de los datos recopilados.
3. Consolidar los datos para soportar el cálculo de las métricas acordadas.
4. Alinear los datos consolidados a los enfoques y objetivos de presentación de información de la compañía.
5. Utilizar herramientas y sistemas apropiados para el procesamiento y formateo de datos para análisis.

MEA01.04 Analizar e informar sobre el rendimiento

Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
-	- Informes de desempeño

Actividades

1. Diseñar informes de rendimiento de procesos que sean concisos, fáciles de entender y ajustados a las diferentes necesidades de gestión y audiencias. Facilitar la toma efectiva y oportuna de decisiones (p. ej., cuadros de mando, informes con semáforos) y asegurar que la causa y el efecto entre objetivos y métricas se comunican de una forma comprensible.
2. Comparar los valores de rendimiento con metas y estudios comparativos internos (*benchmarks*) y, cuando sea posible, con estudios comparativos externos (tanto del sector, como respecto a competidores clave).
3. Recomendar cambios a los objetivos y métricas, cuando sea procedente.
4. Distribuir los informes a las partes interesadas relevantes.
5. Analizar la causa de las desviaciones respecto a las metas, iniciar acciones correctivas, asignar responsabilidades para la remediación y realizar su seguimiento. En el momento oportuno, revisar todas las desviaciones y buscar causas raíz cuando sea necesario. Documentar las incidencias para contar con guía adicional si el problema vuelve a aparecer. Documentar los resultados.
6. Cuando sea factible, enlazar el cumplimiento de objetivos de desempeño con el sistema de compensación y gratificación de la organización.

MEA01.05 Asegurar la implantación de medidas correctivas

Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.

Iniciativas y/o Documentos E/S

Entrada	**Salida**
- Acciones correctivas de incumplimiento	- Acciones y asignaciones correctivas - Estado y resultado de las acciones

Actividades

1. Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores.
2. Asegurar que se mantiene la asignación de responsabilidades en las acciones correctivas.
3. Hacer seguimiento de los resultados de las acciones comprometidas.
4. Informar de los resultados a las partes interesadas.

3. Instrumento de evaluación de la capacidad de procesos de TI para el Nivel 1 – Proceso DSS05 Gestión de los servicios de seguridad

INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS

NIVEL 1: PROCESO EJECUTADO

ATRIBUTO: 1.1. RENDIMIENTO DEL PROCESO

PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

PRÁCTICA DE GESTIÓN: DSS05.01 - PROTEGER CONTRA SOFTWARE MALICIOSO							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	1	Se realiza concienciación sobre software malicioso en el personal?	30%			
		2	Existen procedimientos de prevención sobre software malicioso?	40%			
		3	Se ha asignado responsabilidades de prevención sobre software malicioso?	30%			
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	4	Se ha instalado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	30%			
		5	Se ha instalado herramientas de protección frente a software malicioso que se actualizan de forma automática o semiautomática	30%			
		6	Se ha activado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	20%			
		7	Se ha activado herramientas de protección frente a software malicioso que se actualizan de forma automática o semiautomática	20%			
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	8	El software de protección contra software malicioso se distribuye de forma centralizada?	50%			
		9	El software de protección contra software malicioso se distribuye usando una configuración específica?	50%			
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	10	Se revisa la información sobre nuevas amenazas?	50%			
		11	Se evalúa la información sobre nuevas amenazas?	50%			
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	12	Se filtra el tráfico entrante para protección de software espía o correo de pishing?	100%			
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	13	Se realiza formación sobre software malicioso en el uso de correos electrónicos e internet?	50%			
		14	Se orienta a los usuarios a no instalar software compartido o no autorizado?	50%			
PRÁCTICA DE GESTIÓN: DSS05.02 - GESTIONAR LA SEGURIDAD DE LA RED Y LAS CONEXIONES							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	15	Se ha establecido una Política de seguridad para las conexiones basado en análisis de riesgos?	50%			
		16	Se ha establecido una Política de seguridad para las conexiones basado en los requerimientos del negocio?	50%			
2	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	17	El acceso a la información de la empresa está restringido solo para dispositivos autorizados?	30%			
		18	El acceso a la red de la empresa está restringido solo a dispositivos autorizados?	40%			
		19	Se ha configurado los dispositivos autorizados para solicitar contraseña antes del acceso ?	30%			
3	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con	20	Se ha implementado mecanismos de filtrado de red para el control del tráfico entrante y saliente?	100%			

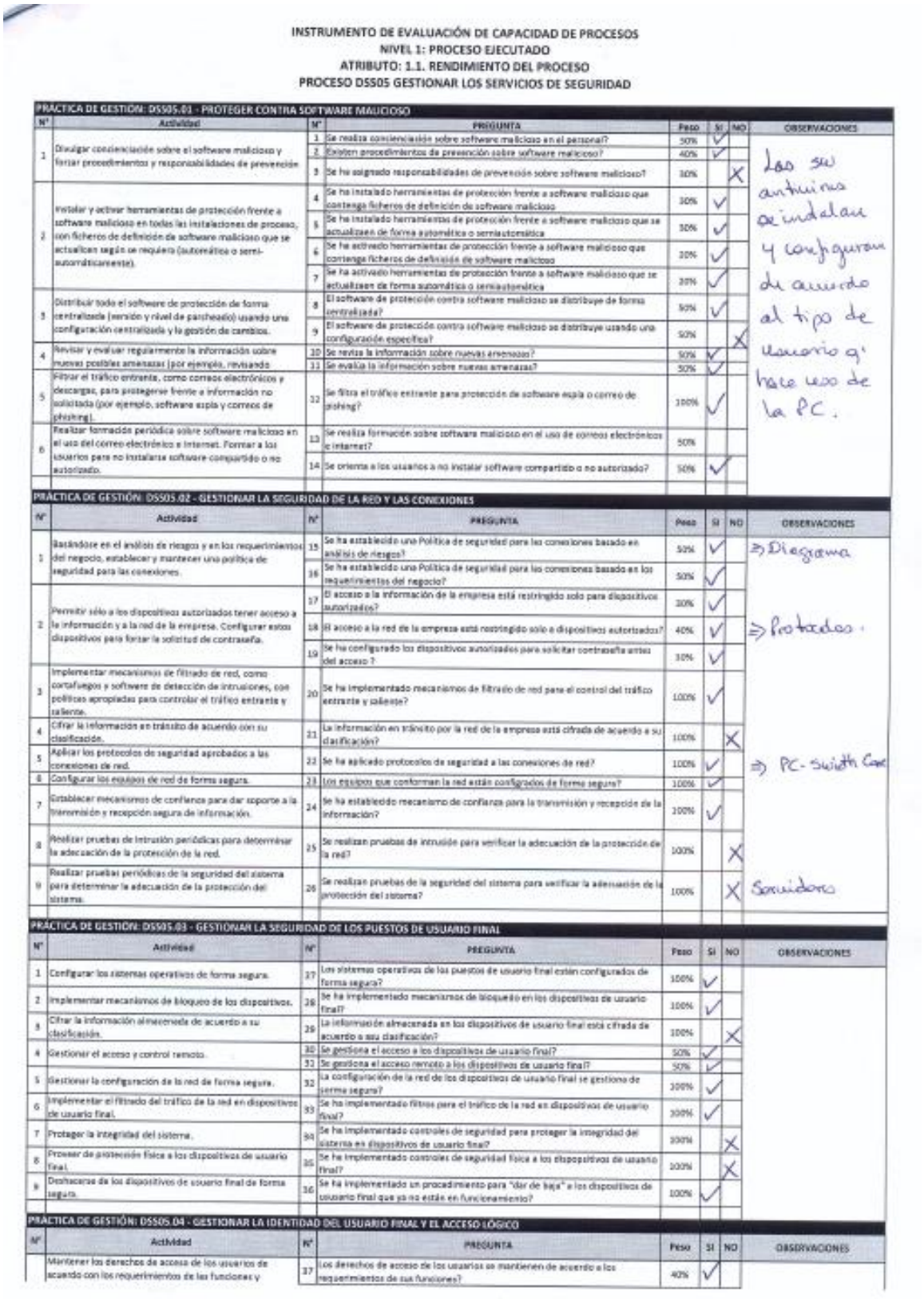
	políticas apropiadas para controlar el tráfico entrante y saliente.						
4	Cifrar la información en tránsito de acuerdo con su clasificación.	21	La información en tránsito por la red de la empresa está cifrada de acuerdo a su clasificación?	100%			
5	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	22	Se ha aplicado protocolos de seguridad a las conexiones de red?	100%			
6	Configurar los equipos de red de forma segura.	23	Los equipos que conforman la red están configurados de forma segura?	100%			
7	Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	24	Se ha establecido mecanismo de confianza para la transmisión y recepción de la información?	100%			
8	Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	25	Se realizan pruebas de intrusión para verificar la adecuación de la protección de la red?	100%			
9	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	26	Se realizan pruebas de la seguridad del sistema para verificar la adecuación de la protección del sistema?	100%			
PRÁCTICA DE GESTIÓN: DSS05.03 - GESTIONAR LA SEGURIDAD DE LOS PUESTOS DE USUARIO FINAL							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Configurar los sistemas operativos de forma segura.	27	Los sistemas operativos de los puestos de usuario final están configurados de forma segura?	100%			
2	Implementar mecanismos de bloqueo de los dispositivos.	28	Se ha implementado mecanismos de bloqueo en los dispositivos de usuario final?	100%			
3	Cifrar la información almacenada de acuerdo a su clasificación.	29	La información almacenada en los dispositivos de usuario final está cifrada de acuerdo a asu clasificación?	100%			
4	Gestionar el acceso y control remoto.	30	Se gestiona el acceso a los dispositivos de usuario final?	50%			
		31	Se gestiona el acceso remoto a los dispositivos de usuario final?	50%			
5	Gestionar la configuración de la red de forma segura.	32	La configuración de la red de los dispositivos de usuario final se gestiona de forma segura?	100%			
6	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	33	Se ha implementado filtros para el tráfico de la red en dispositivos de usuario final?	100%			
7	Proteger la integridad del sistema.	34	Se ha implementado controles de seguridad para proteger la integridad del sistema en dispositivos de usuario final?	100%			
8	Proveer de protección física a los dispositivos de usuario final.	35	Se ha implementado controles de seguridad física a los dispositivos de usuario final?	100%			
9	Deshacerse de los dispositivos de usuario final de forma segura.	36	Se ha implementado un procedimiento para "dar de baja" a los dispositivos de usuario final que ya no están en funcionamiento?	100%			
PRÁCTICA DE GESTIÓN: DSS05.04 - GESTIONAR LA IDENTIDAD DEL USUARIO FINAL Y EL ACCESO LÓGICO							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	37	Los derechos de acceso de los usuarios se mantienen de acuerdo a los requerimientos de sus funciones?	40%			
		38	Los derechos de acceso de los usuarios se mantienen de acuerdo a los requerimientos de los procesos de negocio?	40%			
		39	La gestión de identidades y derechos de acceso se alinea con los roles y responsabilidades definidas para cada tipo de usuario?	20%			
2	Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.	40		30%			
		41		35%			
		42		35%			
3	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad,	43	Los accesos a los activos de información son autenticados según la clasificación de seguridad?	35%			

	coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	44	Los accesos a los activos de información se coordinan con las unidades de negocio q las gestionan?	35%			
		45	Se asegura que los controles de autenticación son administrados adecuadamente?	30%			
4	Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	46	Los cambios en los derechos de acceso son aprobados por gestores designados?	30%			
		47	Los cambios en los derechos de acceso son documentados?	30%			
		48	Los cambios en los derechos de acceso son autorizados por gestores designados?	40%			
5	Segregar y gestionar cuentas de usuario privilegiadas	49	Las cuentas de usuario privilegiadas son segregadas?	40%			
		50	Las cuentas de usuario privilegiadas son gestionadas?	60%			
6	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	51	Se realiza revisiones a las cuentas de usuarios y sus privilegios relacionados a intervalos regulares?	100%			
7	Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	52	La identificación de los usuarios (internos, externos y temporales) se realiza de forma segura?	35%			
		53	La identificación de las actividades sobre los sistemas e infraestructura de TI que tiene cada usuario se realiza de forma segura?	35%			
		54	Las actividades sobre el procesamiento de información que tiene cada usuario se realiza de forma segura?	30%			
8	Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible	55	Se mantiene una pista de auditoría de los accesos a la información clasificada como sensible?	100%			
PRÁCTICA DE GESTIÓN: DSS05.05 - GESTIONAR EL ACCESO FÍSICO A LOS ACTIVOS DE TI							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.	56	El acceso físico a las instalaciones de TI se realiza a través de peticiones formales que son revisadas por la dirección de TI?	25%			
		57	Se concede el acceso físico a las instalaciones de TI solo a las áreas que se solicitaron?	25%			
		58	El acceso físico a las instalaciones de TI es autorizado por la dirección de TI?	25%			
		59	Existe un registro de las peticiones formales realizadas a la dirección de TI?	25%			
2	Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	60	Los perfiles de acceso físico a las instalaciones de TI están actualizados?	50%			
		61	El acceso físico a las instalaciones de TI se realiza en función al trabajo y responsabilidades?	50%			
3	Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	62	Los puntos de entrada a las instalaciones de TI se encuentran en un registro formal?	35%			
		63	Los puntos de entrada a las instalaciones de TI son supervisados regularmente?	35%			
		64	Se lleva un registro del acceso a las instalaciones de TI de todos los visitantes (proveedores, vendedores)	30%			
4	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	65	El personal que labora en las instalaciones de TI cuenta con tarjetas de identificación?	25%			
		66	Se capacita al personal que labora en las instalaciones de TI sobre el uso de la tarjeta de identificación?	25%			
		67	El personal que labora en las instalaciones de TI mantiene visible la tarjeta de identificación?	25%			
		68	Se previene la entrega de tarjetas de identificación sin autorización?	25%			
5	Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un	69	Las visitas autorizadas a ingresar a las instalaciones de TI son escoltadas en todo momento?	50%			

	individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	70	Se alerta al personal de seguridad sobre la presencia de algún individuo que no porte la tarjeta de identificación?	50%			
6	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	71	El acceso a las instalaciones de TI sensibles está restringido con controles de seguridad en el perímetro?	50%			
		72	Se verifica que los controles de seguridad en el perímetro restringen el acceso no autorizado?	25%			
		73	Se verifica que los controles de seguridad en el perímetro disparan una alarma en caso de acceso no autorizado?	25%			
7	Realizar regularmente formación de concienciación de seguridad física.	74	Se capacita al personal que labora en las instalaciones de TI sobre seguridad física regularmente?	100%			
PRÁCTICA DE GESTIÓN: DSS05.06 - GESTIONAR DOCUMENTOS SENSIBLES Y DISPOSITIVOS DE SALIDA							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa.	75	Se ha establecido un procedimiento para la recepción de formularios especiales y dispositivos de salida?	25%			
		76	Se ha establecido un procedimiento para el uso de formularios especiales y dispositivos de salida?	25%			
		77	Se ha establecido un procedimiento para la eliminación de formularios especiales y dispositivos de salida?	25%			
		78	Se ha establecido un procedimiento para la destrucción de formularios especiales y dispositivos de salida?	25%			
2	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	79	Se han asignado privilegios de acceso a los documentos sensibles y dispositivos de salida considerando el riesgo?	50%			
		80	Se han asignado privilegios de acceso a los documentos sensibles y dispositivos de salida considerando los requerimientos del negocio?	50%			
3	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	81	Se ha establecido un inventario de documentos sensibles y dispositivos de salida?	50%			
		82	Se realiza conciliaciones del inventario de documentos sensibles y dispositivos de salida?	50%			
4	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos de salida.	83	Se ha establecido controles de seguridad físicos sobre los formularios especiales y dispositivos de salida?	100%			
5	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).	84	La información contenida en los documentos o dispositivos sensibles es destruida de forma segura?	50%			
		85	Se protege los dispositivos de salida de forma adecuada?	50%			
PRÁCTICA DE GESTIÓN: DSS05.07 - SUPERVISAR LA INFRAESTRUCTURA PARA DETECTAR EVENTOS RELACIONADOS CON LA SEGURIDAD							
N°	**Actividad**	**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**	**OBSERVACIONES**
1	Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	86	Los eventos relacionados con la seguridad reportados por las herramientas de monitoreo de infraestructura son registrados formalmente?	**35%**			
		87	Se identifica información sensible que debe guardarse considerando el riesgo asociado?	**35%**			
		88	La información obtenida es retenida por un periodo apropiado?	**30%**			
2	Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la	89	La naturaleza de los incidentes potenciales relacionados con la seguridad son definidos adecuadamente?	**25%**			

	seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta mensurada.	90	Las características de los incidentes potenciales relacionados con la seguridad son definidos adecuadamente?	**25%**			
		91	La naturaleza de los incidentes potenciales relacionados con la seguridad es comunicada a todos los interesados?	**25%**			
		92	Las características de los incidentes potenciales relacionados con la seguridad son comunicados a todos los interesados?	**25%**			
3	Revisar regularmente los registros de eventos para detectar incidentes potenciales.	93	El registro de eventos relacionados con la seguridad es revisado regularmente?	100%			
4	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	94	Se mantiene un procedimiento para la recopilación de evidencias en línea?	50%			
		95	Se asegura que el personal conoce los requerimientos para la recopilación de evidencias?	50%			
5	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	96	La creación de tickets de incidentes de seguridad se realiza en el momento que indica el sistema de monitoreo?	100%			

4. Instrumentos de evaluación aplicado en la evaluación de la capacidad del proceso DSS05 Gestionar los servicios de seguridad



INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 1: PROCESO EJECUTADO
ATRIBUTO: 1.1. RENDIMIENTO DEL PROCESO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

PRÁCTICA DE GESTIÓN: DSS05.01 - PROTEGER CONTRA SOFTWARE MALICIOSO

Nº	Actividad	Nº	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Divulgar concienciación sobre el software malicioso y fortalecer procedimientos y responsabilidades de prevención	1	Se realiza concienciación sobre software malicioso en el personal?	50%	✓		Los SW antivirus se instalan y configuran de acuerdo al tipo de usuario q' hace uso de la PC.
		2	Existen procedimientos de prevención sobre software malicioso?	40%	✓		
		3	Se ha asignado responsabilidades de prevención sobre software malicioso?	10%		X	
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	4	Se ha instalado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	30%	✓		
		5	Se ha instalado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	30%	✓		
		6	Se ha activado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	20%	✓		
		7	Se ha activado herramientas de protección frente a software malicioso que se actualizaen de forma automática o semiautomática	20%	✓		
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	8	El software de protección contra software malicioso se distribuye de forma centralizada?	50%	✓		
		9	El software de protección contra software malicioso se distribuye usando una configuración específica?	50%		X	
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando	10	Se revisa la información sobre nuevas amenazas?	50%	✓		
		11	Se evalúa la información sobre nuevas amenazas?	50%	✓		
5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	12	Se filtra el tráfico entrante para protección de software espía o correo de phishing?	100%	✓		
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	13	Se realiza formación sobre software malicioso en el uso de correos electrónicos e internet?	50%			
		14	Se orienta a los usuarios a no instalar software compartido o no autorizado?	50%	✓		

PRÁCTICA DE GESTIÓN: DSS05.02 - GESTIONAR LA SEGURIDAD DE LA RED Y LAS CONEXIONES

Nº	Actividad	Nº	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	15	Se ha establecido una Política de seguridad para las conexiones basado en análisis de riesgos?	50%	✓		⇒ Diagrama
		16	Se ha establecido una Política de seguridad para las conexiones basado en los requerimientos del negocio?	50%	✓		
2	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	17	El acceso a la información de la empresa está restringido solo para dispositivos autorizados?	30%	✓		
		18	El acceso a la red de la empresa está restringido solo a dispositivos autorizados?	40%	✓		⇒ Protocolos.
		19	Se ha configurado los dispositivos autorizados para solicitar contraseña antes del acceso ?	30%	✓		
3	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	20	Se ha implementado mecanismos de filtrado de red para el control del tráfico entrante y saliente?	100%	✓		
4	Cifrar la información en tránsito de acuerdo con su clasificación.	21	La información en tránsito por la red de la empresa está cifrada de acuerdo a su clasificación?	100%		X	
5	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	22	Se ha aplicado protocolos de seguridad a las conexiones de red?	100%	✓		⇒ PC - Switch Core
6	Configurar los equipos de red de forma segura.	23	Los equipos que conforman la red están configurados de forma segura?	100%	✓		
7	Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	24	Se ha establecido mecanismo de confianza para la transmisión y recepción de la información?	100%	✓		
8	Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	25	Se realizan pruebas de intrusión para verificar la adecuación de la protección de la red?	100%		X	
9	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	26	Se realizan pruebas de la seguridad del sistema para verificar la adecuación de la protección del sistema?	100%		X	Servidores

PRÁCTICA DE GESTIÓN: DSS05.03 - GESTIONAR LA SEGURIDAD DE LOS PUESTOS DE USUARIO FINAL

Nº	Actividad	Nº	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Configurar los sistemas operativos de forma segura.	27	Los sistemas operativos de los puestos de usuario final están configurados de forma segura?	100%	✓		
2	Implementar mecanismos de bloqueo de los dispositivos.	28	Se ha implementado mecanismos de bloqueado en los dispositivos de usuario final?	100%	✓		
3	Cifrar la información almacenada de acuerdo a su clasificación.	29	La información almacenada en los dispositivos de usuario final está cifrada de acuerdo a su clasificación?	100%		X	
4	Gestionar el acceso y control remoto.	30	Se gestiona el acceso a los dispositivos de usuario final?	50%	✓		
		32	Se gestiona el acceso remoto a los dispositivos de usuario final?	50%	✓		
5	Gestionar la configuración de la red de forma segura.	32	La configuración de la red de los dispositivos de usuario final se gestiona de forma segura?	100%	✓		
6	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	33	Se ha implementado filtros para el tráfico de la red en dispositivos de usuario final?	100%	✓		
7	Proteger la integridad del sistema.	34	Se ha implementado controles de seguridad para proteger la integridad del sistema en dispositivos de usuario final?	100%		X	
8	Proveer de protección física a los dispositivos de usuario final.	35	Se ha implementado controles de seguridad física a los dispositivos de usuario final?	100%		X	
9	Deshacerse de los dispositivos de usuario final de forma segura.	36	Se ha implementado un procedimiento para "dar de baja" a los dispositivos de usuario final que ya no están en funcionamiento?	100%	✓		

PRÁCTICA DE GESTIÓN: DSS05.04 - GESTIONAR LA IDENTIDAD DEL USUARIO FINAL Y EL ACCESO LÓGICO

Nº	Actividad	Nº	PREGUNTA	Peso	SI	NO	OBSERVACIONES
	Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y	37	Los derechos de acceso de los usuarios se mantienen de acuerdo a los requerimientos de sus funciones?	40%	✓		

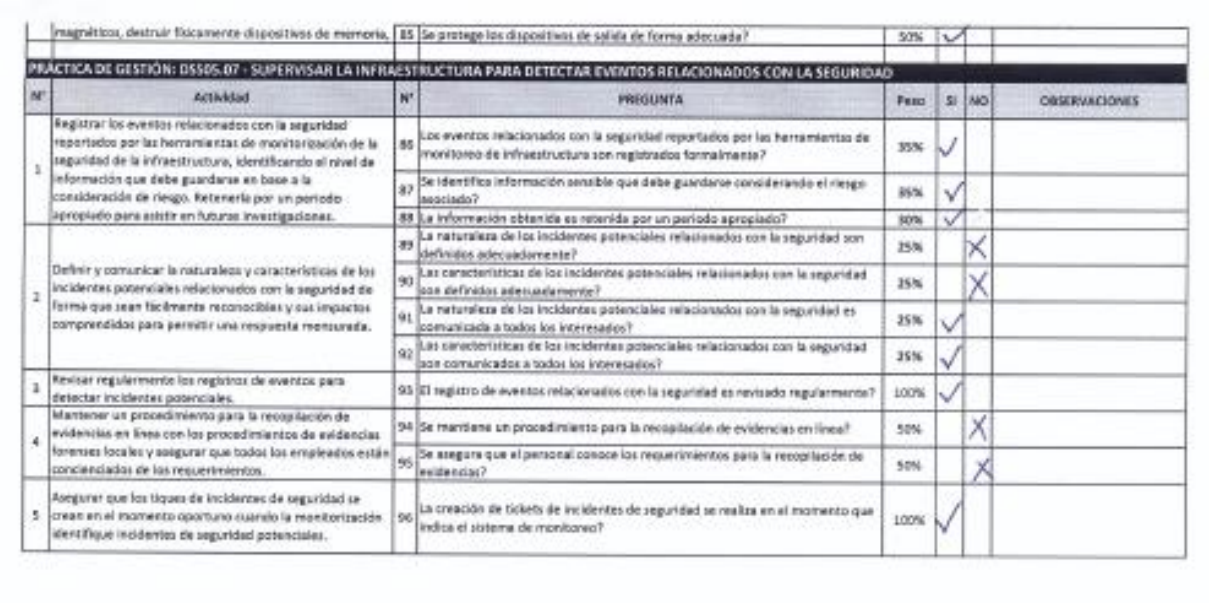
1	procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	38	Los derechos de acceso de los usuarios se mantienen de acuerdo a los requerimientos de los procesos de negocio?	40%	✓		
		39	La gestión de identidades y derechos de acceso se alinea con los roles y responsabilidades definidos para cada tipo de usuario?	20%	✓		
2	Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles	40		30%		X	
		41		35%		X	
		42		35%		X	
3	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	43	Los accesos a los activos de información son autenticados según la clasificación de seguridad?	35%	✓		
		44	Los accesos a los activos de información se coordinan con las unidades de negocio o las gestionan?	35%	✓		Correo
		45	Se asegura que los controles de autenticación son administrados adecuadamente?	30%	✓		
4	Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	46	Los cambios en los derechos de acceso son aprobados por gestores designados?	30%	✓		
		47	Los cambios en los derechos de acceso son documentados?	30%		X	
		48	Los cambios en los derechos de acceso son autorizados por gestores designados?	40%	✓		
5	Segregar y gestionar cuentas de usuario privilegiadas	49	Las cuentas de usuario privilegiadas son segregadas?	40%	✓		
		50	Las cuentas de usuario privilegiadas son gestionadas?	60%	✓		
6	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	51	Se realiza revisiones a las cuentas de usuarios y sus privilegios relacionados a intervalos regulares?	100%	✓		
7	Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	52	La identificación de los usuarios (internos, externos y temporales) se realiza de forma segura?	35%	✓		
		53	La identificación de las actividades sobre los sistemas e infraestructura de TI que tiene cada usuario se realiza de forma segura?	35%	✓		
		54	Las actividades sobre el procesamiento de información que tiene cada usuario se realiza de forma segura?	30%	✓		
8	Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible	55	Se mantiene una pista de auditoría de los accesos a la información clasificada como sensible?	100%		X	

PRÁCTICA DE GESTIÓN: DS5DS.05 - GESTIONAR EL ACCESO FÍSICO A LOS ACTIVOS DE TI

N°	Actividad	N°	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.	56	El acceso físico a las instalaciones de TI se realiza a través de peticiones formales que son revisadas por la dirección de TI?	25%		X	
		57	Se concede el acceso físico a las instalaciones de TI solo a las áreas que se solicitaron?	25%		X	
		58	El acceso físico a las instalaciones de TI es autorizado por la dirección de TI?	25%	✓		
		59	Existe un registro de las peticiones formales realizadas a la dirección de TI?	25%		X	
2	Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	60	Los perfiles de acceso físico a las instalaciones de TI están actualizados?	50%		X	
		61	El acceso físico a las instalaciones de TI se realiza en función al trabajo y responsabilidades?	50%	✓		
3	Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	62	Los puntos de entrada a las instalaciones de TI se encuentran en un registro formal?	35%	✓		
		63	Los puntos de entrada a las instalaciones de TI son supervisados regularmente?	35%	✓		
		64	Se lleva un registro del acceso a las instalaciones de TI de todos los visitantes (proveedores, vendedores)	30%		X	
4	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	65	El personal que labora en las instalaciones de TI cuenta con tarjetas de identificación?	25%	✓		
		66	Se capacita al personal que labora en las instalaciones de TI sobre el uso de la tarjeta de identificación?	25%	✓		
		67	El personal que labora en las instalaciones de TI mantiene visible la tarjeta de identificación?	25%		X	
		68	Se previene la entrega de tarjetas de identificación sin autorización?	25%		X	
5	Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al	69	Las visitas autorizadas a ingresar a las instalaciones de TI son escoltadas en todo momento?	50%	✓		
		70	Se alerta al personal de seguridad sobre la presencia de algún individuo que no porte la tarjeta de identificación?	50%		X	
6	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen	71	El acceso a las instalaciones de TI sensibles está restringido con controles de seguridad en el perímetro?	50%		X	
		72	Se verifica que los controles de seguridad en el perímetro restringen el acceso no autorizado?	25%		X	
		73	Se verifica que los controles de seguridad en el perímetro disparen una alarma en caso de acceso no autorizado?	25%		X	
7	Realizar regularmente formación de concienciación de seguridad física.	74	Se capacita al personal que labora en las instalaciones de TI sobre seguridad física regularmente?	100%	✓		

PRÁCTICA DE GESTIÓN: DS5DS.06 - GESTIONAR DOCUMENTOS SENSIBLES Y DISPOSITIVOS DE SALIDA

N°	Actividad	N°	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa.	75	Se ha establecido un procedimiento para la recepción de formularios especiales y dispositivos de salida?	25%	✓		
		76	Se ha establecido un procedimiento para el uso de formularios especiales y dispositivos de salida?	25%	✓		
		77	Se ha establecido un procedimiento para la eliminación de formularios especiales y dispositivos de salida?	25%	✓		
		78	Se ha establecido un procedimiento para la destrucción de formularios especiales y dispositivos de salida?	25%	✓		
2	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	79	Se han asignado privilegios de acceso a los documentos sensibles y dispositivos de salida considerando el riesgo?	50%	✓		
		80	Se han asignado privilegios de acceso a los documentos sensibles y dispositivos de salida considerando los requerimientos del negocio?	50%	✓		
3	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	81	Se ha establecido un inventario de documentos sensibles y dispositivos de salida?	50%		X	
		82	Se realiza conciliaciones del inventario de documentos sensibles y dispositivos de salida?	50%		X	
4	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos de salida.	83	Se ha establecido controles de seguridad físicos sobre los formularios especiales y dispositivos de salida?	100%	✓		
5	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes	84	La información contenida en los documentos o dispositivos sensibles es destruida de forma segura?	50%	✓		



	magnéticos, destruir físicamente dispositivos de memoria.	85	Se protege los dispositivos de salida de forma adecuada?	50%	✓		
PRÁCTICA DE GESTIÓN: DSS05.07 - SUPERVISAR LA INFRAESTRUCTURA PARA DETECTAR EVENTOS RELACIONADOS CON LA SEGURIDAD							
N°	Actividad	N°	PREGUNTA	Peso	SI	NO	OBSERVACIONES
1	Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	86	Los eventos relacionados con la seguridad reportados por las herramientas de monitoreo de infraestructura son registrados formalmente?	35%	✓		
		87	Se identifica información sensible que debe guardarse considerando el riesgo asociado?	35%	✓		
		88	La información obtenida es retenida por un periodo apropiado?	30%	✓		
2	Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta mensurada.	89	La naturaleza de los incidentes potenciales relacionados con la seguridad son definidos adecuadamente?	25%		X	
		90	Las características de los incidentes potenciales relacionados con la seguridad son definidos adecuadamente?	25%		X	
		91	La naturaleza de los incidentes potenciales relacionados con la seguridad es comunicada a todos los interesados?	25%	✓		
		92	Las características de los incidentes potenciales relacionados con la seguridad son comunicados a todos los interesados?	25%	✓		
3	Revisar regularmente los registros de eventos para detectar incidentes potenciales.	93	El registro de eventos relacionados con la seguridad es revisado regularmente?	100%	✓		
4	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	94	Se mantiene un procedimiento para la recopilación de evidencias en línea?	50%		X	
		95	Se asegura que el personal conoce los requerimientos para la recopilación de evidencias?	50%		X	
5	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	96	La creación de tickets de incidentes de seguridad se realiza en el momento que indica el sistema de monitoreo?	100%	✓		

5. Procesamiento de la evaluación de la capacidad del proceso DSS05 Gestionar los servicios de seguridad

INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 1: PROCESO EJECUTADO
ATRIBUTO: 1.1. RENDIMIENTO DEL PROCESO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

PRÁCTICA DE GESTIÓN: DSS05.01 - PROTEGER CONTRA SOFTWARE MALICIOSO									
N°	Actividad	Peso	Logrado		N°	PREGUNTA	Peso	SI	NO
1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención	15%	11%	70%	1	Se realiza concienciación sobre software malicioso en el personal?	30%	1	
					2	Existen procedimientos de prevención sobre software malicioso?	40%	1	
					3	Se ha asignado responsabilidades de prevención sobre software malicioso?	30%		
2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	25%	25%	100%	4	Se ha instalado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	30%	1	
					5	Se ha instalado herramientas de protección frente a software malicioso que se actualizan de forma automática o semiautomática	30%	1	
					6	Se ha activado herramientas de protección frente a software malicioso que contenga ficheros de definición de software malicioso	20%	1	
					7	Se ha activado herramientas de protección frente a software malicioso que se actualizan de forma automática o semiautomática	20%	1	
3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	15%	8%	50%	8	El software de protección contra software malicioso se distribuye de forma centralizada?	50%	1	
					9	El software de protección contra software malicioso se distribuye usando una configuración específica?	50%		
4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	10%	10%	100%	10	Se revisa la información sobre nuevas amenazas?	50%	1	
					11	Se evalúa la información sobre nuevas amenazas?	50%	1	

5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	20%	20%	100%	12	Se filtra el tráfico entrante para protección de software espía o correo de pishing?	100%	1	
6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	15%	8%	50%	13	Se realiza formación sobre software malicioso en el uso de correos electrónicos e internet?	50%		
					14	Se orienta a los usuarios a no instalar software compartido o no autorizado?	50%	1	
		100%	**81%**						
PRÁCTICA DE GESTIÓN: DSS05.02 - GESTIONAR LA SEGURIDAD DE LA RED Y LAS CONEXIONES									
N°	**Actividad**	**Peso**	**Logrado**		**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**
1	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	20%	20%	100%	1	Se ha establecido una Política de seguridad para las conexiones basado en análisis de riesgos?	50%	1	
					2	Se ha establecido una Política de seguridad para las conexiones basado en los requerimientos del negocio?	50%	1	
2	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	15%	15%	100%	3	El acceso a la información de la empresa está restringido solo para dispositivos autorizados?	30%	1	
					4	El acceso a la red de la empresa está restringido solo a dispositivos autorizados?	40%	1	
					5	Se ha configurado los dispositivos autorizados para solicitar contraseña antes del acceso ?	30%	1	
3	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	20%	20%	100%	6	Se ha implementado mecanismos de filtrado de red para el control del tráfico entrante y saliente?	100%	1	
4	Cifrar la información en tránsito de acuerdo con su clasificación.	5%	0%	0%	7	La información en tránsito por la red de la empresa está cifrada de acuerdo a su clasificación?	100%		
5	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	5%	5%	100%	8	Se ha aplicado protocolos de seguridad a las conexiones de red?	100%	1	
6	Configurar los equipos de red de forma segura.	10%	10%	100%	9	Los equipos que conforman la red están configurados de forma segura?	100%	1	
7	Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	5%	5%	100%	10	Se ha establecido mecanismo de confianza para la transmisión y recepción de la información?	100%	1	
8	Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	10%	0%	0%	11	Se realizan pruebas de intrusión para verificar la adecuación de la protección de la red?	100%		
9	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	10%	0%	0%	12	Se realizan pruebas de la seguridad del sistema para verificar la adecuación de la protección del sistema?	100%		
		100%	**75%**						
PRÁCTICA DE GESTIÓN: DSS05.03 - GESTIONAR LA SEGURIDAD DE LOS PUESTOS DE USUARIO FINAL									
N°	**Actividad**	**Peso**	**Logrado**		**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**
1	Configurar los sistemas operativos de forma segura.	10%	10%	100%	1	Los sistemas operativos de los puestos de usuario final están configurados de forma segura?	100%	1	
2	Implementar mecanismos de bloqueo de los dispositivos.	10%	10%	100%	2	Se ha implementado mecanismos de bloqueo en los dispositivos de usuario final?	100%	1	
3	Cifrar la información almacenada de acuerdo a su clasificación.	10%	0%	0%	3	La información almacenada en los dispositivos de usuario final está cifrada de acuerdo a a su clasificación?	100%		
4	Gestionar el acceso y control remoto.	10%	10%	100%	4	Se gestiona el acceso a los dispositivos de usuario final?	50%	1	
					5	Se gestiona el acceso remoto a los dispositivos de usuario final?	50%	1	
5	Gestionar la configuración de la red de forma segura.	10%	10%	100%	6	La configuración de la red de los dispositivos de usuario final se gestiona de forma segura?	100%	1	
6	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	10%	10%	100%	7	Se ha implementado filtros para el tráfico de la red en dispositivos de usuario final?	100%	1	
7	Proteger la integridad del sistema.	15%	0%	0%	8	Se ha implementado controles de seguridad para proteger la integridad del sistema en dispositivos de usuario final?	100%		

8	Proveer de protección física a los dispositivos de usuario final.	15%	0%	0%	9	Se ha implementado controles de seguridad física a los dispositivos de usuario final?	100%		
9	Deshacerse de los dispositivos de usuario final de forma segura.	10%	10%	100%	10	Se ha implementado un procedimiento para "dar de baja" a los dispositivos de usuario final que ya no están en funcionamiento?	100%	1	
		100%	**60%**						
PRÁCTICA DE GESTIÓN: DSS05.04 - GESTIONAR LA IDENTIDAD DEL USUARIO FINAL Y EL ACCESO LÓGICO									
N°	**Actividad**	**Peso**	**Logrado**		**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**
1	Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	15%	15%	100%	1	Los derechos de acceso de los usuarios se mantienen de acuerdo a los requerimientos de sus funciones?	40%	1	
					2	Los derechos de acceso de los usuarios se mantienen de acuerdo a los requerimientos de los procesos de negocio?	40%	1	
					3	La gestión de identidades y derechos de acceso se alinea con los roles y responsabilidades definidas para cada tipo de usuario?	20%	1	
2	Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.	15%	0%	0%	4		30%		
					5		35%		
					6		35%		
3	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	20%	20%	100%	7	Los accesos a los activos de información son autenticados según la clasificación de seguridad?	35%	1	
					8	Los accesos a los activos de información se coordinan con las unidades de negocio q las gestionan?	35%	1	
					9	Se asegura que los controles de autenticación son administrados adecuadamente?	30%	1	
4	Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	10%	7%	70%	10	Los cambios en los derechos de acceso son aprobados por gestores designados?	30%	1	
					11	Los cambios en los derechos de acceso son documentados?	30%		
					12	Los cambios en los derechos de acceso son autorizados por gestores designados?	40%	1	
5	Segregar y gestionar cuentas de usuario privilegiadas	5%	5%	100%	13	Las cuentas de usuario privilegiadas son segregadas?	40%	1	
					14	Las cuentas de usuario privilegiadas son gestionadas?	60%	1	
6	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	10%	10%	100%	15	Se realiza revisiones a las cuentas de usuarios y sus privilegios relacionados a intervalos regulares?	100%	1	
7	Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	15%	15%	100%	16	La identificación de los usuarios (internos, externos y temporales) se realiza de forma segura?	35%	1	
					17	La identificación de las actividades sobre los sistemas e infraestructura de TI que tiene cada usuario se realiza de forma segura?	35%	1	
					18	Las actividades sobre el procesamiento de información que tiene cada usuario se realiza de forma segura?	30%	1	
8	Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible	10%	0%	0%	19	Se mantiene una pista de auditoría de los accesos a la información clasificada como sensible?	100%		
		100%	**72%**						
PRÁCTICA DE GESTIÓN: DSS05.05 - GESTIONAR EL ACCESO FÍSICO A LOS ACTIVOS DE TI									
N°	**Actividad**	**Peso**	**Logrado**		**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**
1	Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las	15%	4%	25%	1	El acceso físico a las instalaciones de TI se realiza a través de peticiones formales que son revisadas por la dirección de TI?	25%		

	peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.				2	Se concede el acceso físico a las instalaciones de TI solo a las áreas que se solicitaron?	25%		
					3	El acceso físico a las instalaciones de TI es autorizado por la dirección de TI?	25%	1	
					4	Existe un registro de las peticiones formales realizadas a la dirección de TI?	25%		
2	Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	15%	8%	50%	5	Los perfiles de acceso físico a las instalaciones de TI están actualizados?	50%		
					6	El acceso físico a las instalaciones de TI se realiza en función al trabajo y responsabilidades?	50%	1	
3	Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	20%	14%	70%	7	Los puntos de entrada a las instalaciones de TI se encuentran en un registro formal?	35%	1	
					8	Los puntos de entrada a las instalaciones de TI son supervisados regularmente?	35%	1	
					9	Se lleva un registro del acceso a las instalaciones de TI de todos los visitantes (proveedores, vendedores)	30%		
4	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	10%	5%	50%	10	El personal que labora en las instalaciones de TI cuenta con tarjetas de identificación?	25%	1	
					11	Se capacita al personal que labora en las instalaciones de TI sobre el uso de la tarjeta de identificación?	25%	1	
					12	El personal que labora en las instalaciones de TI mantiene visible la tarjeta de identificación?	25%		
					13	Se previene la entrega de tarjetas de identificación sin autorización?	25%		
5	Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	10%	5%	50%	14	Las visitas autorizadas a ingresar a las instalaciones de TI son escoltadas en todo momento?	50%	1	
					15	Se alerta al personal de seguridad sobre la presencia de algún individuo que no porte la tarjeta de identificación?	50%		
6	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	20%	0%	0%	16	El acceso a las instalaciones de TI sensibles está restringido con controles de seguridad en el perímetro?	50%		
					17	Se verifica que los controles de seguridad en el perímetro restringen el acceso no autorizado?	25%		
					18	Se verifica que los controles de seguridad en el perímetro disparan una alarma en caso de acceso no autorizado?	25%		
7	Realizar regularmente formación de concienciación de seguridad física.	10%	10%	100%	19	Se capacita al personal que labora en las instalaciones de TI sobre seguridad física regularmente?	100%	1	
		100%	**45%**						

PRÁCTICA DE GESTIÓN: DSS05.06 - GESTIONAR DOCUMENTOS SENSIBLES Y DISPOSITIVOS DE SALIDA									
N°	**Actividad**	**Peso**	**Logrado**		**N°**	**PREGUNTA**	**Peso**	**SI**	**NO**
1	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa.	25%	25%	100%		Se ha establecido un procedimiento para la recepción de formularios especiales y dispositivos de salida?	25%	1	
						Se ha establecido un procedimiento para el uso de formularios especiales y dispositivos de salida?	25%	1	
						Se ha establecido un procedimiento para la eliminación de formularios especiales y dispositivos de salida?	25%	1	
						Se ha establecido un procedimiento para la destrucción de formularios especiales y dispositivos de salida?	25%	1	

2	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	20%	20%	100%		Se han asignado privilegios de acceso a los documentos sensibles y dispositivos de salida considerando el riesgo?	50%	1	
						Se han asignado privilegios de acceso a los documentos sensibles y dispositivos de salida considerando los requerimientos del negocio?	50%	1	
3	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	15%	0%	0%		Se ha establecido un inventario de documentos sensibles y dispostivos de salida?	50%		
						Se realiza conciliaciones del inventario de documentos sensibles y dispositivos de salida?	50%		
4	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos de salida.	25%	25%	100%		Se ha establecido controles de seguridad físicos sobre los formularios especiales y dispositivos de salida?	100%	1	
5	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).	15%	15%	100%		La información contenida en los documentos o dispositivos sensibles es destruida de forma segura?	50%	1	
						Se protege los dispositivos de salida de forma adecuada?	50%	1	
		100%	**85%**						

PRÁCTICA DE GESTIÓN: DSS05.07 - SUPERVISAR LA INFRAESTRUCTURA PARA DETECTAR EVENTOS RELACIONADOS CON LA SEGURIDAD

N°	Actividad	Peso	Logrado		N°	PREGUNTA	Peso	SI	NO
1	Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	25%	25%	100%		Los eventos relacionados con la seguridad reportados por las herramientas de monitoreo de infraestructura son registrados formalmente?	**35%**	1	
						Se identifica información sensible que debe guardarse considerando el riesgo asociado?	**35%**	1	
						La información obtenida es retenida por un periodo apropiado?	**30%**	1	
2	Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta mensurada.	25%	13%	50%		La naturaleza de los incidentes potenciales relacionados con la seguridad son definidos adecuadamente?	**25%**		
						Las características de los incidentes potenciales relacionados con la seguridad son definidos adecuadamente?	**25%**		
						La naturaleza de los incidentes potenciales relacionados con la seguridad es comunicada a todos los interesados?	**25%**	1	
						Las características de los incidentes potenciales relacionados con la seguridad son comunicados a todos los interesados?	**25%**	1	
3	Revisar regularmente los registros de eventos para detectar incidentes potenciales.	15%	15%	100%		El registro de eventos relacionados con la seguridad es revisado regularmente?	100%	1	
4	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	20%	0%	0%		Se mantiene un procedimiento para la recopilación de evidencias en línea?	50%		
						Se asegura que el personal conoce los requerimientos para la recopilación de evidencias?	50%		
5	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	15%	15%	100%		La creación de tickets de incidentes de seguridad se realiza en el momento que indica el sistema de monitoreo?	100%	1	
		100%	**68%**						

6. Instrumento de evaluación de la capacidad de procesos de TI del Nivel 2

INSTRUMENTO DE EVALUACIÓN DE CAPACIDAD DE PROCESOS
NIVEL 2: PROCESO GESTIONADO
PROCESO DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD

Atributo: 2.1. Gestión del rendimiento											
RESULTADO DE CUMPLIMIENTO			**PRÁCTICA GENÉRICA (GP) PRODUCTO DE TRABAJO GENÉRICO (GWP)**				**N°**	**PREGUNTA**	**PESO**	**SI**	**NO**
N°	**DESCRIPCIÓN**	**PESO**	**N°**	**TIPO**	**DESCRIPCIÓN**	**PESO**					
1	Los objetivos para el rendimiento del proceso están identificados.	20%	2.1.1.	GP	Identificar los objetivos para el rendimiento del proceso. Los objetivos de rendimiento, junto con los supuestos y limitaciones, están definidos y comunicados.	60%	1	Se ha definido los objetivos para el rendimiento del proceso?	25%		
							2	Se ha definido los supuestos para el rendimiento del proceso?	25%		
							3	Se ha definido las limitaciones para el rendimiento del proceso?	25%		
							4	Los objetivos, supuestos y limitaciones para el rendimiento del proceso fueron comunicados a los interesados?	25%		
			1.0	GWP	**Documentación del proceso**: debe describir el alcance del proceso.	20%	5	La documentación del proceso proporciona el alcance del proceso?	100%		
			2.0	GWP	**Plan del proceso:** debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	6	El plan del proceso proporciona los objetivos de rendimiento del proceso?	100%		
2	El rendimiento del proceso está planificado y monitorizado.	20%	2.1.2.	GP	Planificar y monitorizar el rendimiento del proceso para cumplir con los objetivos identificados. Medidas básicas de rendimiento de procesos vinculados a los objetivos de negocio están establecidas y monitorizadas. Incluyen hitos clave, actividades requeridas, estimaciones y planificaciones.	60%	7	Se ha planificado el rendimiento del proceso que permita cumplir con los objetivos?	35%		
							8	Se ha establecido medidas básicas de rendimiento (hitos, actividades, estimaciones)?	35%		
							9	Se monitorea el rendimiento del proceso para ver el cumplimiento de los objetivos?	30%		
			2.0	GWP	**Plan del proceso:** debe proporcionar detalles de los objetivos de rendimiento del proceso.	20%	10	El plan del proceso proporciona los objetivos de rendimiento del proceso?	100%		
			9.0	GWP	**Registros del desempeño del proceso:** deben proporcionar detalles de los resultados.	20%	11	Los registros de desempeño del proceso proporcionan los resultados del rendimiento del proceso?	100%		
3	El rendimiento del proceso está ajustado para satisfacer planes.	15%	2.1.3.	GP	Ajustar el rendimiento del proceso. Se llevan a cabo acciones cuando no se alcanza el rendimiento previsto. Las acciones incluyen la identificación de los problemas de rendimiento de proceso y ajuste de los planes y planificaciones, según proceda.	60%	12	Se ha identificado los problemas asociados al rendimiento del proceso?	35%		
							13	Se definen planes para ajustar el rendimiento del proceso?	35%		
							14	Se realizan las acciones planificadas para ajustar el rendimiento del proceso?	30%		
			4.0	GWP	**Registros de calidad:** deben dar detalles de las medidas adoptadas cuando no se alcanza el rendimiento.	40%	15	Los registros de calidad proporcionan las medidas adoptadas cuando no se alcanza el rendimiento del proceso?	100%		
4	Las responsabilidades y autoridades para llevar a cabo el proceso están definidas, asignadas y comunicadas.	15%	2.1.4.	GP	Definir las responsabilidades y autoridades para llevar a cabo el proceso. Las principales responsabilidades y autoridades para la realización de las actividades clave del proceso están definidas, asignadas y comunicadas. Las necesidades de experiencia del rendimiento del proceso, conocimientos y habilidades están definidas.	60%	16	Se ha definido el perfil (experiencia, conocimiento, habilidades) de los responsables de llevar a cabo el proceso?	35%		
							17	Se ha asignado las responsabilidades y niveles de autoridada las personas responsables de llevar a cabo el proceso?	35%		
							18	Se ha comunicado formalmente las asignaciones a las personas responsables de llevar a cabo el proceso?	30%		

			1.0	GWP	**Documentación del proceso:** debe proporcionar detalles sobre el propietario del proceso y quién es responsable, encargado, consultado y/o informado (RACI).	20%	19	La documentación del proceso proporciona información sobre el propietario del proceso y los roles definidos según la matriz RACI?	100%		
			2.0	GWP	**Plan del proceso:** debe incluir detalles del plan de comunicación de procesos, así como la experiencia de rendimiento del proceso, y requisitos de habilidades.	20%	20	El Plan del proceso proporciona el Plan de comunicaciones requerida para el proceso?	100%		
5	Los recursos y la información necesarios para llevar a cabo el proceso se han identificado, están disponibles, asignados y utilizados.	20%	2.1.5.	GP	Identificar y hacer que estén disponibles los recursos para llevar a cabo el proceso de acuerdo al plan. Los recursos e información necesarias para la realización de las actividades clave del proceso están identificados, disponibles, asignados y utilizados.	60%	21	Se ha identificado los recursos necesarios para llevar a cabo el plan del proceso?	35%		
							22	Los recursos identificados están disponibles para cuando el proceso los requiera?	35%		
							23	Los recursos son utilizados de acuerdo al plan del proceso para el cumplimiento de los objetivos?	30%		
			2.0	GWP	**Plan del proceso:** debe proporcionar detalles del plan de formación y el plan de recursos de procesos.	40%	24	El plan del proceso proporciona el plan de recursos del proceso?	50%		
							25	El Plan del proceso proporciona el plan de formación para el recurso humano del proceso?	50%		
6	Las interfaces entre las partes involucradas están gestionadas para garantizar una comunicación eficaz y una clara asignación de responsabilidades.	10%	2.1.6.	GP	Gestionar las interfaces entre las partes involucradas. Las personas y los grupos que participan en el proceso están identificadas, las responsabilidades están definidas y los mecanismos eficaces de comunicación están en marcha.	60%	26	Se ha identificado a las partes interesadas (personas y grupos) del proceso?	35%		
							27	Se ha definido las responsabilidades para las partes interesadas del proceso?	35%		
							28	Se ha establecido mecanismos de comunicación eficaces para las partes interesadas del proceso?	30%		
			1.0	GWP	**Documentación del proceso:** debe proporcionar detalles de las personas y grupos involucrados (proveedores, clientes y RACI).	20%	29	La documentación del proceso proporciona las partes interesadas y sus responsabilidades?	100%		
			2.0	GWP	**Plan del proceso:** debe proporcionar detalles sobre el plan de comunicación de procesos.	20%	30	El Plan del proceso proporciona el plan de comunicación para las partes interesadas?	100%		

Atributo: 2.2. Gestión del resultado de trabajo

RESULTADO DE CUMPLIMIENTO			PRÁCTICA GENÉRICA (GP) PRODUCTO DE TRABAJO GENÉRICO (GWP)				N°	PREGUNTA	PESO	SI	NO
N°	DESCRIPCIÓN	PESO	N°	TIPO	DESCRIPCIÓN	PESO					
1	Los requisitos para los productos de trabajo del proceso están definidos.	25%	2.2.1.	GP	Definir los requisitos para los resultados de trabajo, incluyendo la estructura de contenidos y criterios de calidad.	60%	1	Se ha definido requisitos para los productos de trabajo?	35%		
							2	Se ha definido la estructura para el contenido de los productos de trabajo?	35%		
							3	Se ha definido los criterios de calidad de los productos de trabajo?	30%		
			3.0	GWP	**Plan de calidad:** debe proporcionar detalles de los criterios de calidad y contenido de los productos de trabajo y la estructura.	40%	4	El plan de calidad proporciona los requisitos, estructura y criterios de calidad de los productos de trabajo en el plan de calidad?	100%		
2	Los requisitos para la documentación y el control de los productos de trabajo están definidos.	25%	2.2.2.	GP	Definir los requisitos de documentación y control de los resultados de trabajo. Esto debe incluir la identificación de las dependencias, aprobaciones y trazabilidad de requisitos.	60%	5	Se ha definido los requisitos de documentación de los productos de trabajo del proceso?	50%		
							6	Se ha definido los requisitos de control de los productos de trabajo del proceso?	50%		

			1.0	GWP	**Documentación del proceso:** debe proporcionar detalles de los controles (matriz de control).	20%	7	La documentación del proceso proporciona los controles de los productos del trabajo (matriz de control)?	100%		
			3.0	GWP	**Plan de calidad:** debe proporcionar detalles de los resultados de trabajo, criterios de calidad, los requisitos de documentación y control de cambios.	20%	8	El plan de calidad proporciona los criterios de calidad, requisitos de documentación y control de cambios de los productos de trabajo?	100%		
3	Los resultados de trabajo estén debidamente identificados, documentados y controlados.	30%	2.2.3.	GP	Identificar, documentar y controlar los resultados de trabajo. Los resultados de trabajo están sujetos al control de cambios, control de versiones y la gestión de la configuración según corresponda.	60%	9	Se ha identificado los productos de trabajo del proceso?	35%		
							10	Se ha documentado los productos de trabajo del proceso?	35%		
							11	Se controlan los productos de trabajo (cambios, versiones) del proceso?	30%		
			3.0	GWP	**Plan de calidad:** debe proporcionar detalles de los resultados de trabajo, criterios de calidad, los requisitos de documentación y control de cambios.	40%	12	El plan de calidad proporciona los criterios de calidad, requisitos de documentación y control de cambios de los productos de trabajo?	100%		
4	Los resultados de trabajo son revisados de acuerdo con las disposiciones planificadas y ajustados si es necesario para cumplir con los requisitos.	20%	2.2.4.	GP	Revisar y ajustar los resultados de trabajo para cumplir con los requisitos definidos. Los resultados de trabajo están sujetos a revisiones contra de los requisitos según acuerdos planificaciones y cualquier problema que surja, siendo resueltos.	60%	13	Se revisan los productos de trabajo para cumplir con los requisitos definidos?	50%		
							14	Se ajustan los productos de trabajo resolviendo cualquier problema para cumplir con los requisitos definidos?	50%		
			4.0	GWP	**Registros de calidad:** deben proporcionar una pista de auditoría de la revisiones realizadas.	40%	15	El registro de calidad proporciona una pista de auditoríade las revisiones?	100%		