ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

MODELO DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN EN LOS PROCESOS CRÍTICOS DE LAS ÁREAS FINANCIERAS UNIVERSITARIAS. CASO PUCE

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGISTER EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

YOLANDA CECILIA GARCÍA PAREDES
ygarciap@gmail.com

DIRECTOR: ING. ROSA DEL CARMEN NAVARRETE RUEDA MSc.
rosa.navarrete@epn.edu.ec

Quito, Mayo 2015

DECLARACIÓN

Yo, Yolanda Cecilia García Paredes, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Yolanda Cecilia García Paredes

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Yolanda Cecilia García Paredes, bajo mi supervisión.

MSc. Rosa Navarrete R.
DIRECTORA DE PROYECTO

AGRADECIMIENTO

Al cielo, a mi familia y a los seres queridos que me han apoyado con su compañía y su bondad, convirtiéndose en un estímulo para mí.

A mi directora de tesis, MSc. Rosa Navarrete Rueda por su invaluable ayuda y compromiso con mi trabajo.

A mi profesor, MSc. Jaime Naranjo por su guía y su mano amiga a lo largo del camino.

A mis profesores lectores, MSc. Andrés Larco y MSc. Bolívar Palán, por su guía en este proceso.

Yolanda García Paredes

DEDICATORIA

A mi hija Sofía, le dedico mi esfuerzo como muestra del profundo anhelo que tengo de verla seguir siempre adelante con tenacidad y perseverancia, a pesar de las adversidades de la vida y de las circunstancias que debamos superar.

Yolanda García Paredes

CONTENIDO

CAPÍTULO 1 ESTADO DEL ARTE 14
1.1 SEGURIDAD DE LA INFORMACIÓN - GENERALIDADES 14
1.2 INFORMACIÓN FINANCIERA Y PROCESOS CRÍTICOS 15
1.2.1 POLÍTICAS SOBRE FINANCIAMIENTO UNIVERSITARIO 15
1.2.2 FUENTES DE FINANCIAMIENTO 15
1.2.3 GESTIÓN FINANCIERA 16
1.2.4 CALIDAD EDUCATIVA Y PROCESOS 16
1.3 ESTÁNDARES Y NORMAS INTERNACIONALES PARA SEGURIDAD DE LA INFORMACIÓN – MEJORES PRÁCTICAS 17
1.3.1 COBIT 18
1.3.2 OCTAVE 19
1.3.3 MAGERIT 19
1.3.4 ISO/IEC 31000 20
1.3.5 ITIL 21
1.3.6 COSO 22
1.3.7 ISO 27000 23
CAPÍTULO 2 DISEÑO DEL MODELO DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN FINANCIERA DE LA PUCE 24
2.1 LEVANTAMIENTO DE INFORMACIÓN 24
2.1.1 ORGANIZACIÓN 24
2.1.2 PLANIFICACIÓN INSTITUCIONAL 26
2.1.3 AUDITORIA INTERNA 27
2.1.3 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN 28
2.1.4 GESTIÓN DE TI E INFRAESTRUCTURA TECNOLÓGICA 30
2.1.5 ÁREA FINANCIERA DE LA INSTITUCIÓN 33
2.2 DETERMINACIÓN DE PROCESOS CRÍTICOS 41
2.3 IDENTIFICACIÓN DE RIESGOS 44
2.4 COMPARATIVA DE NORMAS Y MODELOS 48
2.4.1 ANÁLISIS DEL MARCO DE REFERENCIA COBIT 5.0 50
2.4.2 ANÁLISIS DE LA NORMA ISO/IEC 31000 56

2.4.3 SELECCIÓN DEL MARCO DE REFERENCIA Y NORMA PARA EL DISEÑO DEL MODELO. INTEGRACIÓN DE ISO/IEC 31000 Y COBIT 5 60
2.5 DESARROLLO DE PROPUESTA DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MGSI-PUCE-DGF 62
2.5.1 MOTIVO DE LAS PARTES INTERESADAS 63
2.5.2 NECESIDADES DE LAS PARTES INTERESADAS 64
2.5.3 METAS INSTITUCIONALES 67
2.5.4 METAS RELACIONADAS CON TI 69
2.5.5 METAS DE LOS CATALIZADORES 70
CAPÍTULO 3 RESULTADOS Y DISCUSIÓN 91
3.1 ADAPTACIÓN DEL MODELO PROPUESTO EN UN PROCESO CRÍTICO DEL ÁREA FINANCIERA 91
3.1.1 SELECCIÓN DEL PROCESO CRÍTICO 91
3.1.2 PROCESO DE EVALUACIÓN PRESUPUESTARIA 92
3.1.3 EVALUACIÓN DEL RIESGO 100
3.1.4 TRATAMIENTO, SEGUIMIENTO Y REVISIÓN DEL RIESGO 108
3.2 DETERMINACIÓN DEL APORTE DEL MODELO 114
3.3 PROPUESTA DE ESTRATEGIAS DE IMPLEMENTACIÓN DEL MODELO 114
CAPÍTULO 4 CONCLUSIONES Y RECOMENDACIONES 118
4.1 CONCLUSIONES 118
4.2 RECOMENDACIONES 119
REFERENCIAS BIBLIOGRÁFICAS 120
ANEXOS 122

ÍNDICE DE ILUSTRACIONES

Ilustración 1-1. Principios de COBIT 5 18
Ilustración 1-2. Procesos de Octave 19
Ilustración 1-3. Elementos de análisis de riesgos potenciales con MAGERIT 20
Ilustración 1-4. Proceso de Gestión de riesgos ISO 31000 21
Ilustración 1-5. Fundamentos de la Gestión con ITIL 21
Ilustración 1-6. Modelo interno de Control de Coso 22
Ilustración 1-7. Modelo interno ISO 27000 23
Ilustración 2-1. PUCE – Organigrama estructural de la PUCE 25
Ilustración 2-2. Proyectos 2015 Dirección General Financiera 27
Ilustración 2-3. BAAN – Creación de usuarios – datos del sistema 38
Ilustración 2-4. BAAN – Asignación de roles 38
Ilustración 2-5. BAAN – Convertir usuario BAAN en usuario BD 39
Ilustración 2-6. BAAN - Asignación de permisos de sesión y tablas a roles 41
Ilustración 2-7. Catalizadores de COBIT 5 50
Ilustración 2-8. Áreas clave de Gobierno y Administración COBIT 5 51
Ilustración 2-9. Dominios de COBIT 52
Ilustración 2-10. Procesos para la gestión de TI empresarial 53
Ilustración 2-11. Visión general de la cascada de metas de COBIT 5 54
Ilustración 2-12. Meta corporativa y su relación con los objetivos de gobierno de COBIT 5 54
Ilustración 2-13. Metas relacionadas con TI COBIT 5 55
Ilustración 2-14. Mapeo entre metas corporativas y metas relacionadas con TI. COBIT 5 55
Ilustración 2-15. Modelo Capacidad de procesos COBIT 5 56
Ilustración 2-16. Arquitectura ISO/IEC 31000 57
Ilustración 2-17. Cobertura de COBIT 5 de otros estándares y marcos de referencia 60
Ilustración 2-18. Integración COBIT 5 e ISO 31000 61
Ilustración 2-19. MGSI – PUCE (Dimensión Financiera) 63
Ilustración 2-20. MGSI–PUCE Necesidades de las partes interesadas 65
Ilustración 2-21. MGSI–PUCE Metas corporativas 68
Ilustración 2-22. MGSI–PUCE Metas relacionadas con TI 69
Ilustración 2-23. MGSI–PUCE Metas de los catalizadores 71
Ilustración 2-24. MGSI–PUCE Procesos 72
Ilustración 2-25. Ciclo de vida de la gestión del riesgo 77
Ilustración 2-26. Dirección General Financiera - Ciclos de requerimiento y respuesta 79
Ilustración 3-1. Dir. Presupuestos - Ciclos de requerimiento y respuesta 94
Ilustración 3-2. PR4200 – Proceso de evaluación presupuestaria 95
Ilustración 3-3. BAAN – Presupuestos – Maestro de dimensiones 96

Ilustración 3-4. BAAN – Presupuestos – Mantener transferencia de presupuestos 97
Ilustración 3-5. Estrategia de implementación de MGSI-PUCE-DGF 115

ÍNDICE DE TABLAS

Tabla 2-1. Roles en ERP BAAN 5.0 para la PUCE 39
Tabla 2-2. Procesos internos del área financiera documentados en BAAN 42
Tabla 2-3. Identificación de riesgos y vulnerabilidad financiera en función de recursos de TI institucional 45
Tabla 2-4. Comparativa entre marcos de referencia y modelos de seguridad de información 49
Tabla 2-5. Descripción de procesos COBIT adaptados al MGSI-PUCE-DGF 73
Tabla 2-6. Comparación modelos de madurez COBIT 4.0 y 5.0 74
Tabla 2-7. Nivel de madurez y medición de un proceso 75
Tabla 2-8. Inventario de factores internos y externos en relación al riesgo 80
Tabla 2-9. Determinación de los criterios del riesgo 81
Tabla 2-10. Preguntas orientadoras para identificar riesgos 82
Tabla 2-11. Análisis de riesgos 83
Tabla 2-12. Matriz para evaluación de riesgos 84
Tabla 2-13. Plan de tratamiento y seguimiento de riesgos 86
Tabla 2-14. Roles y estructuras PUCE en relación a TI y al área financiera 87
Tabla 3-1. Identificación de procesos críticos financieros a través de informantes 91
Tabla 3-2. Nivel de madurez del proceso EDM03 – Asegurar la optimización del riesgo 98
Tabla 3-3. Nivel de madurez del proceso APO13 – Definir, operar y supervisar un sistema para la gestión de seguridad de información. 99
Tabla 3-4. Preguntas orientadoras para identificar riesgos en el proceso crítico seleccionado 101
Tabla 3-5. Análisis del riesgo financiero institucional 101
Tabla 3-6. Análisis del riesgo de toma de acciones preventivas y correctivas 102
Tabla 3-7. Análisis del riesgo de acceso no controlado a la información confidencial 102
Tabla 3-8. Análisis del riesgo de pérdida de información para toma de decisiones 103
Tabla 3-9. Matriz para evaluación del riesgo financiero institucional 104
Tabla 3-10. Matriz para evaluación del riesgo de toma de acciones preventivas y correctivas 105
Tabla 3-11. Matriz para evaluación del riesgo de acceso no controlado a la información confidencial 106
Tabla 3-12. Matriz para evaluación del riesgo de pérdida de información para 107
Tabla 3-13. Plan de tratamiento y seguimiento del riesgo financiero institucional del proceso de evaluación presupuestaria 108
Tabla 3-14. Plan de tratamiento y seguimiento del riesgo de toma de acciones preventivas y correctivas del proceso de evaluación presupuestaria 109

Tabla 3-15. Plan de tratamiento y seguimiento del riesgo de acceso no controlado a la información confidencial del proceso de evaluación presupuestaria 110
Tabla 3-16. Plan de tratamiento y seguimiento del riesgo de pérdida de información para toma de decisiones del proceso de evaluación presupuestaria 111
Tabla 3-17. Relación proceso críticos financiero versus procesos de TI relacionados 112

RESUMEN

Las instituciones educativas buscan fortalecer sus procesos administrativos consolidando de mejor manera los recursos de los que dispone, teniendo siempre como meta, poder tomar decisiones acertadas y oportunas. El área financiera de cualquier institución es considerada una unidad de apoyo a la gestión académica y sobre ella recae la administración económica que conlleva un manejo sensible de información.

Continuamente se están desarrollando nuevos y mejores métodos para comprometer la seguridad de la información, considerada actualmente un activo importante en las instituciones y es por ello que es necesario contar con una estrategia que permita prevenir y minimizar vulnerabilidades internas y externas, y el instrumento idóneo para ello es desarrollar un modelo de gestión de seguridad informática orientado al área específica de análisis, de una manera holística, considerando el sistema financiero con el que cuenta y las particularidades de sus procesos internos.

Existen normas y herramientas que permiten cubrir todas las funciones y procesos dentro una organización de una manera integral y no se enfoca exclusivamente en la función de TI; ello trae como resultado que se puedan abordar de mejor manera aquellos procesos críticos dentro de una institución, considerando tanto a la información como a las tecnologías como activos de la institución. Sin embargo, ninguna norma se puede aplicar de manera efectiva en ciertas áreas; es necesario recurrir a cierta especialización construyendo modelos definidos para ello.

El siguiente trabajo propone un modelo de gestión de seguridad de información acorde a las políticas institucionales, con una visión integradora sobre las necesidades de seguridad de la Dirección General Financiera, a través de una adaptación técnica minimizando las deficiencias de los modelos escogidos en combinación con las fortalezas de otros.

PRESENTACIÓN

El siguiente trabajo consiste en una propuesta de un modelo de gestión de seguridad de información en las áreas financieras universitarias.

En el primer capítulo se aborda el marco conceptual que permitirá al lector entender el concepto de seguridad de información, la dinámica de una institución universitaria en términos de su gestión financiera, y sobre la calidad educativa y procesos relacionados.

Adicionalmente se mencionar algunos marcos de referencia y normas existentes sobre seguridad de la información, de una manera condensada.

En el segundo capítulo se identifican tres secciones desarrolladas: Primeramente se documenta el levantamiento de información y diagnóstico inicial realizado en la Pontificia Universidad Católica del Ecuador, matriz, que es el sitio que se propone como caso para el diseño del modelo. La segunda sección parte de la información orientadora del primera sección con la finalidad de permitir sustentar y elegir un marco de referencia y un modelo que se ajusten de mejor manera a la institución. En la tercera sección se diseña el modelo de gestión de seguridad de información personalizado para la Universidad basado en COBIT 5.0 acoplado con ISO/IEC 31000.

En el tercer capítulo se documenta un pilotaje realizado en un proceso crítico del área financiera complementando la comprensión y entendimiento del modelo y el acoplamiento adoptado. Se determina el aporte del modelo hacia la institución y se propone una estrategia de implementación.

Finalmente se documentan las conclusiones y recomendaciones más relevantes producto de la realización del trabajo.

CAPÍTULO 1
ESTADO DEL ARTE

1.1 SEGURIDAD DE LA INFORMACIÓN - GENERALIDADES

Las instituciones educativas han estado constantemente buscando calidad y excelencia en sus procesos administrativos y académicos con la finalidad de desarrollarse y evolucionar conforme a su estado de madurez, a su adaptabilidad a los cambios y al dinamismo desarrollado.

Actualmente el mejoramiento de la gestión administrativa ha recobrado impulso, por el proceso de evaluación realizado por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES) a través del Modelo de Evaluación Institucional y de Carreras considerando los criterios de Organización e Infraestructura, que dan cuenta de una variedad de indicadores cuyos planes de mejora recaen insistentemente en lograr eficiencia en varios procesos.

Para alcanzar los objetivos de calidad se hace necesario contar con técnicas, herramientas y metodologías que permitan lograrlo y sostenerlo en el tiempo a través de mejoras constantes; el análisis de cuáles son las mejores herramientas dentro de una institución universitaria conlleva a un análisis profundo de la organización como tal, de sus procesos críticos y de la identificación de vulnerabilidades.

Dentro de la gestión de seguridad hay que considerar las tareas de análisis y gestión de riesgos y que habitualmente forman parte de la actividad continua de dicha gestión.

La información en cualquier organización constituye actualmente un recurso clave. La tecnología juega un rol clave en la creación, uso, retención, divulgación y destrucción de la información que se genera. Es por ello que la tecnología es ahora parte integral de todos los aspectos de la organización.

Las organizaciones se esfuerzan para lograr que la tecnología brinde un soporte para apoyar las decisiones y logar metas estratégicas, minimizando el riesgo que se pueda generar con ella; para ello se requiere de una correcta definición de gobierno y de una correcta administración de los activos de TI y de la información.

Es un requisito fundamental para las instituciones lograr una buena coordinación en el área de tecnología y alinearla con la estrategia institucional a través del gobierno de TI y del afinamiento de procesos y su consecuente revisión y toma de decisiones con respecto a la gestión de riesgos y seguridad de información

1.2 INFORMACIÓN FINANCIERA Y PROCESOS CRÍTICOS

Varios son los aportes y análisis acerca de los procesos universitarios, desde investigaciones puntuales hasta aquellas consideradas dentro de los modelos de evaluación y acreditación universitaria.

A continuación se hace un análisis y adaptación derivados de una importante investigación académica y de la normativa ecuatoriana acerca de la gestión estratégica financiera en las instituciones de educación superior, sin dejar de lado los aportes que se han hecho en varias publicaciones de tesis enfocados a la mejora de procesos de organizaciones. Estos trabajos han sido realizados en su gran mayoría por estudiantes de las áreas de administración y auditoría. [1]

1.2.1 POLÍTICAS SOBRE FINANCIAMIENTO UNIVERSITARIO

En el Ecuador y otros países de la región, es indispensable la presencia del Estado a través de una política pública que a la vez sea coherente con la importancia de apoyar a la educación en todos los niveles.

El estado financia en mayor o menor grado a las universidades con el fin de mejorar la calidad académica a través de eficacia y eficiencia. En contraste, las universidades perciben que esta asignación afecta y resta autonomía a la institución.

Existe una tendencia en reducir la asignación estatal a las universidades, sin embargo, la demanda educativa no ha disminuido y ello puede provocar un desequilibrio financiero. Es importante apoyar la planeación de la acción universitaria para poder buscar soluciones a los desequilibrios financieros.

1.2.2 FUENTES DE FINANCIAMIENTO

Las fuentes de financiamiento a las que pueden acceder las universidades son:

- Aporte fiscal.- Actualmente en el Ecuador está apuntado a financiar actividades específicas tales como proyectos de investigación y becas, dejando por fuera las práctica de utilizar esta fuente para infraestructura por ejemplo.
- Arancel de matrícula.- Los aranceles de los estudiantes generalmente se destinan a cubrir los costos relacionados directamente con la actividad académica. Se han implementado fórmulas para aplicar políticas de becas o matrículas diferenciadas basadas en la condición socio-económica del estudiante y su entorno familiar.
- Asignación de fondos.- Este fondo llega a las universidades a través de convenios con el sector privado o fundaciones a través de una vinculación con ciertos sectores.

- Donaciones.- Es posible establecer lazos con sectores privados o grupos con enlaces fuertes en la vida de la institución para poder percibir donaciones como otra forma de fuente de financiamiento.
- Empresas universitarias.- Es una práctica que permite tener una fuente de ingresos válida, en la medida que el costo de oportunidad de tenerlas justifique su existencia, dado que la razón de ser de una universidad es la educación.

1.2.3 GESTIÓN FINANCIERA

El estilo de la gestión financiera depende del tipo de institución, de su estructura, legislación, misión, visión por lo que no se puede establecer un solo estilo de gestión que calce a todas las universidades.

Generalmente la gestión financiera, cualquiera sea el tipo de institución, tiene a centralizase en el gobierno de la universidad, práctica que deja por fuera tareas y responsabilidades institucionales.

Una estrategia para alcanzar la eficiencia de la gestión financiera, es importante fortalecer el proceso de autoanálisis de tal manera que se puedan establecer criterios de calidad internos, medirlos y alcanzarlos.

La tendencia para mejorar la calidad sugiere la descentralización de la decisión y la gestión y la centralización.

Deben establecerse indicadores de calidad que permitan tender al mejoramiento continuo de la universidad. Sólo la calidad del servicio educativo puede ser una garantía para contar con alumnos, proyectos, investigación, servicios, influencia y proposiciones creíbles en el medio externo.

1.2.4 CALIDAD EDUCATIVA Y PROCESOS

Mucho se ha hablado de la calidad y excelencia educativa. El propósito de la acreditación universitaria es promover y estimular el continuo mejoramiento y determinar si una institución posee calidad a nivel general o respecto a sus carreras y programas, y si su mejora es continua de acuerdo a los criterios de calidad establecidos.

El estado cuenta con organismos destinados a elaborar instrumentos de evaluación así como evaluar el resultado de las instituciones haciendo uso de indicadores cuantitativos en su mayoría que proporcionan una información incompleta y que por lo general no permiten medir correctamente el estado mismo de la educación universitaria.

Por otro lado están los procesos que permiten gestionar el valor agregado institucional en varios ámbitos. Es a través de los procesos, su calidad y las

relaciones entre ellos insumos que se puede observar y medir si la organización universitaria responde a su misión y a sus principios de excelencia y calidad.

Los macro procesos claves dentro de cualquier universidad son dos:

- Docencia.
- Investigación.

Los macro procesos se desarrollan en fases (Planificación, ejecución y evaluación) cuya correcta aplicación se pueden entender desde el enfoque de mejora continua.

Dentro de las áreas financieras los procesos fundamentales son los siguientes:

- El proceso de planificación.
- El proceso contable.
- El proceso de análisis, seguimiento y evaluación.

Las actividades críticas están relacionadas con:

- Elaboración y cumplimiento del presupuesto anual de la universidad.
- Elaboración de los Estados Financieros para su presentación ante las entidades de control.
- Control Tributario.
- Manejo de Tesorería.
- Proceso de cobranza de aranceles y matrículas.
- Control desembolso a proveedores.

1.3 ESTÁNDARES Y NORMAS INTERNACIONALES PARA SEGURIDAD DE LA INFORMACIÓN – MEJORES PRÁCTICAS

Existen varias metodologías y estándares internacionales que permiten cubrir temas como la confidencialidad, integridad y disponibilidad de recursos abordando la seguridad de la información y la gestión de riesgos como su pilar principal; entre ellos se han escogido las siguientes referencias toda vez que permiten medir con mayor o menor grado de dificultad procesos en áreas financieras.

ISO 17.779, 27000, que son estándares para la administración de seguridad información; ISO 31000 que está diseñado para evaluar la gestión de riesgos y su complemento ISO 31010; COBIT que hacer referencia a la gobernabilidad, control, información entre otras, ITIL que es una norma sobre las mejores prácticas para la administración de servicios de TI; COSO que está orientada a la administración financiera y contable de las organizaciones; OCTAVE que permite hacer análisis de riesgo informático desde el riesgo organizacional; LEY SOX [2] que obliga a la administración financiera a llevar un control de su actividad, entre

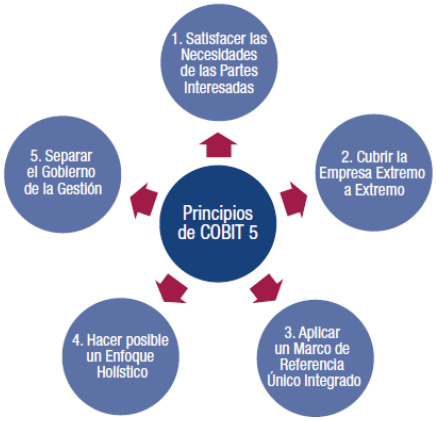
otros, todos y cada uno de ellos con sus fortalezas y debilidades. Una visión más amplia de cada uno de los citados, se explica a continuación:

1.3.1 COBIT

COBIT (Control Objectives for Information and Relative Technologies) es el marco de referencia de mayor difusión a nivel empresarial. En su versión 5.0 une los 5 principios claves: satisfacer las necesidades de las partes interesadas, cubrir la organización de forma integral, aplicar un solo marco integrador, habilitar un enfoque holístico, separar el gobierno de la administración, como se puede apreciar en el siguiente gráfico: además, busca complementar su enfoque de manera holística integrando 7 categorías de catalizadores o habilitadores: políticas, procesos, estructuras organizativas, cultura, información, servicios, personas.

Separa los procesos de responsabilidad del gobierno de los procesos relativos a la gestión, debido a que en la mayoría de organizaciones el gobierno e responsabilidad del consejo administrativo y la gestión es responsabilidad de la dirección ejecutiva [3].

Ilustración 1-1. Principios de COBIT 5



Fuente: COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa,2012

Durante los últimos 20 años las empresas y organizaciones a nivel mundial han utilizado COBIT para mejorar y evaluar sus procesos de TI, sin embargo, no es sino hasta la llegada el programa de evaluación, guías para asesores y guías de autoevaluación que ofrece ISACA, que fueron lanzados con COBIT 4 y que se ha integrado a COBIT 5, a principios del 2012.

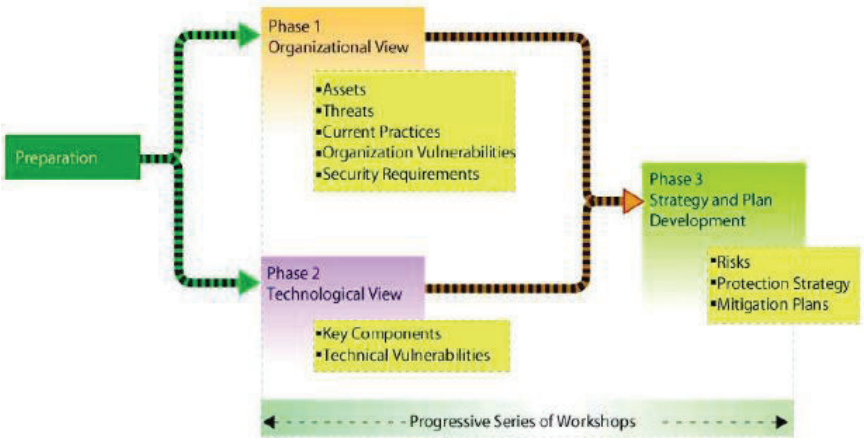
Actualmente en el Ecuador se ofrecen cursos y asesorías para la implementación de COBIT 5. El Instituto de Auditores Internos ofrece capacitaciones permanentes.

1.3.2 OCTAVE

Es considerada una técnica en seguridad y se basa en el riesgo; se diferencia de otras técnicas porque se enfoca en el riesgo organizacional, la estrategia y la práctica misma llevada a cabo en la empresa.

Dispone de tres métodos de implementación, y ellos se basan en criterios con enfoque en la práctica y evaluación basada en la información del riesgo [4]. El siguiente gráfico permite visualizar el proceso usado por Octave.

Ilustración 1-2. Procesos de Octave



Fuente: Fluidsignal, 2007

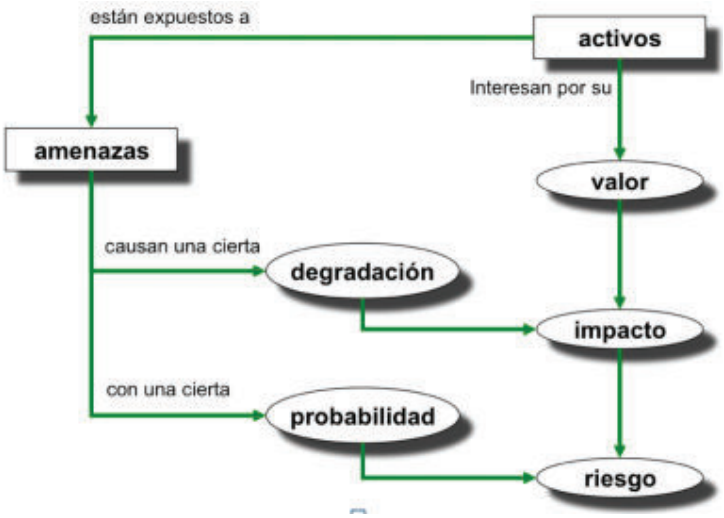
El uso de Octave en el país ha sido referenciado hasta el año 2013 en el Ecuador. Al dividir a los activos únicamente en Sistemas y personas y por concentrarse en la seguridad informática sin contemplar una verdadera relación con la organización, esta técnica ha ido perdiendo soporte.

1.3.3 MAGERIT

Es una metodología promocionada por el gobierno español, y propone la generalización del uso de los medios electrónicos, informáticos y telemáticos, para minimizar los riesgos con medidas de seguridad que generen confianza en el uso de los medios tecnológicos [6].

Se basa en la gestión de riesgos estructurada en las normas ISO 31000.

Ilustración 1-3. Elementos de análisis de riesgos potenciales con MAGERIT



Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1- Método

Esta metodología es una de las más referenciadas a nivel de latinoamérica por la facilidad del idioma en el que se produce. Existen referencias sobres los tres submodelos que la componen y son: Elementos, Eventos y Procesos.

1.3.4 ISO/IEC 31000

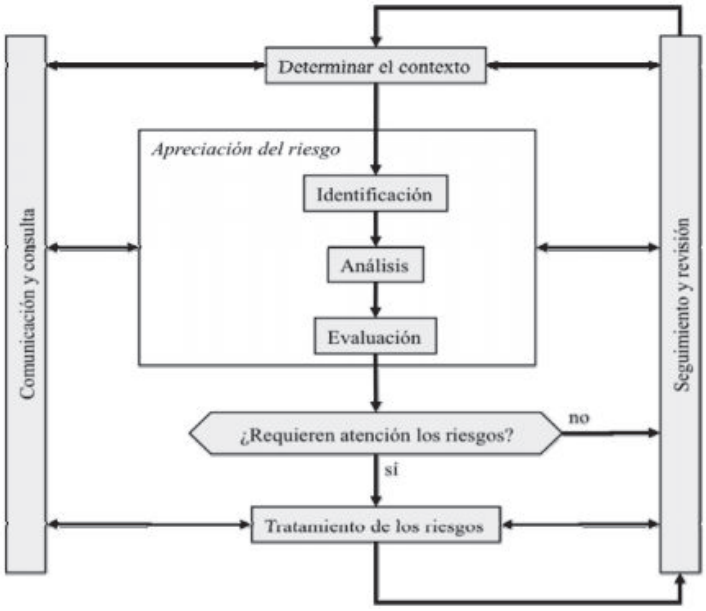
Desarrollada en el año 2009, proporciona principios y directrices genéricas sobre la gestión de riesgos y resulta interesante porque puede aplicarse a cualquier sector, en su totalidad o en un área, en un proyecto o en una actividad. Por estas características se ha convertido en un referente de nivel mundial.

Adicionalmente se adapta de manera interesante al nivel de madurez de la institución indistintamente de su tamaño o tipo con el fin de desarrollar, aplicar y mejorar continuamente sus procesos. Si los niveles son bajos proporciona lineamientos para ordenarse y si son altos proporciona guías para analizar las prácticas que se están llevando a cabo [7].

Es una recomendación en esta normativa que antes del proceso de gestión de riesgo se establezca un contexto de la institución con el fin de identificar los objetivos estratégicos, su ambiente y consecuentemente los criterios de riesgo.

El enfoque descrito en esta norma contempla los principios y directrices para gestionar varios tipos de riesgos. Su arquitectura se presenta a continuación:

Ilustración 1-4. Proceso de Gestión de riesgos ISO 31000

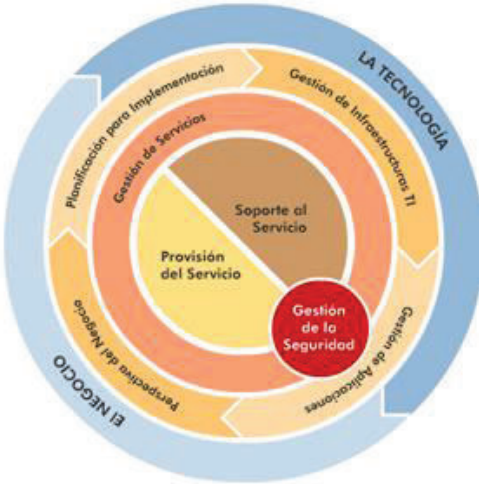


Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1- Método

1.3.5 ITIL

ITIL (Information Technology Infraestructure Library) es un marco de trabajo sobre las mejores prácticas para la administración de servicios de TI en el tema de servicios especialmente para hacerlos de alta calidad, a través de procedimientos que sirven de guía a las instituciones que lo aplican [8].

Ilustración 1-5. Fundamentos de la Gestión con ITIL



Fuente: Econocom-Osiatis, ITIL-Gestión de Servicios TI

Como marco de referencia, ITIL se creó como un modelo para la administración de servicios de TI e incluye información sobre metas, actividades, entradas y salidas de procesos. La versión 3.0 consta de 5 libros que giran alrededor del ciclo de vida del servicio.

Están disponibles 4 niveles de certificación que son ofertados por los proveedores de servicios de seguridad de TI.

1.3.6 COSO

COSO (Committee of Sponsoring Organizations of the Treadway Commission) es el estándar de referencia que contiene directivas para la implantación, gestión y control de un sistema de control dentro de una organización y que consta de los siguientes componentes [10]:

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Supervisión y seguimiento de control, y los aborda como procesos multidireccionales repetitivos y permanentes.

Ilustración 1-6. Modelo interno de Control de Coso

Fuente: Experiencias de auditoría informática - Modelo COSO

En Ecuador el Instituto de Auditores Internos comercializa COSO como el referente para el Control Interno.

1.3.7 ISO 27000

Es un conjunto de estándares desarrollados por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información a través de un proceso sistemático, documentado y conocido por la organización [12].

Ilustración 1-7. Modelo interno ISO 27000

Fuente: El portal de ISO 27001l

En el Ecuador la firma I-SEC del Ecuador es el mayor referente, seguido del Centro de Educación Continua de la Escuela Politécnica Nacional, y ofrece capacitación y servicios de implementación de esta norma, a través de un análisis sobre la existencia de controles y posteriormente desarrolla estrategias para superar una situación inicial y llegar a la óptima.

CAPÍTULO 2
DISEÑO DEL MODELO DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN FINANCIERA DE LA PUCE

Se entiende por modelo de gestión de seguridad de información a un conjunto de políticas, procesos, controles, organización interna, soportados en marcos de referencia y normativas comúnmente aceptadas y adaptadas.

Para poder diseñar un modelo de gestión de seguridad de la información para la Universidad, es necesario conocer el entorno actual: organización, planificación, áreas de TI, seguridad, auditoría y finanzas. A continuación se detalla la situación actual:

2.1 LEVANTAMIENTO DE INFORMACIÓN

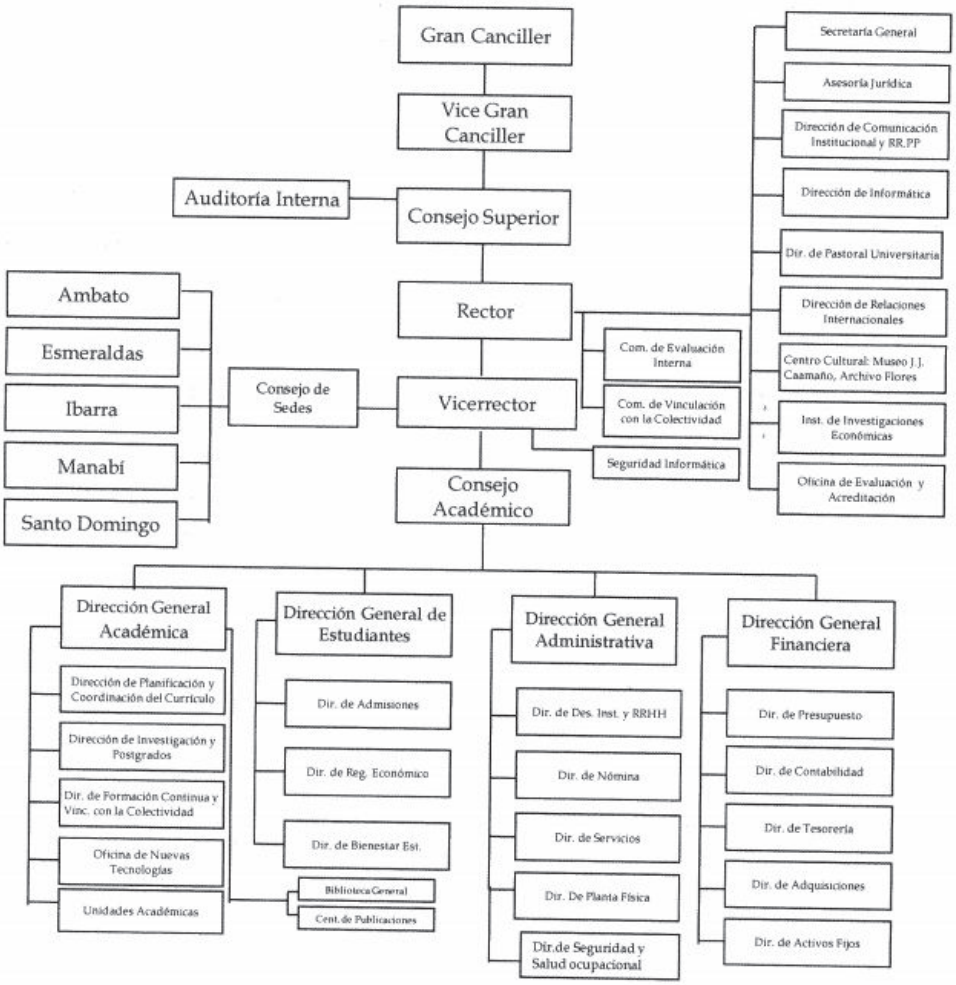
2.1.1 ORGANIZACIÓN

La Pontificia Universidad Católica del Ecuador (PUCE) fue fundada en 1946 por la Compañía de Jesús y es reconocida como “Pontificia” por la Santa Sede. Es la universidad privada más antigua del Ecuador, autónoma, sin fines de lucro, con características y principios propios, a servicio de la comunidad y que se encuentra constituida como un Sistema Nacional PUCE (SINAPUCE) [14, pp. 1, Art.1].

El SINAPUCE está conformado por la PUCE matriz en Quito y cinco sedes en Ibarra, Esmeraldas, Ambato, Manabí y Santo Domingo.

Su estructura organizacional se detalla a continuación:

Ilustración 2-1. PUCE – Organigrama estructural de la PUCE



Fuente: PUCE-ORGANIGRAMA ESTRUCTURAL

La PUCE (Pontificia Universidad Católica del Ecuador) consta de cuatro direcciones generales con la misma jerarquía que responden al Consejo Académico. La Dirección General Financiera es aquella en la que se concentran las actividades de índole financiera a través de las Direcciones de Presupuesto, Contabilidad, Tesorería, Adquisiciones y Activos Fijos, cada uno de ellos con sus funciones específicas dentro de la institución.

La unidad de Auditoría Interna, asesora del Consejo Superior de la Universidad, se encarga de realizar actividades de revisión y análisis de los procesos que, a su juicio, son relevantes para la institución; este trabajo actualmente se hace una vez que dichos procesos han sido ejecutados y sobre el cual se hacen un conjunto de recomendaciones a través del Informe de Auditoria y se lo hace llegar a las áreas involucradas para que sean revisadas y si es del caso se generen estrategias que permitan mejorar tales procesos.

Actualmente la PUCE cuenta con la oficina de Seguridad Informática, adscrita a la oficina del Vicerrector y que estaría estableciendo normativas de seguridad institucionales tales como: acceso a los recursos de internet y manejo de cuentas de red de los usuarios de la PUCE; actualmente existe una campaña combinada con la Dirección de Informática para la no divulgación de claves de red.

Los clientes internos en la Universidad son:

- Directivos.
- Decanos.
- Administrativos.
- Docentes.
- Estudiantes.
- Servicio.

2.1.2 PLANIFICACIÓN INSTITUCIONAL

Entre las metas internas de la PUCE a través del Plan Estratégico de Desarrollo Institucional 2008-2013, Objetivo 4, Implantar un sistema de gestión administrativa-financiera que contribuya de manera efectiva al desarrollo académico, Estrategia 4.1 – Mejorar los procesos actuales, se hace referencia a algunos que se han llevado a la práctica parcialmente durante ese periodo. El informe del año 2013 no da cuenta de haber cumplido con este objetivo estratégico [16].

El PEDI 2014-2018 cuenta con cuatro objetivos estratégicos y doce objetivos tácticos que pueden revisarse en el *Anexo 1*.

La Dirección General Financiera tiene a su cargo el Objetivo táctico 2.2 alineado al objetivo estratégico 2 – “En los próximos 5 años, perfeccionar el sistema de gestión integral del SINAPUCE a través de la implementación de buenas prácticas de gestión de infraestructura física, tecnológica, educativa y financiera, que apoyen de manera transversal y eficiente a la comunidad universitaria en sus tareas fundamentales”, ese objetivo táctico se muestra a continuación:

Ilustración 2-2. Proyectos 2015 Dirección General Financiera

PROYECTOS - AÑO 2015
Dirección General Financiera

LEYENDA »
Proyectos activos | Proyectos terminados | Proyectos suspendidos

Id	Nombre del Proyecto	Persona Responsable
OBJETIVO TÁCTICO 2.2		
2.2.1	Elaboración de un estudio técnico que permita establecer los costos por carrera, profesor y estudiante, en el SINAPUCE	Cevallos Velastegui Rosa Consuelo
2.2.1.2	Reestructuración del proceso presupuestario por carreras en el SINAPUCE	Cevallos Velastegui Rosa Consuelo

Fuente: PUCE, Plan estratégico de desarrollo institucional 2014-2018

Uno de los proyectos asociados a este objetivo, apunta a la reestructuración del proceso presupuestario por carrera en la PUCE matriz y sus sedes. A la fecha de presentación de este trabajo, aún no se reporta avance en este proyecto.

El PEDI, a través de los objetivos tácticos y estrategias hace mención a la práctica financiera mediante un sistema integral sin hacer una mención explícita sobre procesos, calidad o seguridad de información. Actualmente el objetivo estratégico 2 se encuentra en un 37,58% de avance [17].

2.1.3 AUDITORIA INTERNA

Por otro lado está la unidad de Auditoría interna, adscrita al Consejo Superior, que tiene dentro de sus funciones la auditoría informática en la Universidad.

La misión de esta unidad, según consta en el Estatuto de Auditoría Interna se define como: “Contribuir al logro de los objetivos institucionales a través de proveer de forma independiente y objetiva, servicios de aseguramiento y consulta diseñados para agregar valor y mejorar las operaciones del SINAPUCE, con un enfoque sistemático y disciplinario que le permita evaluar y mejorar la eficacia de los procesos de control interno, gestión del riesgo y gobierno corporativo”.

Cada año, esta unidad presenta un plan de trabajo que está encaminado a evaluar fundamentalmente la aptitud del sistema de control implantado por el auditado para cumplir las metas trazadas en base a COSO. Para la unidad de Auditoría interna está claro que la PUCE no ha establecido formalmente una metodología para gestionar riesgos.

Los trabajos realizados por esta unidad no incluye un trabajo específico sobre Evaluación presupuestaria en ningún periodo, y, el trabajo básicamente se centra en información histórica.

Está planificando iniciar un proceso de evaluación de procesos para todas las áreas de la Universidad utilizando COBIT 4.1, pero este proyecto aún no ha sido

integrado en el cronograma de trabajo, mientras tanto, se revisan procesos puntuales.

2.1.3 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN

Los requerimientos de información están orientados a la toma de decisiones en los respectivos niveles donde se utiliza, por consiguiente deben ser entregados bajo los siguientes parámetros de calidad:

- Oportuna: en el momento y lugar requeridos.
- Confiable: no requiere verificaciones.
- Utilizable: no requiere reproceso.

Hace once años la PUCE contrató una consultoría para la Seguridad de Información con la empresa Deloitte & Touche que dio como resultado un conjunto de recomendaciones globales que no han sido puestas en práctica. En el año 2009 se creó el cargo de Oficial de Seguridad de la Información y con él la Oficina de Seguridad de la Información que depende del vicerrectorado de la Universidad.

El trabajo de la oficina tiene como principal objetivo la coordinación con la Dirección de Informática las actividades que permitan brindar un alto grado de seguridad de la información. La Oficina de Seguridad de la Información ha concentrado en desarrollar un punto de partida para una adecuada administración de la seguridad de la información a través de la generación de políticas y normativas de base para el manejo institucional, con el siguiente detalle:

- **Política general y normativa de seguridad de información.-**

  Se encuentra vigente desde septiembre 2010, y está basada en los estándares internacionales ISO 27001 e ISO 270002 y los aspectos que comprende esta normativa son [18] :

  - Gestión de riesgos.
  - Organización de la seguridad de la información.
  - Gestión de activos de información.
  - Recursos humanos y seguridad.
  - Seguridad física y ambiental.
  - Gestión de comunicaciones y operaciones.
  - Control de acceso a la información.
  - Adquisición, desarrollo y mantenimiento de aplicaciones.
  - Gestión de incidentes de seguridad.
  - Gestión de la continuidad de los servicios.
  - Cumplimiento de normas.

- **Política detallada de usuario final para la seguridad de la información.-** Se encuentra vigente desde marzo 2011, y está relacionada con la política PGSI, y rige para el personal docente y administrativo dotado de un computador dentro de la Universidad, y con acceso a los servicios institucionales. Los aspectos que comprende son [19]:
    - Seguridades lógicas (contraseñas).
    - Prevención de virus.
    - Uso de internet, correo y otros servicios relacionados.
    - Seguridad física y uso de computadores personales.

- **Política detallada y normas de seguridad lógica de la información procesada con sistemas informáticos.-**

  Su vigencia aún no se determina. Esta política tiene como política de base la PGSI y está relacionada con la PDUF, y fue creado con el fin de normar la recolección, transmisión, almacenamiento, proceso y distribución de información por medio de sistemas informáticos con el objetivo de salvaguardarla de eventos adversos que pudieran ocasionar la suspensión de servicios, uso o divulgación no autorizados o alteraciones intencionales o no. Los aspectos en detalle que comprende son [20]:

    - Calidad de confidencial de la información de identificación de las personas y de otra información.
    - Necesidad de protección de la información de carácter confidencial.
    - Acciones encaminadas a proteger la información: seguridades lógicas.
    - Contenido de los registros de información.
    - Uso de la información.
    - Definiciones de requerimientos de seguridad.
    - Separación de ambientes de desarrollo y producción.
    - Controles preventivos técnicos.
    - Definición de roles funcionales con privilegios mínimos.
    - Reporte de incidentes de seguridad.
    - Coordinación de aspectos relacionados con la propiedad de la información, clasificación y responsabilidades.
    - Cifrado de la información.
    - Políticas complementarias.
    - Autenticación de usuarios.
    - Procedimientos relacionales con los derechos de acceso a la información.

- Debido proceso para el desecho de medios de almacenamiento o documentos con información clasificada.
- Política de escritorio limpio.

Los Política General y Normativa de Seguridad de Información y la Política Detallada de Usuario Final para la Seguridad de la Información, han sido aprobadas y posteriormente socializadas a la comunidad universitaria a través del correo electrónico institucional así como del portal web institucional.

Es importante mencionar que si bien es cierto, los procesos de la Universidad actualmente no se basan en ningún estándar, la Política General y Normativa de seguridad de información está basada en los estándares internacionales ISO 27001 e ISO 270002 que son normas relacionadas con TI [18].

Existen también referencias al trabajo de campo realizado con usuarios relevantes por cada uno de sistemas informáticos prioritarios. A través del instrumento de encuesta sobre seguridad de la información de las aplicaciones existentes los aspectos que se han evaluado están relacionados con la confiabilidad de datos, el tiempo de respuesta de la aplicación, grado de actualización de la información, confidencialidad y completitud de los datos que proporciona la aplicación.

Adicionalmente existe evidencia de los riesgos relacionados a la tecnología de la información que impactan en los POAs (Planes Operativos Anuales) y en el PEDI (Plan Estratégico de Desarrollo Institucional) sin que estos hayan podido ser gestionados en conjunto con la Dirección de Informática [21, p. 305].

2.1.4 GESTIÓN DE TI E INFRAESTRUCTURA TECNOLÓGICA

La PUCE cuenta con la Dirección de Informática que tiene a cargo las funciones de gestión de TI, entre ellas: definir las políticas tecnológicas, delinear el desarrollo informático institucional y liderar nuevos proyectos tecnológicos. Las últimas gestiones de esta dirección se resumen a continuación [22]:

- Dotar de equipos de computación al personal administrativo, docente y estudiantes.
- Administrar las herramientas de gestión de infraestructura tecnológica.
- Definición de la arquitectura del sistema operativo institucional.
- Desarrollo de un programa de Seguimiento del Programa Microcurricular para estudiantes.
- Gestión de información para todos los procesos de evaluación.
- Soporte tecnológico para la implementación de la facturación electrónica.
- Desarrollo de nuevas funcionalidad de los aplicativos académicos.
- Soporte para la lectura y corrección de exámenes de ingreso, idiomas y fin de carrera.

- Estandarización de los repositorios digitales.
- Mejoramiento del perímetro de seguridad inalámbrica.
- Renovación de equipos de comunicación para mejora de la interconexión.
- Mejoramiento en la contingencia de servidores.
- Etiquetamiento y reconocimiento físico y lógico de los puntos de red.
- Recableado de edificios del campus.
- Implementación de listas de control de acceso en redes virtuales.
- Reorganización del directorio activo.
- Almacenamiento centralizado para direcciones, departamentos y facultades.
- Implementación de seguridad de la información de BD y aplicaciones web.
- Plan de alta disponibilidad y continuidad de negocios para los motores de bases de datos.
- Cambios de puertos en bases de datos.
- Mejorar la virtualización y standby de bases de datos.
- Implementación de un sistema de administración y reorganización de BD.
- Depuración y segregación de usuarios a nivel de datos.
- Soporte técnico a la plataforma educativa institucional.

En cuanto a la infraestructura tecnológica, la PUCE cuenta con [23]:

Equipamiento:

- Servidores multiplataforma y múltiple propósito.
- Equipos de red y comunicación inalámbrica con cobertura total en espacios académicos.
- Más de doscientos puntos de red con banda ancha de 245 Mb.
- 2875 equipos de computación.
- 387 aulas equipadas con computadores y proyectores.
- 15 salas de profesores con 75 computadoras.
- 16 laboratorios con 623 equipos.
- 30000 cuentas de correo electrónico.

Adicionalmente cuenta con Bases de Datos y aplicaciones:

- Bases de datos Oracle, MySQL, Postgres.
- Sistema de gestión académica UXXI.
- Sistema de investigación UXXI – Investigación.
- Sistema de gestión financiera – BAAN.
- Sistema de gestión administrativa – ADAM.
- Sistema de indicadores estadísticos – SIEPUCE.
- Sistema de integración de procesos – PISP.

- Gestión de Biblioteca.
- Portal Web.
- Intranet universitaria.
- Administración de documentos digitales – Document Manager.

Servicios tecnológicos:

- Correo electrónico estudiantil.
- Correo electrónico para personal administrativo y docente.
- Internet.
- Red inalámbrica.
- Aulas virtuales.
- Antivirus.
- Servicio de impresión de calidad.
- Servicio de préstamos de equipos portátiles.
- Servicios de aulas equipadas para docencia.
- Salas de profesores con equipamiento básico.
- Pantallas informativas.
- Centro de informática para atención estudiantil.
- Soporte a usuarios.

2.1.5 ÁREA FINANCIERA DE LA INSTITUCIÓN

La Dirección General Financiera (DGF) es la unidad a cargo de todos los procesos de índole financiero de la PUCE y consta de las siguientes direcciones que son los responsables de estos procesos en la Universidad:

- Dirección de Contabilidad.
- Dirección de Presupuestos.
- Dirección de Tesorería.
- Dirección de Adquisiciones.
- Dirección de Control de Activos.

2.1.5.1 Objetivos generales

Los objetivos generales de esta dirección siguen siendo en su gran mayoría los mismos planteados antes de la implementación del sistema [24]:

- Presentar para aprobación políticas requeridas en las distintas direcciones de la Dirección General Financiera.
- Definir, elaborar y aprobar los procesos estandarizados y optimizados de acuerdo con las necesidades de la Dirección General Financiera.
- Definir e incorporar a los procesos los controles requeridos por esta dirección
- Realizar una oportuna difusión del avance del proyecto.
- Asegurar la generación de información financiera de calidad.
- Lograr el compromiso de los usuarios finales con el proceso de cambio, capaces de utilizar eficiente y efectivamente el nuevo sistema implantado.
- Lograr que los directivos sean capaces de liderar y sostener el cambio generado con la implantación el nuevo sistema.
- Capacitar a los ejecutivos para acceder a información de análisis en línea para la toma de decisiones.
- Integrar la información de las distintas funciones de la Dirección General Financiera y de otras externas.
- Integrar la información de los agentes externos y de los clientes internos.
- Mejorar la satisfacción de los clientes internos y externos.

2.1.5.2 Objetivos específicos

Los objetivos específicos por cada una de las direcciones del área financiera están enmarcados en los siguientes [24]:

DIRECCIÓN GENERAL FINANCIERA

- Establecer un proceso electrónico que permita disponer de alertas financieras.
- Asegurar que todos los procesos tengan los controles internos adecuados para cada sistema o modulo.
- Disponer de información gerencial de calidad (análisis).
- Disponer de un control presupuestario de calidad (variaciones).
- Disponer de información transaccional en línea, para los módulos de Presupuesto, Contabilidad, Tesorería, Adquisiciones y Control de Activos.
- Disponer del flujo de caja oportuno para seguimiento.
- Disponer de la liquidación presupuestaria en forma oportuna y confiable.
- Disponer de estados financieros diariamente.
- Disponer de información actualizada cada día.

DIRECCIÓN DE PRESUPUESTOS

- Establecer procesos para la formulación, aprobación, ejecución, control y liquidación del presupuesto.
- Establecer procesos que permitan a las diferentes unidades académicas, administrativas y financieras elaborar los presupuestos de ingresos y egresos.
- Implantar procesos que permitan actualizar y proyectar los presupuestos por variaciones.
- Disponer de información de seguimiento y avance (interactiva) para la toma de decisiones a nivel gerencial y de cada una de las unidades ejecutoras.
- Establecer un proceso de validación de la información enviada por las diferentes unidades de apoyo para la ejecución presupuestaria.

DIRECCIÓN DE CONTABILIDAD

- Implantar controles en los procesos críticos del área.
- Definir parámetros (datos, periodos, porcentajes, índices) para utilizar adecuadamente las herramientas de análisis.
- Obtener Estados Financieros diarios (Situación, Pérdidas y Ganancias, Evolución del Patrimonio, Flujo de Efectivo).
- Establecer procesos para obtener informes requeridos por el SRI.
- Establecer un proceso para realizar las conciliaciones bancarias en forma automática con información electrónica de las instituciones financieras.

- Establecer procesos para obtener anexos de las cuentas del balance previamente especificadas.
- Establecer un proceso de control del movimiento diario de ingresos y egresos entre las Direcciones de Tesorería y Contabilidad.
- Establecer un proceso de validación de los asientos de diario.

DIRECCIÓN DE ADQUISICIONES

- Definir e implantar políticas para adquisiciones a través de procesos adecuados a las necesidades del área.
- Establecer procesos de planificación anual integrada de adquisición de bienes, y servicios según los requerimientos del presupuesto, a fin de obtener del mercado condiciones favorables de precios y oportunidad.
- Implantar procesos para el manejo de adquisiciones de los diferentes tipos de requerimientos (productos) de manera centralizada, descentralizada, y por medio de terceros.
- Implantar un proceso de calificación y seguimiento de proveedores basado en datos históricos, términos y condiciones.
- Acceder en línea a la información de la base de datos para toma de decisiones y autorizaciones de adquisiciones (Presupuestos, Contabilidad, Activos Fijos, Inventarios, Compras y Tesorería).
- Establecer niveles de autorización para compras en función de rangos de valor.

DIRECCIÓN DE TESORERÍA

- Establecer un proceso de validación de las operaciones de ingreso y egreso (electrónica).
- Establecer un proceso para la obtención del flujo de caja.
- Establecer procesos que optimicen la emisión de la facturación de matrículas y servicios estudiantiles.
- Integrar al sistema los puntos de facturación de la PUCE.
- Establecer controles internos en los procesos críticos (facturación).

DIRECCIÓN DE CONTROL DE ACTIVOS

- Calcular la depreciación, mensual y anual.
- Optimizar la toma de inventario físico con distintos criterios de muestreo de activos versus criterios contables, a través de controles ejecutados mediante lectores ópticos.
- Controlar la movilización temporal o permanente por ítem (cambios, devoluciones, prestamos autorizados, arriendo, en depósito, proyectos).
- Registrar los activos dados de baja por obsolescencia, hurtos, robos o daños irreparables.

2.1.5.3 Sistema financiero ERP BAAN 5.0

ERP (Entreprise Resourcing Planning) es una herramienta de software cuyo objetivo radica en la integración y automatización de los procesos dentro de una organización. Permite gestionar información abundante de forma integral y eficiente para minimizar la carga operativa eliminando tareas que no agregan valor. Es una herramienta proactiva y reactiva que proporciona insumos a la alta gerencia para toma de decisiones.

Un ERP es implementado en una organización cuando se han desgastado los esfuerzos por generar valor a los sistemas desarrollados en casa o existen sistemas desintegrados entre sí. Estos factores incidieron en su oportunidad para que la PUCE busque un sistema flexible que permite el cambio dinámico de los procesos de negocio, con miras a convertirlo en la columna vertebral de todos los sistemas de la empresa.

La Dirección General Financiera de la PUCE ha implementado desde el año 2003 el ERP BAAN 5.0 que funciona hasta la actualidad.

BAAN es un sistema que ofrece una amplia y flexible suite de componentes empresariales integrados que permite manejar, comprar, planificar, enviar, costear, administrar la calidad de las diferentes actividades, integrando los procesos e información de las distintas direcciones de la PUCE. BAAN fue una empresa de software fundada en 1978 por Paul y Jan Baan y es la empresa INFOR la actual propietaria que continúa dando soporte a este producto.

Los módulos de BAAN son: Planeación, Ingeniería, Costos, Finanzas, Inventarios, Ventas, Producción, Compras y Logística, Distribución, Presupuestos.

Los módulos del sistema implementados en la Universidad son los siguientes:

- Distribución.- Módulo que apoya a la organización a desarrollar la mejor solución para resolver los requisitos de los clientes y balancear las necesidades del negocio teniendo en cuenta los requerimientos de distribución, ventas y logísticas, tanto de fabricantes como de distribuidores.
- Finanzas.- Módulo que automatiza los procesos financieros del back office y está integrado con los otros módulos del ERP.
- Presupuestos.- Módulo que gestiona el manejo presupuestario de la organización integrado con el resto de módulos de ERP BAAN.
- DEM (Modelizador dinámico empresarial).- Módulo que integra los conceptos y procesos del negocio a la herramienta ERP, a través de herramientas, como los modelos de funciones, de procesos y organizacional. Permite la parametrización de perfiles de usuario de manera gráfica, reduciendo los tiempos de entrenamiento y generación de pantallas. Permite la documentación de procesos en línea y ofrece mucha flexibilidad para la modificación y optimización de los procesos de la PUCE.Permite modelar gráficamente las estructuras organizacionales y procesos de negocio, adquirir una visión de alto nivel de sus operaciones, y optimizar estos componentes en cualquier momento, haciendo efectiva y real el mejoramiento continuo de procesos, sin causar cambios traumáticos.

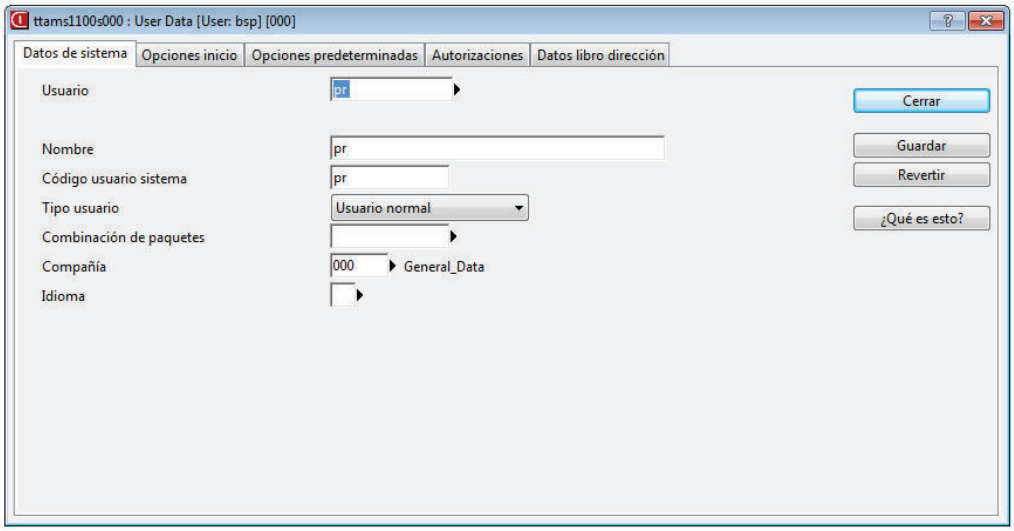
2.1.5.4 Seguridad de la información en ERP BAAN 5.0

2.1.5.4.1 Creación de usuarios

Para poder ingresar al sistema financiero ERP BAAN 5.0 es necesario primeramente crear un usuario dentro del sistema. El usuario clave del área, con la aprobación de la Directora General Financiera, solicitan la creación del usuario mediante un formulario destinado para este efecto.

En la siguiente ilustración se puede apreciar la sesión que permite la asignación del usuario de base de datos a un usuario de BAAN, así como la determinación de la compañía a la cual este usuario tiene acceso. Este proceso lo ejecuta la Dirección de Informática en base al requerimiento inicial.

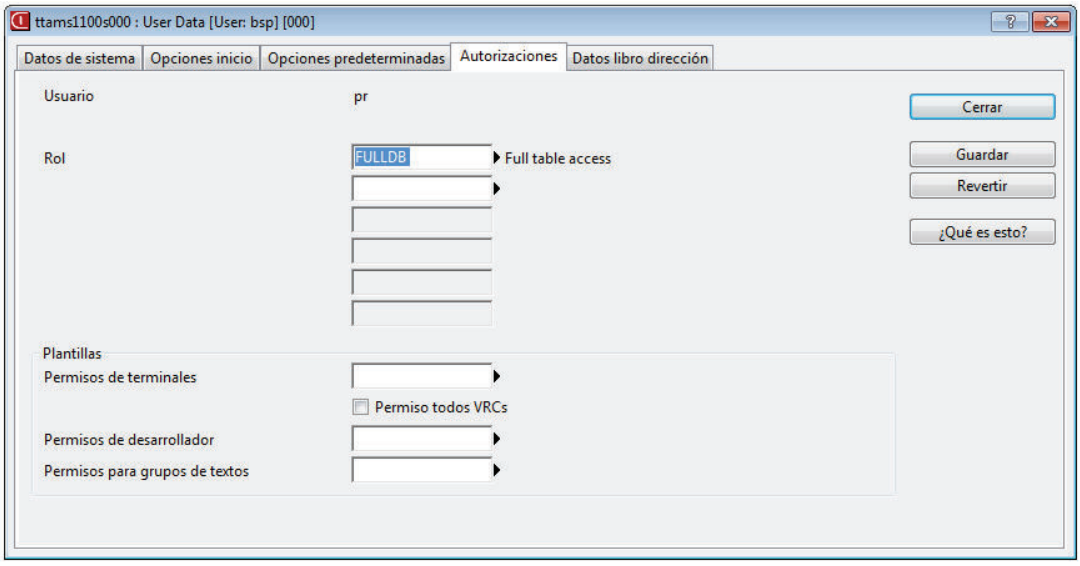
Ilustración 2-3. BAAN – Creación de usuarios – datos del sistema



Fuente: BAAN 5.0 PUCE- Tools

Cuando el usuario es creado, seguidamente se le asigna un rol inicial de acuerdo a lo que el usuario clave ha solicitado. Los funcionarios para el proceso de liquidación presupuestaria tienen asignado el mismo rol. En la siguiente sesión, se indica la sesión sobre la cual se hace la asignación descrita:

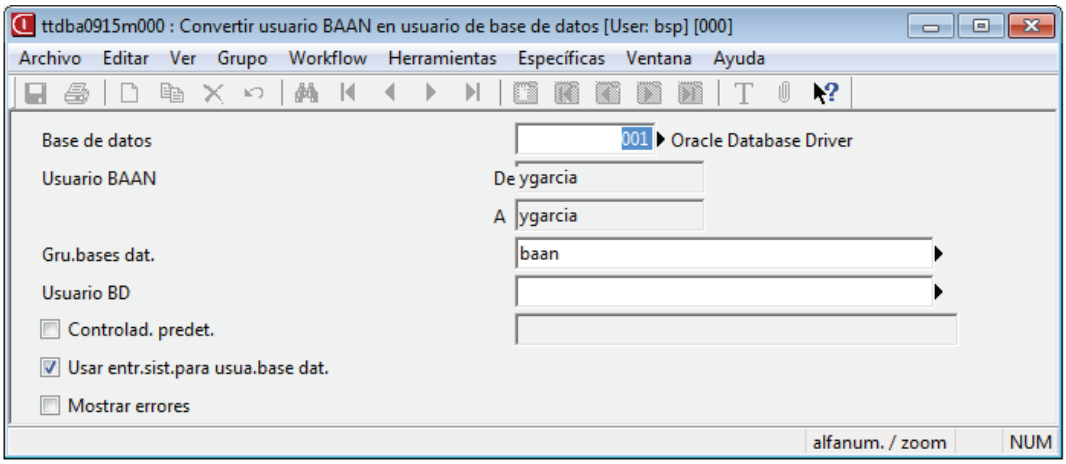
Ilustración 2-4. BAAN – Asignación de roles



Fuente: BAAN 5.0 PUCE- Tools

Para hacer efectivos los permisos a nivel de base de datos se utiliza la sesión que se ilustra a continuación. Mediante este proceso, todos los permisos asignados al rol a través del ERP se consolidan en permisos dentro de la estructura de la base de datos en la que se soporta el sistema:

Ilustración 2-5. BAAN – Convertir usuario BAAN en usuario BD



Fuente: BAAN 5.0 PUCE- Tools

2.1.5.4.2 Identificación de usuarios y roles

Para efectos de determinar riesgos en el acceso a información sensible se hizo un levantamiento de los roles actualmente en el sistema BAAN, específicamente de aquellos relacionados con el usuario final:

Tabla 2-1. Roles en ERP BAAN 5.0 para la PUCE

ÁREAS DIRECCIÓN GENERAL FINANCIERA	ROL EN BAAN	DESCRIPCIÓN
DIRECCIÓN DE ADQUISICIONES	PROY_ADQUISI2	Permisos Adquisiciones - UC
	PROY_ADQUISIC	Permisos Adquisiciones - Jefe
DIRECCIÓN DE CONTROL DE ACTIVOS	PROY_ACTIVOS	Permisos Activos - Jefe
	PROY_ACTIV_A2	Permisos Activos A2 - UC
DIRECCIÓN DE CONTABILIDAD	PROY_RETCONT	Permisos Contabilidad - Jefe
	PROY_RETCONT2	Permiso Contabilidad -P2
	PROY_RETCONT3	Permiso Contabilidad -P2
	PROY_TRIBUTA2	Gestión Tributaria
	PROY_TRIBUTAR	Permisos Tributaria - UC
DIRECCIÓN DE PRESUPUESTOS	PROY_PRESUP	Permisos Presupuestos - UC
	PROY_PRESUP2	Permisos Lect Ext Presupuestos
	PROY_PRESUP3	Permisos Presupuestos - Jefe
DIRECCIÓN DE TESORERÍA	FACT_BG	Permiso facturación Biblioteca

	FACT_CESAQ	Permiso facturación Cesaq
	FACT_CJ	Permiso facturación CJ
	FACT_CM	Permiso facturación Centro Med
	FACT_CP	Permiso facturación Centro Pub
	FACT_DS	Permiso Facturación Diserlab
	FACT_ECY	Permiso facturación ECY
	FACT_MW	Permiso Facturación Museo W
	FACT_PA	Permiso facturación Psicologia
	FACT_PU	Permiso facturación Pastoral
	FACT_SUELOS	Permiso facturación LAB.SUELOS
	PROY_FACTURAC	Permisos Facturación
	PROY_TESORERI	Permisos Tesoreria - UC
USUARIOS CLAVE	PROY_MENU	Permisos Menú Usuarios Clave

Fuente: Elaboración propia

Como puede ilustrarse en la tabla anterior, la mayor parte de roles pertenecen a la Dirección de Tesorería, esto se debe a que el módulo de facturación está disponible, con sus particularidades en algunos puntos de cobranza en las unidades académicas de la PUCE.

Por otro lado se evidencia el concepto de Usuarios clave, que es la persona con el mayor conocimiento el área y que tiene acceso total a sus respectivos módulos y puede hacer un vistazo general a los módulos y sesiones del resto de áreas de la Dirección General Financiera. Actualmente los usuarios clave de cada una de las áreas recae principalmente en el director y en una o dos personas de confianza según corresponda que tienen un rol asignado que les permite acceso al menú principal del sistema con ciertas restricciones a nivel de tablas.

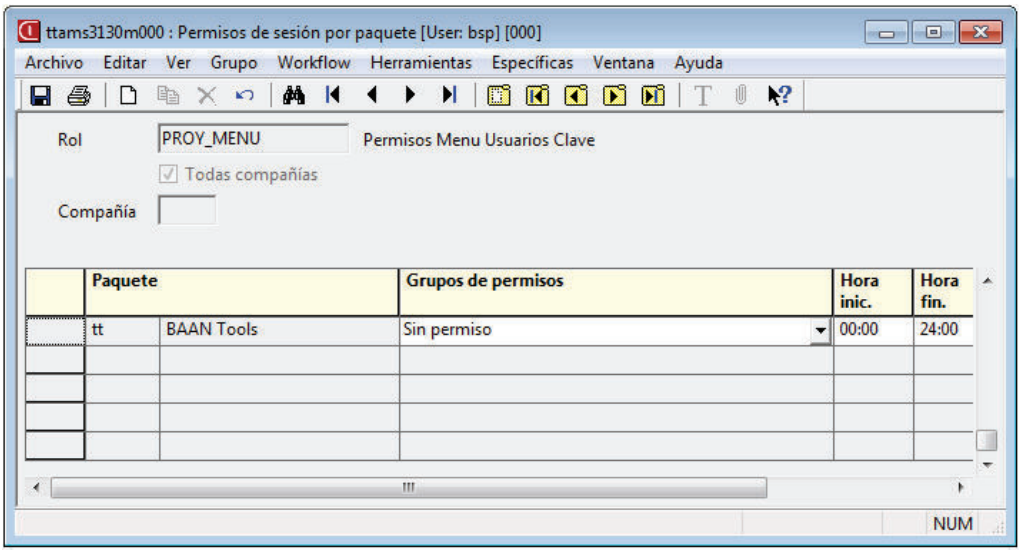
La Dirección de Presupuestos tiene 3 roles asignados; los roles PROY_PRESUP y PROY_PRESUP2 corresponden a los analistas de presupuestos, quienes básicamente manejan los mismos privilegios de acceso a la información.

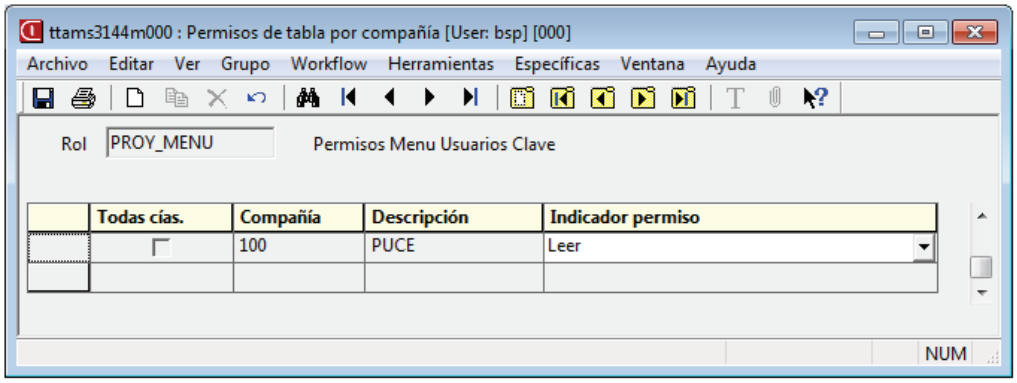
Con respecto al proceso de evaluación, no existe un rol especifico identificado dentro del sistema para esta función, por lo que, en teoría, cualquier persona con los roles presupuestarios podría modificar el presupuesto según se puede ver en el proceso dibujado.

2.1.5.4.3 Asignación de permisos y roles

Eventualmente, cuando un nuevo rol ha sido creado, se deben asignar permisos a dicho rol. La siguiente ilustración muestra la sesión del ERP donde se administra el esquema de permisos:

Ilustración 2-6. BAAN - Asignación de permisos de sesión y tablas a roles





Fuentes: ERP BAAN 5.0 en PUCE

En una entrevista al actual administrador técnico del sistema, indica que no existe documentación previa que permita establecer esta relación y que el levantamiento de roles se hizo en base a las especificaciones funcionales del sistemas levantadas por la empresa proveedora de software en el año 2003 sin que actualmente se haya revisado si estos roles asignados poseen permisos excesivos o limitados dependiendo del cargo y las funciones asociados al personal dentro de la Dirección General Financiera.

2.2 DETERMINACIÓN DE PROCESOS CRÍTICOS

Para poder determinar los procesos de la gestión financiera, se hace necesario conocer a través de un levantamiento de campo su estructura, interacción, actividades, objetivos y necesidades.

La Dirección General Financiera no cuenta con un levantamiento documentado de sus procesos. Algunos procesos fueron levantados hace varios años como parte del trabajo de implementación del ERP BAAN 5.0 y fue realizado por el equipo de implementación constituido por el personal de la empresa asesora así como los usuarios claves de las cinco direcciones.

El resultado de este levantamiento se encuentra documentado a través del módulo de DEM (Modelizador Dinámico Empresarial) de BAAN, con el cual se ha logrado:

- Identificar aquellas sesiones que son utilizadas por los usuarios del sistema para operativizar los procesos diagramados.
- Establecer la relación entre Roles y usuarios dentro de este sistema.

El sistema ERP BAAN 5.0 tiene documentados 42 procesos internos y 7 procesos relacionados con la administración funcional del sistema. A continuación se presenta una tabla condensada de estos procesos:

Tabla 2-2. Procesos internos del área financiera documentados en BAAN

ÁREA	CÓDIGO	NOMBRE DEL PROCESO
Dirección de Adquisiciones	AD0101	Calificación de proveedores
	AD0901	Creación de artículos
	AD1201	Compra de suministros inhouse
	AD1700	Retro ordenes
Dirección de Control de Activos	AF0100	Parametrización de activos fijos
	AF0505	Etiquetación
	AF0700	Entrega activo nuevo a custodio
	AF1300	Reasignación activos fijos
	AF2000	Enajenación de bienes
	AF4300	Creación de artículos
	AF7000	Toma anual inventario SyM
	AF7500	Consulta Kardex
Dirección de Contabilidad	CO0100	Declaración de impuestos
	CO0500	Preparación informes SRI
	CO0700	Conciliación bancaria electrónica
	CO3000	Preparación Estados Financieros

	CO5500	Registros contables
	CO5505	Pagos varios
	CO6001	Control facturación clientes
	CO6500	Control registros contables
	CO6600	Cierre periodo anual
	CO9600	Integración contable
	CO9800	Consulta asientos DGE
Dirección de Presupuestos	PR0000	Mantenimiento de dimensiones
	PR0101	Formulación presupuestaria por la unidad
	PR0600	Generación de presupuestos
	PR1000	Aprobación de proforma presupuestaria
	PR2000	Ejecución presupuestaria
	PR2004	Modificación del presupuesto
	PR4200	Evaluación presupuestaria
	PR4300	Conciliación con finanzas
	PR7001	Creación del presupuesto
	PR7005	Simulación presupuestaria
Dirección de Tesorería	TE0100	Parametrización tesorería
	TE3500	Flujo de caja
	TE4010	Pago de roles
	TE4030	Pago a proveedores con cheque
	TE4525	Cuadre diario de caja
	TE4560	Registro y control de cuentas por cobrar
	TE5520	Cierre de transacciones diarias
	TE6001	Cobro de matrículas en tesorería
	TE7002	Facturación electrónica
Administración funcional	AB0001	Creación de usuarios
	AB0002	Control de errores
	AB0003	Personalizaciones
	AB0004	Levantamiento de auditorias

	AB0005	Consulta de auditorías
	AB0006	Modificación de permisos de usuario
	AB0007	Dar de baja a un usuario

Fuente: Elaboración propia

En una entrevista a la directora de la Dirección de Presupuestos de la PUCE, se pudo establecer que los procesos diagramados en el sistema BAAN e identificados en la tabla anterior son en muchos casos subprocesos o partes de procesos más grandes. La razón atribuida a este levantamiento es porque se levantaron los procesos o partes de procesos que hacen uso de alguna sesión de dicha herramienta y que son considerados críticos para los usuarios.

2.3 IDENTIFICACIÓN DE RIESGOS

La ocurrencia de que cualquier evento que afecte al desempeño de los servicios informáticos institucionales es una preocupación de la Oficina de Seguridad de la Información. En una levantamiento de información realizado a través del jefe de la oficina se pudo determinar que la gestión de riesgos en la PUCE, debe ser adecuadamente administrada mediante un proceso de gestión de riesgos tecnológicos, para lo cual, en un futuro y dentro del cronograma de trabajo interno se coordinarán las respectivas acciones entre esta oficina, la Dirección de Informática y el área de riesgo.

Las actividades que se llevarán a cabo son las siguientes:

- Clasificación de los activos de información institucionales.
- Determinación de las amenazas del entorno y de las vulnerabilidades de los activos de información de la PUCE.
- Valoración de los riesgos en función de su probabilidad de ocurrencia y del impacto que causarían en los servicios de la Universidad. Esta valoración debe revisarse periódicamente en función de los cambios.
- Determinación de las salvaguardas en función del costo/beneficio.
- Coordinación con la Dirección de Informática la implementación de las salvaguardas: medidas preventivas y planes de contingencia.

Al momento no existen documentos oficiales que respondan a los riesgos identificados para el área financiera. A través de la entrevista a funcionarios de la Dirección General Financiera se pudo determinar el riesgo en la gestión financiera en función los recursos de TI con el siguiente resultado:

Tabla 2-3. Identificación de riesgos y vulnerabilidad financiera en función de recursos de TI institucional

ÁREA: Dirección General Financiera		
AMENAZAS	**VULNERABILIDAD**	**RIESGOS FINANCIERO EN FUNCIÓN DE TI**
• Intercambio de información no controlado dentro de la institución • Acceso a información financiera por parte de terceros • Acceso a información financiera a usuarios no autorizados debidamente	• Acceso peligroso a información financiera • Divulgación de información no autorizada	• Acceso no controlado a la información confidencial
• Protección contra código malicioso • Falta de respaldos de información	• Calidad de información deficiente • Falta de coherencia entre los registros y los respaldos de las operaciones financieras	• Pérdida de información para la toma de decisiones

Fuente: Elaboración propia

De acuerdo a la tabla anterior, se contrastaron los riesgos y las vulnerabilidades identificadas con respecto a las funciones asignadas a la Oficina de Seguridad de Información con el fin de determinar estos riesgos serán considerados o formalizados en un futuro:

Acceso no controlado a la información confidencial.-

Con el objetivo de minimizar el riesgo de acceso no controlado a la información confidencial a través de controles de acceso a la red, la Oficina de Seguridad de Información vigilará que [18]:

- A los usuarios se les concedan accesos únicamente a aquellos servicios para los cuales han sido específica y formalmente autorizados.
- Se utilicen métodos de autenticación apropiados para controlar el acceso de usuarios.
- Se considere la identificación automática de equipos como medio de autenticar conexiones desde localizaciones y equipos específicos.
- Se controle el acceso lógico y físico a los equipos servidores de administración de la red.
- En las redes se segreguen los grupos de servicios de información, de usuarios y de sistemas de información,
- En Internet la capacidad de conexión de los usuarios se restrinja en concordancia con la política de control de accesos y los requerimientos de las aplicaciones de la PUCE.

- Se implementen controles de enrutamiento en la red para garantizar que las conexiones de computadoras y los flujos de información no incumplan las políticas de control de accesos a las aplicaciones de la PUCE.

Con el objetivo de minimizar el riesgo de acceso no controlado a la información confidencial a través de controles de acceso al sistema operativo, la Oficina de Seguridad de Información vigilará que [18]:

- Cada usuario del SO tenga un identificador único solamente para su uso personal y exista una técnica adecuada de autenticación para corroborar la identificación que afirma tener un usuario.
- Los sistemas para la administración de contraseñas garanticen contraseñas de calidad, de acuerdo con la sensibilidad de la información y de acuerdo con la política establecida para el efecto.
- Esté restringido y rigurosamente controlado el uso de programas utilitarios que puedan anular los controles del sistema y de la aplicación.
- Las sesiones con el SO sean debidamente cerradas luego de un período de inactividad definido.
- Se apliquen restricciones en la duración de las conexiones para brindar seguridad adicional en aplicaciones de alto riesgo.

Con el objetivo de minimizar el riesgo de acceso no controlado a las aplicaciones y a la información a través de controles de acceso al sistema operativo, la Oficina de Seguridad de Información deberá [18]:

- Desarrollar, implementar y mantener, en conjunto con la Dirección de Informática y la Dirección de Recursos Humanos una política de accesos para que se garantice que el acceso a la información y a las funciones de los sistemas de aplicación por parte de los usuarios y del personal de soporte sea restringido de acuerdo con las políticas de control de accesos definidas.
- Propender que los sistemas sensitivos tengan, en lo posible, un ambiente de computación dedicado, o al menos adecuadamente controlado.

Con el objetivo de minimizar el riesgo de acceso no controlado a la información confidencial que genera el intercambio de información, la Oficina de Seguridad de Información vigilará que [18]:

- Existan y se apliquen políticas, procedimientos y controles formales para proteger el intercambio de información que se realice por cualquier medio de comunicación.
- Se establezcan acuerdos para el intercambio de información y software entre la PUCE y los terceros involucrados.

- Los medios que contengan información estén protegidos de accesos no autorizados, mal uso y daños durante su transporte hacia fuera de las instalaciones de la PUCE.
- La información involucrada en mensajería electrónica esté adecuadamente protegida.
- Se desarrollen e implementen políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información de la PUCE.

Con el objetivo de minimizar el riesgo de acceso no controlado a la información confidencial que genera el acceso a información financiera por parte de terceros, se han establecido las siguientes funciones de la Oficina de Seguridad de Información: [18]:

- Identificar los riesgos de la seguridad de la información de la organización y de sus instalaciones de procesamiento ocasionados por cualquier actividad de la PUCE que involucre a terceros, visitantes, trabajadores externos, etc. Se deberán implementar los controles adecuados antes de dar los accesos.
- Identificar y tratar todos los requerimientos de seguridad identificados antes de dar a terceros accesos a los activos de información o a la información de la PUCE.
- Cubrir todos los requerimientos relevantes de seguridad antes de la puesta en vigor de acuerdos con terceros que involucren el acceso, el procesamiento, la comunicación o el manejo de la información de la PUCE o de sus recursos de procesamiento o al incorporar nuevos productos o servicios tecnológicos.

Con el objetivo de minimizar el riesgo de acceso no controlado a la información confidencial a causa del acceso no autorizado a usuarios, se han establecido las siguientes funciones de la Oficina de Seguridad de Información vigilará que [18]:

- Exista y esté en aplicación un procedimiento para conceder y revocar derechos de acceso a todos los servicios y sistemas de información. La concesión y revocatoria de derechos de acceso a la información deberá estar basada en las necesidades de los usuarios de las diferentes unidades administrativas de la PUCE, para lo que se deberá establecer un esquema de roles y responsabilidades.
- La asignación y uso de privilegios sea restringida y controlada sobre la base de las necesidades de acceso y de la sensibilidad y criticidad de la información.
- La asignación de contraseñas sea controlada por medio de una política y un proceso formal de administración.
- Los derechos de acceso de los usuarios se revisen a intervalos regulares, al menos dos veces al año, mediante un procedimiento formal, y se establezcan

los flujos de información necesarios para mantener actualizados los derechos de acceso en función de las novedades administrativas del personal.

Pérdida de información para la toma de decisiones.-

Con el objetivo de minimizar la pérdida de información para la toma de decisiones confidencial que genera la falla de protección contra código malicioso, la Oficina de Seguridad de Información vigilará que [18]:

- Se implementen controles preventivos, detectivos y correctivos, así como adecuados procedimientos de capacitación y creación de compromiso por parte de los usuarios, para protección contra toda clase de código malicioso.
- Se mantengan actualizados en todos los equipos los sistemas antivirus y los parches de seguridad

Con el objetivo de minimizar la pérdida de información para la toma de decisiones confidencial que genera la falta de respaldos para mantener la integridad y disponibilidad de información, la Oficina de Seguridad de Información vigilará que [18]:

- Se definan y apliquen políticas y procedimientos adecuados de respaldo de información en función de su criticidad.
- Se obtengan copias de respaldo de la información y del software y éstas sean probadas regularmente de acuerdo con la política vigente para el efecto.

2.4 COMPARATIVA DE NORMAS Y MODELOS

La Gestión de la Seguridad de la Información demanda el conocimiento de normas legales y técnicas aplicables a la organización. Cuando no existe madurez en cuanto a este tema dentro de la organización, es posible facilitar la gestión adaptando normas internacionales existentes.

La adaptación y uso de una norma a través de un marco de referencia permite transparentar si se están o no cubriendo los aspectos de seguridad. Esta práctica va más allá de impartir políticas porque se apoya en el conocimiento de expertos que se encuentra expresado en la documentación del modelo o norma.

A continuación se presenta un cuadro resumen de los marcos y normas de mayor difusión, con el fin de que permitan guiar la elección para este trabajo:

Tabla 2-4. Comparativa entre marcos de referencia y modelos de seguridad de información

	COBIT 5.0	ITIL	OCTAVE	MAGERIT	COSO	ISO27000	ISO31000
OBJETIVO	Marco de referencia para objetivos de control sobre la información.	Marco de referencia para la Infraestructura de Tecnologías de la Información.	Metodología de gestión basada en el riesgo.	Metodología de Análisis y Gestión de Riesgos de los sistemas de Información. Se basa en ISO31000	Estándar de referencia que contiene directrices para la implantación, gestión y control de un sistema de control dentro de una organización	Estándar enfocado en la seguridad la información. Es más robusto que la seguridad manejada por COBIT o ITIL aunque su alcance sea menor.	Estándar que proporciona directrices sobre la gestión de riesgos. Puede aplicarse en su totalidad o en un área.
ÁREA DE APLICACIÓN	Enfocada en el Gobierno y control de TI. Permite mapear los procesos base y sus riesgos de acuerdo a las mejores prácticas. Usualmente implementado para auditorias de sistemas de información relacionadas con auditoría financiera o TI en general.	Enfocada en la gestión de los diferentes niveles de servicios de TI. Implementado en compañías de consultoría de TI	Enfocada en el riesgo organizacional, la estrategia y la práctica. Permite medir el grado de madurez de los proceso de desarrollo de software.	Enfocada en seguridad a través del uso de los medios tecnológicos.	Enfocada en el control de una organización. Implementado en empresas de seguridad, compañías de consultoría de TI.	Enfocada exclusivamente en la seguridad e información	Enfocada en el proceso de gestión de riesgos

Fuente: Elaboración propia

Haciendo un análisis de la información levantada en el apartado 2.1 – Situación actual institucional de la PUCE, con respecto a la gestión de seguridad de información en los procesos críticos de su área financiera, y el cuadro comparativo anterior, se desprende que:

La Universidad requiere apoyo para la toma de decisiones en niveles gerenciales para llevar adelante la implementación de políticas de seguridad de la información, a la vez que requiere de un mapeo de procesos institucional liderado al más alto nivel. COBIT 5.0 es robusto en este enfoque porque ayuda la dirección en la definición de un plan de TI estratégico, la definición de la arquitectura de la información, la adquisición del hardware necesario TI y el software para ejecutar una estrategia TI, la aseguración del servicio continuo, y la supervisión del funcionamiento del sistema TI, y de la misma manera permite el mapeo de procesos requerido. COBIT es utilizado en las auditorías financieras lo cual indica una ventaja en la adaptación dentro del área financiera de la PUCE.

Sin embargo la desventaja de COBIT 5.0 recae en que el estándar de base no abarca a profundidad los temas de seguridad. ISO 31000 es el estándar que proporciona directrices sobre gestión de riesgos de una manera sólida supliendo esta desventaja. Adicionalmente ISO 31000 puede implementarse total o parcialmente; esta versatilidad permite mantener una coherencia de la aplicación

de la norma integrándola de manera sutil con el marco de referencia a través de un acoplamiento a medida.

2.4.1 ANÁLISIS DEL MARCO DE REFERENCIA COBIT 5.0

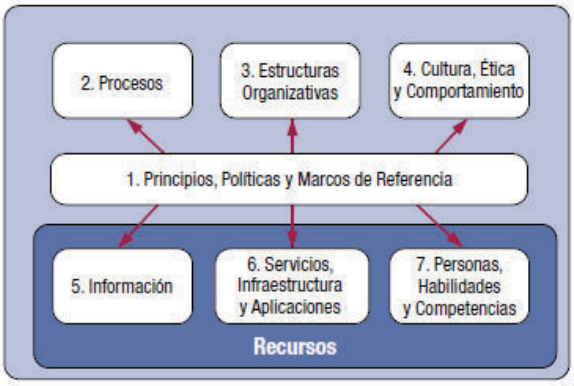
Es aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan, dando así el mayor soporte de seguridad de procesos y lineamientos de una organización.

COBIT 5.0 es un marco de referencia reconocido mundialmente cuya particularidad es que permite alcanzar las metas estratégicas de la organización mediante un gobierno y una administración de TI dentro de la organización.

Enfoque holístico a través de catalizadores.-

Los catalizadores son factores guiados por una cascada de metas. COBIT 5 describe 7 categorías de catalizadores.

Ilustración 2-7. Catalizadores de COBIT 5



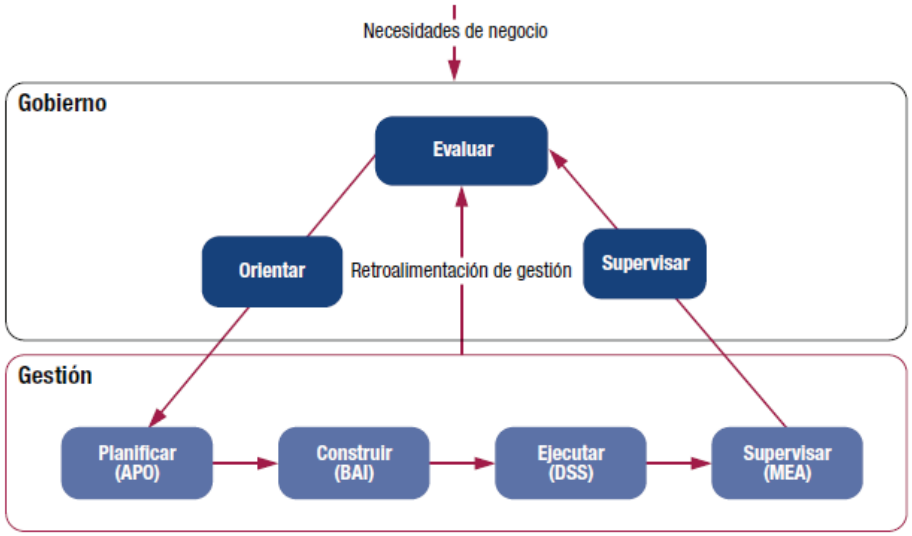
Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

Estos catalizadores pueden ser también identificados como recurso corporativos en algunas organizaciones. Estos catalizadores pueden ser utilizados en varios aspectos, entre ellos, en la información que necesita ser gestionada como un recurso.

Separación del Gobierno y la Gestión.-

En la siguiente ilustración se puede ver la separación del gobierno de la Administración propuesto por COBIT en su principio 5.

Ilustración 2-8. Áreas clave de Gobierno y Administración COBIT 5



Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

Gobierno.-

Asegura el logro de los objetivos de la organización, evaluando las necesidades las partes interesadas, condiciones y opciones, fijando directivas. En la mayoría de organizaciones el Gobierno es responsabilidad de la Junta Directiva bajo el liderazgo de su presidente. Contiene cinco procesos de gobierno y dentro de cada uno de ellos se definen prácticas de evaluación, orientación y supervisión (EDM).

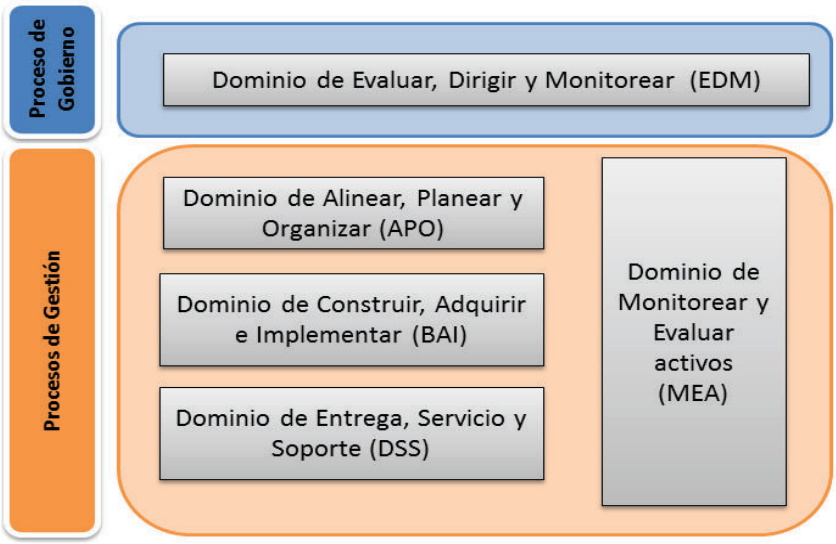
Gestión.-

Se encarga de la planificación, construcción, ejecución y monitoreo de las actividades conforme a las directivas finadas por el Gobierno, con miras a lograr los objetivos de la organización. En la mayoría de las organizaciones, la Gestión o Administración es responsabilidad de la Gerencia Ejecutiva, bajo el liderazgo del Gerente General (CEO). Por cada una de las áreas de responsabilidad, contiene cuatro dominios listados a continuación:

- Alinear, Planificar y Organizar (APO): Proporciona dirección para la entrega de soluciones y de servicios.
- Construir, Adquirir e Implementar (BAI): Proporciona soluciones y las traduce para convertirlas en servicios.
- Entregar, dar Servicio y Soporte (DSS): Recibe las soluciones y las hace utilizables por los usuarios finales.
- Supervisar, Evaluar y Valorar (MEA): Monitorea todos los procesos para asegurar que se sigue dirección elegida como la mejor.

En la siguiente ilustración se pueden observar la interrelación entre los dominios de COBIT.

Ilustración 2-9. Dominios de COBIT

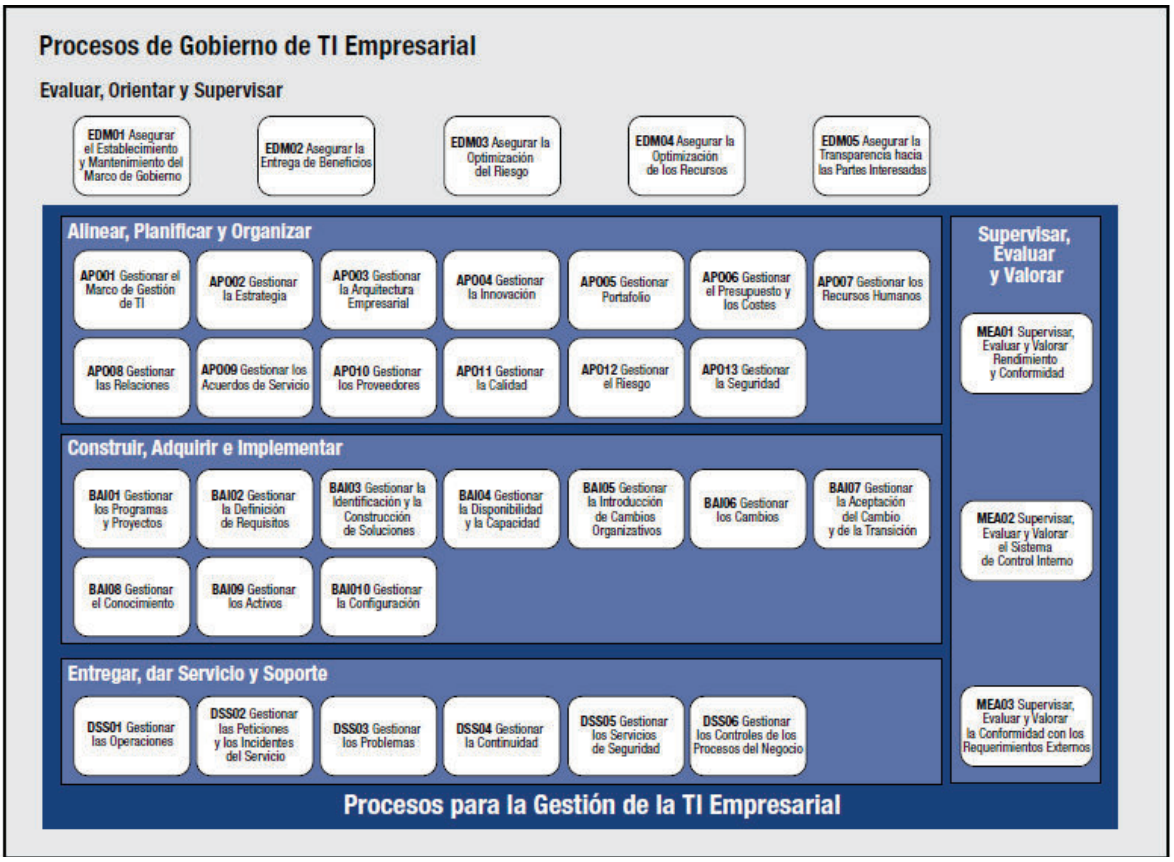


Fuente: Propia

Procesos de gobierno y gestión.-

COBIT presenta un conjunto de treinta y siete procesos de gobierno y gestión que pueden verse en la siguiente ilustración:

Ilustración 2-10. Procesos para la gestión de TI empresarial



Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

Cascada de metas.-

Para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con TI y metas catalizadoras se utiliza la cascada de metas que puede verse en la siguiente ilustración:

Ilustración 2-11. Visión general de la cascada de metas de COBIT 5

Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

Las metas corporativas de la dimensión financiera en relación con los objetivos del gobierno son las siguientes:

Ilustración 2-12. Meta corporativa y su relación con los objetivos de gobierno de COBIT 5

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

Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

En la ilustración anterior se puede determinar que la mayoría de las metas corporativas prioritariamente son susceptibles de optimizar el riesgo.

Las metas relacionadas con TI en relación con la dimensión financiera son las siguientes:

Ilustración 2-13. Metas relacionadas con TI COBIT 5

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

Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

A continuación se despliega la relación existente entre las metas corporativas y metas relacionadas con TI, calificándolas de relación principal (P) o relación secundaria (S) según corresponda.

Ilustración 2-14. Mapeo entre metas corporativas y metas relacionadas con TI. COBIT 5

			Meta corporativa				
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera
			1.	2.	3.	4.	5.
		Meta relacionada con las TI	Financiera				
Financiera	01	Alineamiento de TI y la estrategia de negocio	P	P	S		
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P	
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S		
	04	Riesgos de negocio relacionados con las TI gestionados			P	S	
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P			
	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P

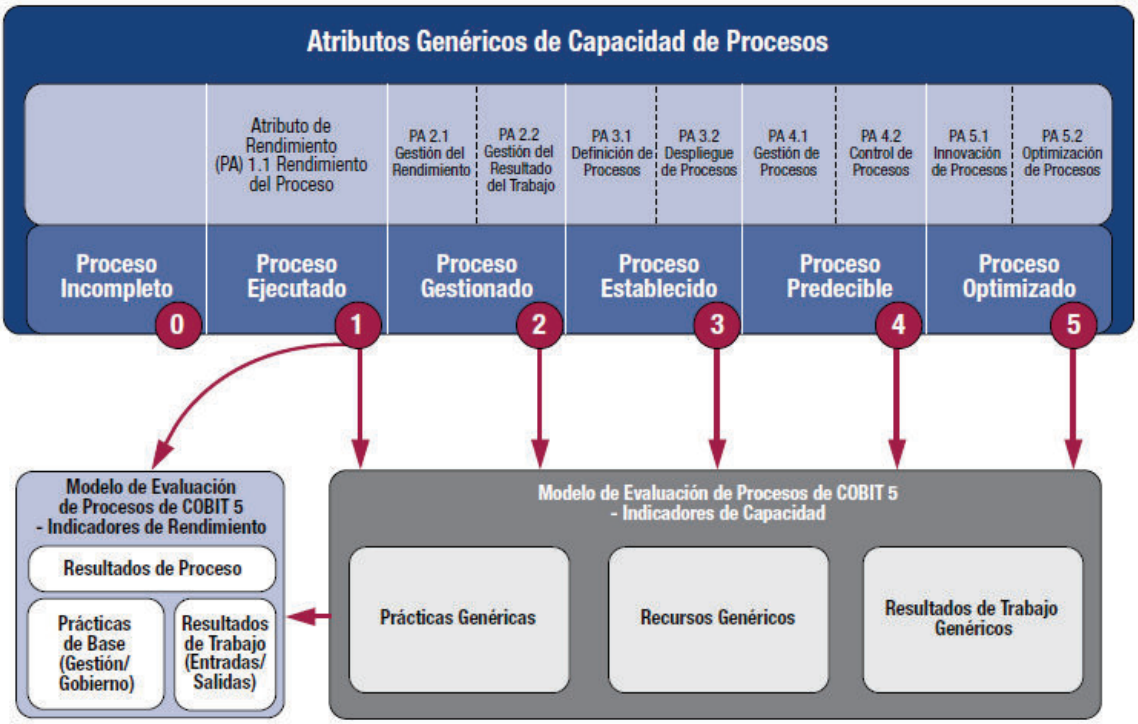
Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

Modelo de capacidad de los procesos.-

Este modelo está diseñado para alcanzar los objetivos generales de la evaluación de procesos y apoyo a la mejora misma proporcionando un medio para medir el desempeño e identificar áreas de mejora.

A continuación se presente una ilustración que resume el enfoque de COBIT 5 de capacidad de procesos:

Ilustración 2-15. Modelo Capacidad de procesos COBIT 5



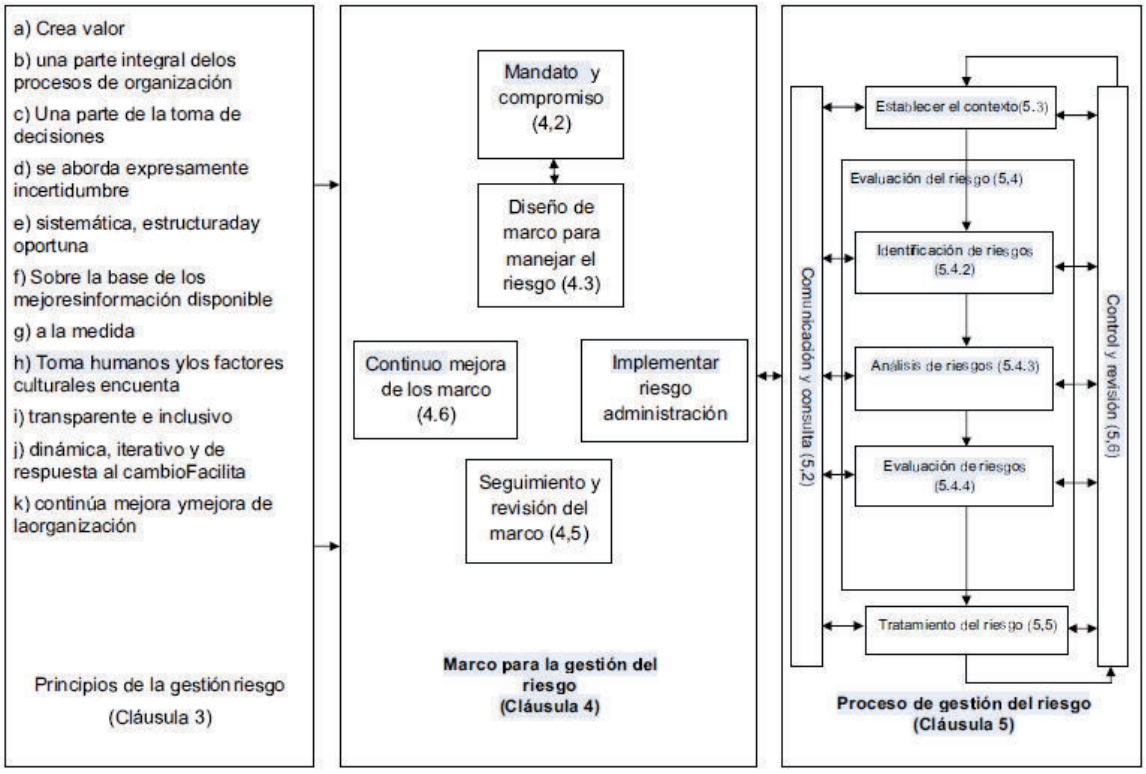
Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

2.4.2 ANÁLISIS DE LA NORMA ISO/IEC 31000

La norma ISO es un estándar internacional que tiene por objetivo orientar, coordinar, simplificar y unificar los usos para conseguir menores costos y efectividad.

La ISO 31000 está adaptado a los procesos de negocio de la organización, permite establecer el contexto, identificar, analizar, evaluar y tratar los riesgos apoyado también en los procesos estratégicos y de apoyo identificados. En la siguiente ilustración puede verse la arquitectura de ISO.

Ilustración 2-16. Arquitectura ISO/IEC 31000



Fuente: ISO 31000-2009 La gestión de riesgos – Principios y directrices

El cumplimiento de los objetivos planteados por una institución se puede ver afectados por la presencia de riesgos ocasionados por factores internos o externos.

Manejar de manera adecuada los riesgos permite el crecimiento de la organización y es por ello que resulta importante analizar el entorno, definir y valorar apropiadamente el riesgo, evaluar y tratar el mismo.

En la tercera parte de la ilustración anterior se puede ver el proceso para la gestión del riesgo de acuerdo al estándar ISO 31000.

La norma ISO 31010 es un complemento que permite profundizar en el análisis de los riesgos y de los impactos con una serie de instrumentos de gestión que se explican brevemente a continuación [7]:

Comunicación y consulta.-

Se refiere a la interrelación con las partes interesadas internas y externas que tienen lugar sobre todas las fases del proceso. Deben desarrollarse en una etapa temprana para garantizar que los responsables de la aplicación del proceso conozcan las bases para toma de decisiones.

Establecer el contexto.-

Sirve para articular y definir los objetivos internos y externos de la organización, luego de lo cual se puede establecer el alcance y los criterios de riesgo para el proceso. En este apartado se espera mayor detalle que en el apartado Marco de Gestión de esta normativa.

- Contexto externo.-

  Se basa en el contexto de toda la organización pero con detalles específicos, requisitos legales y reglamentarios. Puede incluir lo social, cultural, político, jurídico, reglamentario, nacional o internacional.

- Contexto interno.-

  Se refiere a la cultura de la organización, procesos, estructura y estrategia que influyan en la manera en la que una organización gestiona el riesgo.

- Definición de criterios de riesgo.-

  Esta definición le corresponde a la organización y deben reflejar los valores, objetivos y recursos de ella. Se espera que estos criterios sean coherentes con la política de la organización de gestión de riesgos.

Evaluación del riesgo.-

Es el proceso general de identificación, análisis, y evaluación del riesgo. La nota IEC 31010 proporciona lineamientos sobre las técnicas de evaluación de riesgos:

- Identificación del riesgo.-

  Se refiere a la identificación de las fuentes del riesgo, zonas de impactos, eventos, causas y consecuencias con el fin de generar una lista donde participen personas con conocimientos adecuados.

- Análisis de riesgos.-

Consiste en desarrollar una mayor comprensión del riesgo con el objetivo de decidir si los riesgos deben ser o no tratados. También aporta a la toma de decisiones e implica la consideración de causas y fuentes de riesgo.

- Evaluación del riesgo.-:

Su propósito es ayudar a decidir que riesgos necesitan tratamiento y la prioridad para la aplicación del tratamiento y parte de una comparación del nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo.

Tratamiento del riesgo.-

Implica un proceso cíclico de evaluación del tratamiento, aplicación y evaluación.

- Seleccionar opciones de tratamiento de riesgo:

Consiste en un equilibrio entre los costos y esfuerzos de aplicación frente a los beneficios que se obtiene. Generalmente se suelen aplicar estrategias combinadas.

- Elaborar e implementar planes de tratamientos de riesgos:

Se refiere a la documentación de cómo se llevará a cabo las opciones de tratamiento, de tal manera que se pueda hacer seguimiento de los mismos. Estos planes deben ser integrados con los procesos de gestión internos de la organización.

Seguimiento y revisión.-

Son parte planificada del proceso de gestión de riesgos. Es necesaria una definición clara del responsable del seguimiento, pues se debe asegurar que los controles sean eficaces y eficientes, se debe poder obtener más información para mejorar la evaluación de riesgos así como analizar y aprender las lecciones de los acontecimientos, detectar cambios en el contexto e identificar riesgos emergentes que puedan presentarse.

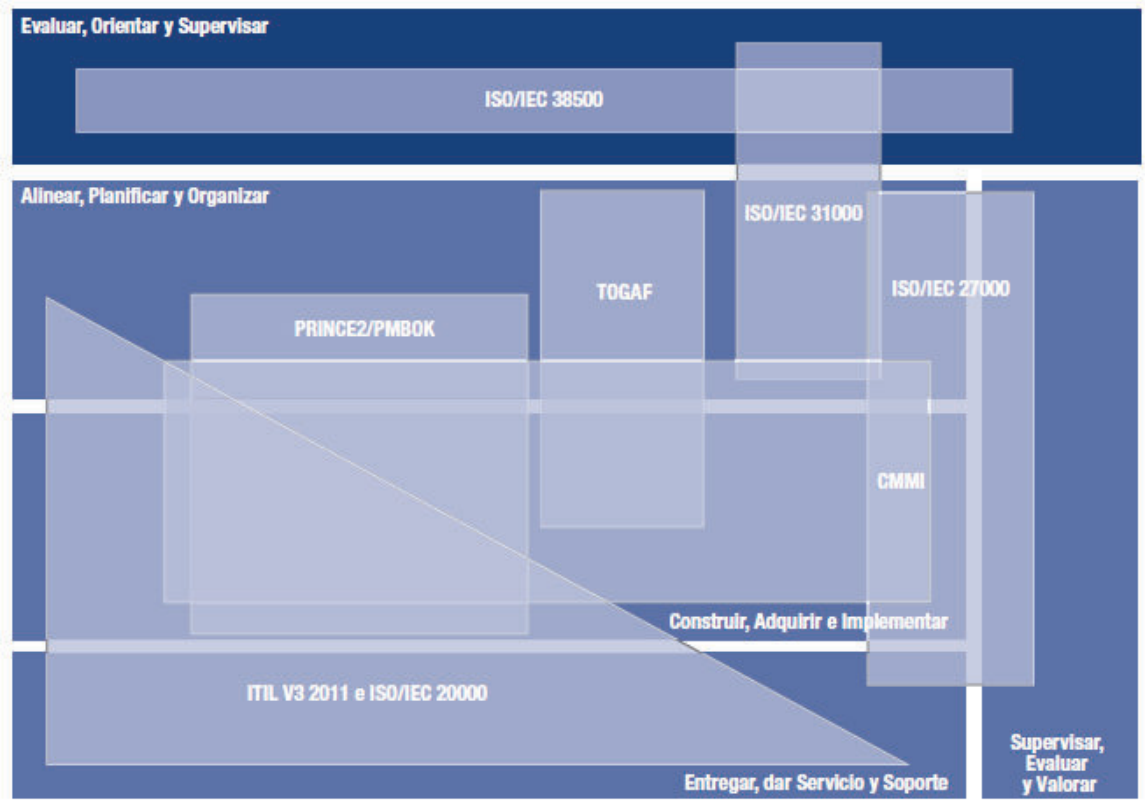
Este documento puede servir de aporte para la revisión del marco de gestión de riesgo.

2.4.3 SELECCIÓN DEL MARCO DE REFERENCIA Y NORMA PARA EL DISEÑO DEL MODELO. INTEGRACIÓN DE ISO/IEC 31000 Y COBIT 5

COBIT 5 está alineado con los últimos marcos y normas comúnmente aceptados por las organizaciones, tanto los relacionados a nivel corporativo como los relacionados con TI.

En el siguiente cuadro se puede visualizar la cobertura y relativa coincidencia de COBIT 5 de otros estándares y marcos de trabajo:

Ilustración 2-17. Cobertura de COBIT 5 de otros estándares y marcos de referencia



Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

Como se puede visualizar en la ilustración anterior, los procesos relativos a la gestión del riesgo en los dominios siguientes de COBIT 5 están cubiertos por las ISO/IEC 31000 que es la normativa relacionada con la gestión corporativa:

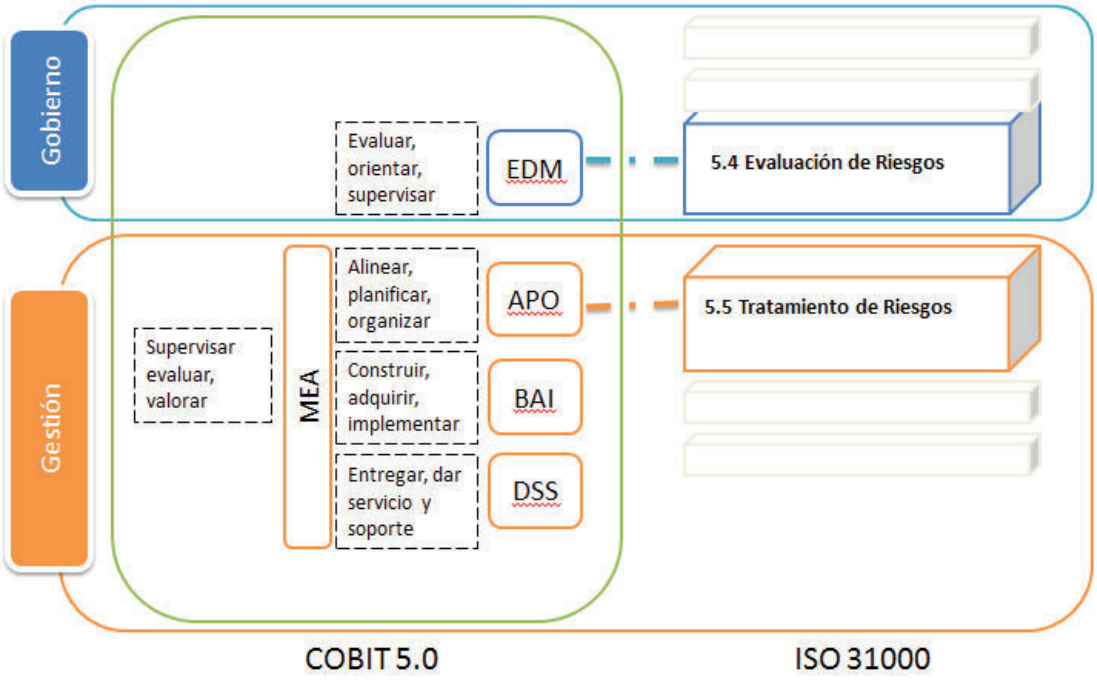
- Evaluar, Orientar, Supervisar (EDM)
- Alinear, planificar y organizar (APO)

COBIT 5 incluye objetivos de control de riesgos y para tener control sobre los riesgos es posible integrar COBIT 5 con ISO 31000 para gestionar de forma efectiva y eficiente los riesgos de TI.

A nivel de detalle este acoplamiento es posible dado que COBIT es un marco de tipo genérico que cada empresa puede utilizarlo como una guía para ajustar el modelo de procesos para la gestión del riesgo que mejor se adapte. ISO 31000 es el modelo que a juicio de la autora de este trabajo se integraría de manera natural para fortalecer el marco de referencia.

En la siguiente ilustración se hace una comparativa general que permita ver la integración mencionada anteriormente:

Ilustración 2-18. Integración COBIT 5 e ISO 31000



Fuente: Elaboración propia

2.5 DESARROLLO DE PROPUESTA DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MGSI-PUCE-DGF

Las instituciones educativas, independientemente de su tamaño o mercado objetivo están expuestas a riesgos que eventualmente afectan a la consecución de sus objetivos.

En la PUCE no existe evidencia de existir un modelo de gestión de seguridad de información propuesto o implementado que permita operativizar un adecuado nivel de control de riesgos en la información financiera como una estrategia completa de seguridad de manera holística que permita minimizar las vulnerabilidades internas y externas.

Existen esfuerzos desarticulados dirigidos a la plataforma tecnológica, al software y a la seguridad de redes, sin considerar a la información como un activo a proteger.

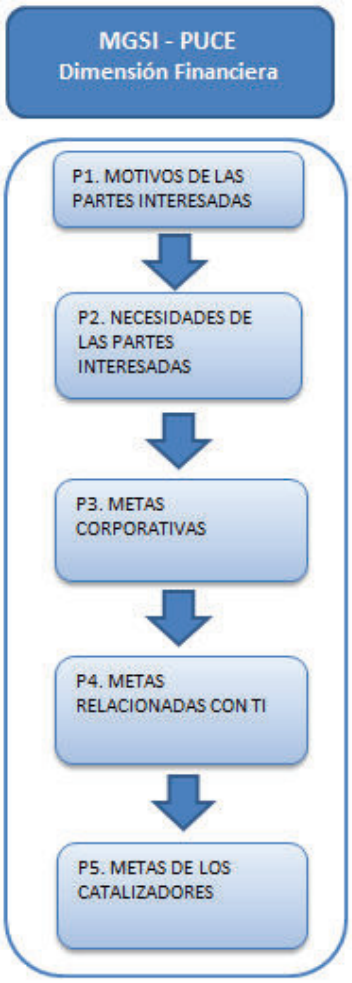
En este apartado se propone un Modelo de Gestión de Seguridad de la Información MGSI-PUCE-DGF, tiene por objetivo enmarcar al área financiera de la PUCE en una herramienta que le permita conocer los riesgos de la seguridad de información relacionada con su función con el fin de gestionar adecuadamente acciones y recursos necesarios para lograr calidad financiera.

El modelo está enmarcado en la norma internacional ISO/IEC 31000:2009 acoplado con COBIT 5 por las razones expuestas en el apartado 2.2 – Selección del marco de referencia y norma para el diseño del modelo.

Se utilizó como insumos para análisis, la documentación institucional a la que se logró acceder y se complementó el levantamiento de información con entrevistas al personal involucrado en varios niveles jerárquicos.

.

Ilustración 2-19. MGSI – PUCE (Dimensión Financiera)



FUENTE: Elaboración propia

A continuación se describe el modelo con detalle:

2.5.1 MOTIVO DE LAS PARTES INTERESADAS

En los últimos años, la Pontificia Universidad Católica del Ecuador se encuentra en un proceso de cambio y fortalecimiento de la SINAPUCE para convertirla en una verdadera red con iguales oportunidades de crecimiento y de posicionamiento a nivel nacional.

Dentro de su misión como Universidad “promueve el compromiso de todos los miembros de la comunidad universitaria para la consecución de los fines institucionales” [25], y dentro de su Plan Estratégico 2014-2018, Objetivo Estratégico 2 tiene como meta “En los próximos 5 años, perfeccionar el sistema de gestión integral del SINAPUCE a través de la implementación de buenas prácticas de gestión de infraestructura física, tecnológica, educativa y financiera,

que apoyen de manera transversal y eficiente a la comunidad universitaria en sus tareas fundamentales" [17].

Con estos antecedentes, las siguientes son las necesidades abordadas en el área financiera de la Universidad.

2.5.2 NECESIDADES DE LAS PARTES INTERESADAS

La Dirección General Financiera es responsable de la administración de todos los procesos relacionados con la gestión financiera de la Universidad. Ha realizado varios esfuerzos a lo largo de su trayectoria para maximizar sus objetivos y desempeñarse de manera eficaz y eficiente.

EL área financiera en la PUCE hizo hace algunos años, un levantamiento importante de necesidades a cubrir que sirvieron de base para la posterior implementación de ERP BAAN 5.0 para su gestión. Las necesidades a cubrir fueron [26]:

- Cultura organizacional tradicional.
- Deficiencias en la información financiera.
- Debilidades de controles internos.
- Procesos manuales e informales.
- No existe una adecuada integración.
- Tecnología de base subutilizada.

Actualmente, a criterio del personal de la Dirección General Financiera, los problemas indicados anteriormente persisten con menor grado, pero aún son retos a superar.

En la siguiente ilustración se identifican las necesidades del área financiera con respecto a los servicios de TI en coherencia con las metas corporativas propuestas por COBIT:

Ilustración 2-20. MGSI–PUCE Necesidades de las partes interesadas

P2. NECESIDADES DE LAS PARTES INTERESADAS						
	Satisfacción de la calidad de servicio de TI	x	x			
	Rendimiento de TI		x			
	Explotación tecnológica para conseguir nuevas oportunidades estratégicas	x	x			
	Dependencia de proveedores externos			x	x	
	Requisitos de control para la información				x	
	Riesgos relacionados con TI			x		
	Generación de confianza en TI				x	
	Seguridad de la información				x	
	Entorno de TI	x				
	Análisis del resultado de proyectos de TI	x	x	x		
	Deterninación de la criticidad de TI para la empresa	x	x			
	Procesos con dependencia en TI	x	x			
	Presupuestos de operación y proyectos de TI					x
	Esfuerzo de TI		x	x		
	TI y objetivos estrategicos		x		x	
P3. Metas corporativas		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 finaciera

FUENTE: Elaboración propia

2.5.2.1 Satisfacción de la calidad de servicio de TI

La cadena de valor del área está directamente relacionada por la calidad de servicios de TI, toda vez que las transacciones registradas por el área financiera están soportada por una infraestructura tecnológica importante dentro del área.

Los servicios brindados dependen de manera importante de la eficacia y eficiencia de las soluciones tecnológicas implementadas tanto dentro de la Dirección General Financiera, como fuera de ella con clientes internos y externos.

2.5.2.2 Rendimiento de TI

El rendimiento de TI puede medirse en la satisfacción de los servicios brindados por la Dirección General Financiera en dos puntos:

- Calidad de información generada.
- Oportunidad de información brindada.

2.5.2.3 Explotación tecnológica para conseguir nuevas oportunidades estratégicas

La Dirección de Informática tiene dentro de sus funciones asesorar, diseñar, desarrollar, implementar tecnología de punta que permitan mejorar la gestión universitaria.

2.5.2.4 Dependencia de proveedores externos

La dependencia de proveedores externos sobre los sistemas sensibles en la Universidad maximiza los riesgos que actualmente presenta el activo de información generada en el área financiera en términos de confidencialidad y del cumplimiento de leyes y regulaciones externas.

2.5.2.5 Requisitos de control para la información

Los organismos del estado establecen una serie de normas y regulaciones a la gestión financiera de las universidades del país, lo que exige que la institución revise constantemente la calidad de información a través de las herramientas de TI para poder sustentar cualquier transacción y gestión relacionada a ella.

2.5.2.6 Riesgos relacionados con TI

La contemplación de los riesgos relacionados con TI relacionados con la salvaguarda de sus activos de su información, es una función que recae actualmente en la Dirección de Informática, cuyas acciones se encuentran soportadas en las políticas y normativas que para el efecto emite la Oficina de Seguridad de la Información. Auditoria Interna en su planificación actual, revisa los riesgos relacionados con TI.

2.5.2.7 Generación de confianza en TI

La confianza en TI en relación con el cumplimiento de leyes y regulaciones externas es importante para el área financiera institucional, toda vez que su operación y evidencia transaccional se generan a través de medios tecnológicos.

2.5.2.8 Seguridad de la información

La seguridad de información es una responsabilidad compartida directa de los usuarios de la Dirección General Financiera, la Dirección de Informática y de la Oficina de Seguridad de la Información.

2.5.2.9 Entorno de TI

La capacidad de respuesta de la Universidad y sus procesos pueden mejorar mediante un entorno de TI con mayor flexibilidad, y como consecuencia lograr beneficios en su cadena de valor.

2.5.2.10 Análisis del resultado de proyectos de TI

Los proyectos de TI se formulan a través de planes operativos anuales y son considerados estratégicos para el desarrollo institucional. Su éxito o fracaso impactan de manera profunda entre los clientes internos relacionados con dichos proyectos.

2.5.2.11 Determinación de la criticidad de TI para la empresa

La tendencia institucional da cuenta de la importancia de TI dentro de la Universidad. Esta área se ha convertido en un punto crítico en la mayor parte de procesos de la vida institucional.

2.5.2.12 Procesos con dependencia en TI

Los macro procesos que dependen de TI en la Dirección General Financiera son:

- Procesos del área contable.
- Procesos del área de presupuestos.
- Procesos del área de tesorería.
- Procesos del área de adquisiciones.
- Procesos del área de control de activos.

2.5.2.13 Presupuestos de operación y proyectos de TI

El control del presupuesto de operación de TI es responsabilidad de la alta gerencia universitaria y Dirección General Financiera. Los ajustes a las asignaciones presupuestarias para TI se hacen de acuerdo a las necesidades y argumentaciones indicadas por la Dirección de Informática.

2.5.2.14 Esfuerzo de TI

Los esfuerzos de la Dirección General Financiera se reflejan en el plan de trabajo interno que permite organizar internamente los recursos asignados.

2.5.2.15 TI y objetivos estratégicos

La Dirección de Informática presenta ante la Dirección General Financiera los recursos e infraestructura requerida para conseguir los objetivos estratégicos que requiere la Universidad.

2.5.3 METAS INSTITUCIONALES

Las metas institucionales a nivel universitario son varias y se reflejan en el PEDI institucional indicadas en el *Anexo 1*.

A continuación se describen las metas del área a nivel de detalle [26]:

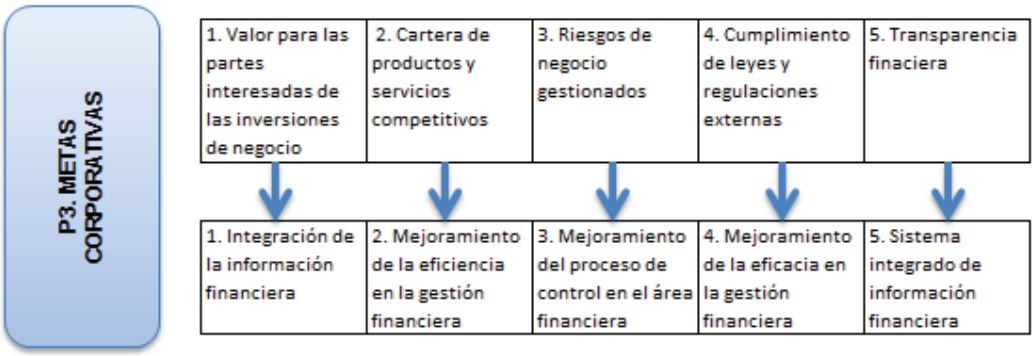
- Implementar un Sistema Integrado de Información Financiera.
- Elaborar un Modelo de Control Financiero adecuado a las necesidades de la PUCE.
- Establecer Políticas para regular los nuevos procesos.
- Asegurar Información Financiera de Calidad.
- Integrar las Áreas de Presupuesto, Contabilidad, Tesorería, Adquisiciones y Control de Activos.
- Integrar los Sistemas de Nómina y Académico a través de interfaces.
- Lograr satisfacción de los clientes internos y externos.

Después de analizar las metas anteriores con las necesidades actuales planteadas por los directivos, se pudieron establecer las siguientes metas:

- Integración de la información financiera.
- Mejoramiento de la gestión en términos de eficacia y eficiencia.
- Mejoramiento del área de control del área financiera
- Implementación de un sistema integrado de información financiera.

Las metas del área financiera han sido relacionadas en términos de las metas corporativas de COBIT de la siguiente manera:

Ilustración 2-21. MGSI–PUCE Metas corporativas



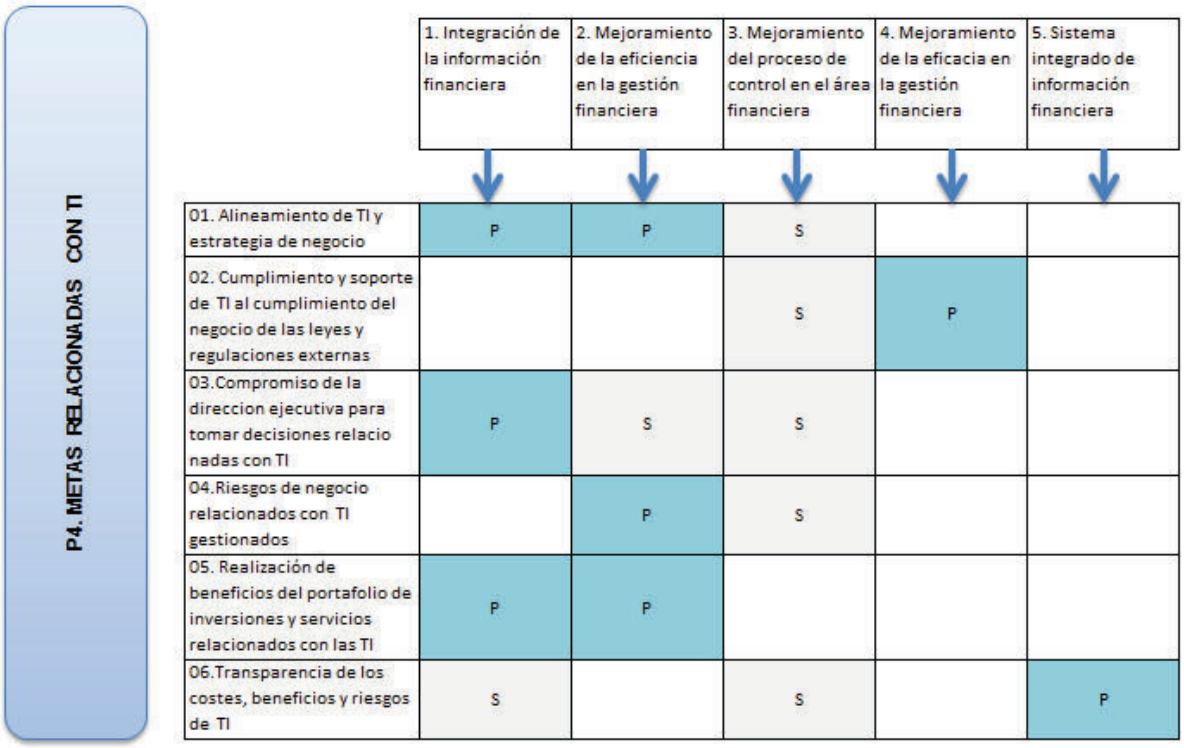
FUENTE: Elaboración propia

2.5.4 METAS RELACIONADAS CON TI

Varias de las metas de la Dirección General Financiera son soportadas por las metas de TI propuestas por el modelo.

En la siguiente ilustración se puede observar la correspondencia entre las metas relacionadas con TI y las metas de la Dirección General Financiera; en ella se han identificado las relaciones principales (P) y secundarias (S):

Ilustración 2-22. MGSI–PUCE Metas relacionadas con TI



	1. Integración de la información financiera	2. Mejoramiento de la eficiencia en la gestión financiera	3. Mejoramiento del proceso de control en el área financiera	4. Mejoramiento de la eficacia en la gestión financiera	5. Sistema integrado de información financiera
01. Alineamiento de TI y estrategia de negocio	P	P	S		
02. Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P	
03.Compromiso de la direccion ejecutiva para tomar decisiones relacionadas con TI	P	S	S		
04.Riesgos de negocio relacionados con TI gestionados		P	S		
05. Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	P	P			
06.Transparencia de los costes, beneficios y riesgos de TI	S		S		P

FUENTE: Elaboración propia

A continuación se consideran las metas de TI de mayor incidencia en la Dirección General Financiera de la Universidad, es decir, aquellas identificadas con relación principal o fuerte:

2.5.4.1. Alineamiento de TI y estrategia de negocio

La meta 01- Alineación de TI y estrategia de negocio, está relacionada principalmente con las metas financieras: Integración de la información y mejoramiento de la eficiencia financiera.

2.5.4.2. Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas

La meta 02- Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas, está relacionada principalmente con la meta financiera: Mejoramiento de la eficacia en la gestión financiera.

2.5.4.3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI

La meta 03- Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI, está relacionada principalmente con meta financiera: integración de la información financiera.

2.5.4.4. Riesgos de negocio relacionados con las TI gestionados

La meta 04- Riesgos de negocio relacionados con TI gestionados, está relacionada principalmente con la meta financiera: mejoramiento de la eficiencia en la gestión financiera.

2.5.4.5. Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI

La meta 05- Realización de beneficios del portafolio de inversiones y servicios relacionados con TI, está relacionada principalmente con las metas financieras: integración de la información financiera y el mejoramiento de la eficiencia en la gestión financiera.

2.5.4.6. Transparencia de los costes, beneficios y riesgos de las TI

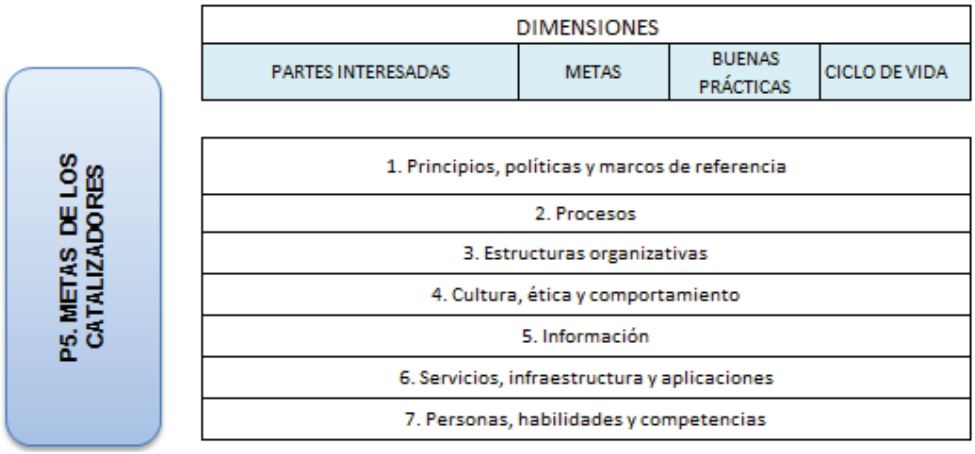
La meta 06- Transparencia de los costes, beneficios y riesgos de TI, está relacionada principalmente con la meta financiera: implementación de un sistema integrado de información financiera.

2.5.5 METAS DE LOS CATALIZADORES

Las metas de los catalizadores giran alrededor de cuatro dimensiones que van tomando protagonismo en la medida en la que el catalizador es analizado y son: Partes interesadas, metas, buenas prácticas y ciclo de vida.

En la siguiente ilustración se visualizan en detalle las metas de los catalizadores:

Ilustración 2-23. MGSI–PUCE Metas de los catalizadores



FUENTE: Elaboración propia

2.5.5.1. Principios, políticas y marcos de referencia

Son los mecanismos de comunicación disponibles para transmitir la dirección e instrucciones.

Los marcos de gestión y gobierno institucionales están dados por el Consejo Superior, Rectorado, Vicerrectorado. Estas instancias son las llamadas a proporcionar a la Direcciones Generales y Dirección de Informática: estructura, directrices, herramientas con las siguientes características:

- Cubriendo las áreas necesarias.
- Permitiendo adaptación a una situación específica requerida.
- Alineados a los objetivos institucionales.

Disponibles y de fácil acceso para las partes interesadas permitiendo la gestión.

Las directrices o declaraciones de política proporcionan directrices para llevar a la práctica los principios y determinan o influencian en la toma de decisiones alineadas a estos principios. Se espera que las políticas cumplan con las siguientes propiedades:

- Logran su propósito de manera efectiva.
- Garantizan que los principios se implemente de manera eficiente.
- No generan resistencia.

Las políticas tienen un ciclo de vida para el apoyo a las metas institucionales definidas y deben alinearse a los requerimientos normativos existentes que

deriven controles internos de distinta intensidad, mismas que deberán estar actualizadas constantemente a través de mecanismos que garanticen su difusión y conocimiento del personal involucrado.

Las buenas prácticas requieren que las políticas formen parte del marco de gobierno y de gestión. Un marco de políticas adecuado debe considerar:

- Definición del alcance y periodo de validez.
- Efectos de la no adopción de la política.
- Buen manejo de excepciones.
- Métricas para medir el cumplimiento de la política.

Al momento no existe un repositorio integrado de políticas institucionales y ni un control riguroso de versiones, validez y efectos de las mismas. En una entrevista a directivos claves se pudo determinar que varias políticas en la Universidad no se encuentran escritas, sin embargo se practican.

2.5.5.2. Identificación de procesos del área financiera en relación con TI

Un proceso se define como "una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de un número dado de fuentes (incluyéndose otros procesos), manipulando las entradas y produciendo salidas" [3].

En la siguiente ilustración se visualiza el acoplamiento de ISO 31000 con COBIT 5.0 para el modelo MGSI-PUCE-DGF. Los procesos de COBIT 5.0 son analizados desde la perspectiva del riesgo a través de la evaluación, tratamiento y seguimiento de los riesgos asociados a dichos procesos:

Ilustración 2-24. MGSI–PUCE Procesos

P5.2 PROCESOS

ORGANIZACIÓN DE TI	DOMINIOS	PROCESOS	GESTIÓN DEL RIESGO ISO/IEC 31000
GOBIERNO	EVALUAR, DIRIGIR Y MONITOREAR	EDM03.Asegurar la optimización del riesgo	5.2 Comunicación y consulta 5.3 Establecimiento del contexto 5.4 Evaluación de riesgos 5.5 Tratamiento del riesgo 5.6 Seguimiento y revisión
GESTIÓN	ALINEAR, PLANIFICAR Y ORGANIZAR	AP011. Gestionar la calidad	
		AP012. Gestionar el riesgo	
		AP013. Gestionar la seguridad	
	CONSTRUIR, ADQUIRIR, IMPLEMENTAR	BAI01. Gestionar los programas y proyectos	
		BAI06. Gestionar los cambios	
	ENTREGAR, DAR SERVICIO, SOPORTE	DSS05. Gestionar los servicios de seguridad	
		DSS06. Gestionar los controles de los procesos de negocio.	

FUENTE: Elaboración propia

En cada proceso es posible identificar las partes interesadas relacionadas con dichos procesos y que pueden ser internos o externos dependiendo de sus características.

En la Universidad no existe un levantamiento formal de procesos y no todos los procesos se avizoran, por lo que los costos de operación son elevados, se dificulta mantener la calidad del servicio, se producen incumplimientos, genera roces internos e individualidades y lo urgente se sobrepone a lo importante.

Las metas de los procesos se refieren a los resultados de dichos procesos y apoyan a las metas relacionadas con TI de acuerdo a la cascada de metas.

Los procesos relevantes de considerar para la gestión financiera en relación con TI surgen de la interpretación de las matrices de COBIT 5.0 tomando en cuenta aquellas cuya importancia caen en categoría principal y son:

Tabla 2-5. Descripción de procesos COBIT adaptados al MGSI-PUCE-DGF

DOMINIO PRINCIPAL		PROCESO	DESCRIPCIÓN
Gobierno	EDM	03. Asegurar la optimización del riesgo	Asegurar que la tolerancia al riesgo de la institución ha sido identificado y gestionado y son entendidos, articulados y comunicados
Gestión	APO	11. Gestionar la calidad	Definir los requisitos de calidad en los procesos y comunicar a los involucrados. Asegurar la entrega de soluciones que satisfagan a las necesidades de las partes interesadas.
		12. Gestionar el riesgo	Identificar, evaluar y reducir los riesgos relacionados con TI.
		13. Gestionar la seguridad	Definir, operar u supervisar un sistema para la gestión de la seguridad de la información.
	BAI	01. Gestionar los programas y proyectos	Alcanzar los beneficios de la institución reduciendo el riesgo de retrasos y costos no planificados.
		06. Gestionar los cambios	Ejecutar cambios en relación con los procesos de la institución de manera controlada
	DSS	05. Gestionar los servicios de seguridad	Proteger la información de la institución para mantener un control de riesgos de acuerdo a las políticas y normativas institucionales.
		06. Gestionar los controles de los procesos de negocio	Establecer y mantener controles de procesos dentro de la institución para asegurar la satisfacción de los requerimientos.

Fuente: Elaboración propia

Cada proceso tiene su ciclo de vida y éstas dependen de la normativa empleada.

Una vez que se han identificado los procesos críticos de la institución, es necesario evaluar su madurez. COBIT 5.0 trae un modelo de madurez en base a niveles de capacidad, en el cual el nivel más bajo es el Nivel 0.- Proceso incompleto, mientras COBIT 4.0 se maneja a base a niveles de madurez cuyo nivel más bajo es el Nivel 0.- No existente. La siguiente tabla muestra una comparativa entre los modelos de madurez de COBIT 4.0 y COBIT 5.0.

Tabla 2-6. Comparación modelos de madurez COBIT 4.0 y 5.0

	MODELO DE MADUREZ	
	COBIT 4.0	**COBIT 5.0**
	MODELO DE MADUREZ	**MODELO DE CAPACIDAD**
NIVEL (0 a 5)	0. No existe 1. Ad-hoc 2. Repetible 3. Definido 4. Gestionado **5.** Optimizado	0. Proceso incompleto 1. Proceso desarrollado 2. Proceso gestionado 3. Proceso establecido 4. Proceso predecible **5.** Proceso en optimización
ESCALA N = No se alcanzó P: Se alcanzó parcialmente L: Alcanzado en gran medida F: Totalmente alcanzado	N: 0%-15% P: >15% al 50% L: >50% al 85% F: >85% al 100%	N: 0%-15% P: >15% al 50% L: >50% al 85% F: >85% al 100%

Fuente: Elaboración propia

A continuación se presenta una tabla adaptada de COBIT 5.0 que permita documentar los procesos en la PUCE. En esta tabla es posible determinar la interpretación de los niveles de madurez que puede alcanzar un proceso en función de su medición:

Tabla 2-7. Nivel de madurez y medición de un proceso

NIVEL DE MADUREZ	DESCRIPCIÓN DEL PROCESO	NIVEL DE MEDICIÓN			
		No alcanzado	Alcanzado parcialmente	Alcanzado en gran medida	Totalmente alcanzado
		0% A 15%	>15% al 50%	>50% al 85%	>85% al 100%
N0 Incompleto	No implementado o no ha conseguido su propósito.				
N1 Desarrollado	Ha conseguido su propósito.				
N2 Gestionado	Ha sido implementado, planificado, monitoreado y ajustado				
N3 Establecido	Ha sido implementado, planificado, monitoreado y ajustado y se usa un proceso para la obtención de resultados.				
N4 Predecible	Opera dentro de los límites y alcanza los resultados deseados				
N5 Optimizado	Es predecible y mejora continuamente				

Fuente: ISACA, COBIT Assessment Programme (PAM) Tool Kit: Using COBIT 5

En un trabajo preliminar realizado a los procesos críticos de la Dirección de Informática de la PUCE [21] y que están desplegados en el *Anexo 2 y Anexo 3*, los autores indican que para discriminar los procesos más críticos dieron un peso mayor al componente de desempeño e importancia (50%) y 6,25 a cada una de las demás. Filtrando los resultados del estudio indicado se obtuvieron seis procesos críticos; para este modelo los procesos de mayor criticidad coinciden con dos de ellos de entre los seleccionados:

- Proceso relacionado con el gobierno: EDM03 - Asegurar la optimización del riesgo.
- Proceso relacionado con la gestión: APO13 - Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

Considerando el mapeo entre metas corporativas y metas relacionadas con TI - COBIT 5 que se visualiza en la sección 2.2.1- Análisis del marco de referencia, se tiene que:

El proceso AP013 - Gestión de la Seguridad, contribuye principalmente a la consecución de las siguientes metas relacionadas con TI:

- 02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
- 04 Riesgos de negocio relacionados con las TI gestionados.
- 06 Transparencia de los costes, beneficios y riesgos de TI.

El proceso EDM03 – Asegurar la optimización del riesgo contribuye:

Principalmente a la consecución de las siguientes metas relacionadas con TI:

- 04 Riesgos de negocio relacionados con las TI gestionados.
- 06 Transparencia de los costes, beneficios y riesgos de TI.

Secundariamente a la consecución de las siguientes metas relacionadas con TI:

- Valor para las partes interesadas de las Inversiones de Negocio.
- Cartera de productos y servicios competitivos.
- Riesgos de negocio gestionados (salvaguarda de activos).

La relación entre los procesos críticos y su contribución a la consecución de metas de TI, dan cuenta de que el área TI está relacionada fuertemente con los riesgos propios del negocio. El compromiso de TI debe girar al cumplimiento de los siguientes propósitos relacionados:

- Asegurar que los riesgos relacionados con TI de la PUCE no exceden ni el apetito ni la tolerancia del riesgo, que el impacto de los riesgos de TI en el valor de la Universidad se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.
- Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa

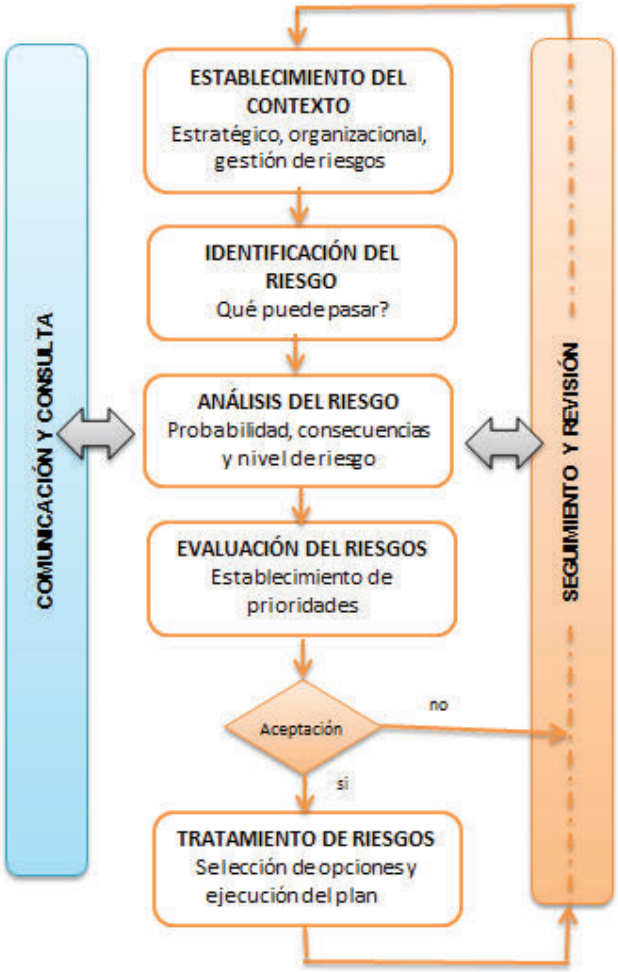
2.5.5.3. Gestión de riesgos

Son todas las actividades orientadas a minimizar el riesgo en una institución y deben cumplir con los siguientes principios:

- Crear valor y proteger.
- Ser una parte integral de todos los procesos de la institución.
- Ser parte de la toma de decisiones.
- Ser transparente e inclusivo.
- Ser dinámico, interactivo y dar respuesta al cambio.

En la siguiente ilustración se visualiza el ciclo de vida de la gestión de riesgo propuesta a partir de ISO 31000:

Ilustración 2-25. Ciclo de vida de la gestión del riesgo



Fuente: Elaboración propia

2.5.5.3.1 Establecimiento del contexto

Son las condiciones que pueden generar eventos que afectan positiva o negativamente el cumplimiento de la misión y objetivos de la institución. Los factores de riesgos que se extraen dentro del análisis del contexto pueden ser de tipo interno o externo.

El contexto estratégico define la relación que existe entre la universidad y el entorno sobre el cual gira, mientras que el contexto institucional se refiere a las metas, objetivos y estrategias implementadas para su consecución.

a) Determinación del contexto estratégico e institucional

La PUCE forma parte de las universidades cofinanciadas ecuatorianas porque a pesar de ser privada, recibe fondos estatales, mismos que son considerados

dentro del presupuesto, por tanto está regulada a través de varias instancias gubernamentales, entre ellas: la Secretaría Nacional de Planificación y Desarrollo (SENPLADES), la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) y el Consejo de Educación Superior (CES). El estado solicita a través de estos organismos la rendición de cuentas del uso de los fondos entregados, y regula las operaciones universitarias.

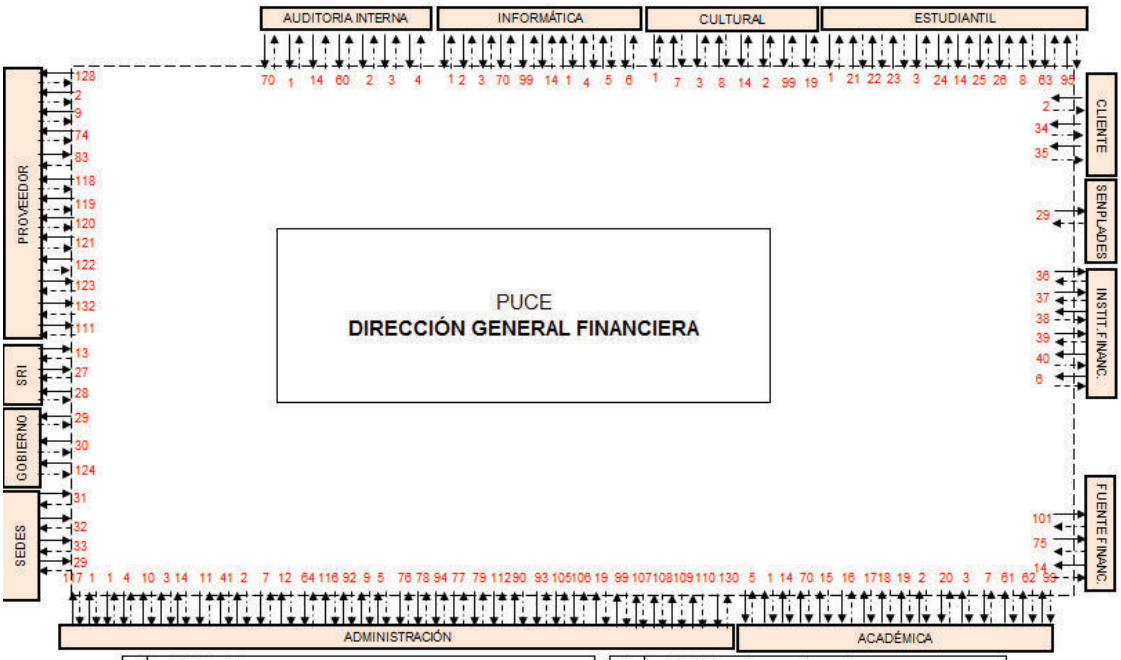
Adicionalmente la Universidad ha firmado varios convenios con organizaciones internacionales especialmente para la consecución de proyectos de investigación que requieren que la administración central administre los fondos destinados a estos proyectos y presente informes de acuerdo a las exigencias internacionales.

La PUCE atiende a los requerimientos estatales e internacionales de la mejor manera posible, a pesar de las limitaciones de tipo operativa que al interior de la institución se pueda presentar para el procesamiento de la información solicitada.

La Dirección General Financiera de la PUCE está relacionada por su función con varias áreas internas y entidades externas a la Universidad. Estas áreas y entidades demandan una cantidad importante de información, lo que conlleva a necesitar que la misma se trate de manera eficaz y eficiente.

En la ilustración siguiente puede visualizarse el ciclo de requerimientos y respuestas que demandan y se demandan de las unidades externas al área financiera:

Ilustración 2-26. Dirección General Financiera - Ciclos de requerimiento y respuesta



1	Solicitud Uso Presupuesto
2	Solicitud Compra de Bienes y Servicios
3	Solicitud validación documentos compras bienes y servicios
4	Solicitud Distribución de gastos
5	Solicitud Especificaciones Técnicas
6	Envio Informacion Hoja Electronica al Banco
7	Solicitud de reportes y documentos sobre Facturación
8	Solicitud Depósito Ingresos Varios
9	Solicitud Reclamos y Devoluciones
10	Solicitud Disponibilidad de Fondos
11	Solicitud de reportes y documentos para conciliación
12	Depósito Recuperación Seguros
13	Solicitud Declaración de Impuestos
14	Solicitud Informes de Saldos y Liquidaciones
15	Solicitud Elaboración Presupuestos Maestrias y Postgrados
16	Solicitud presupuesto educación continua
17	Solicitud Elaboración Presupuestos para Proyectos con Financ. Externo
18	Validacion aranceles e impedimentos en Hojas de Credito
19	Solicitud Elaboracion presupuesto proyectos con financ. PUCE
20	Solicitud notificacion de Postgrados Maestrias y Carreras
21	Solicitud de aranceles
22	Solicitud Valor Bonificacion para Becarios
23	Solicitud listado estudiantes en entrenamiento
24	Solicitud Informacion Financiera para Aranceles
25	Solicitud Devolución de Aranceles
26	Solicitud Factura y Depósito por eventos
27	Solicitud documentos de respaldo
28	Solicitud Devolución IVA
29	Solicitud Informacion Subvención Estado
30	Solicitud Transferencia Asignaciones
31	Solicitud Informe Asignaciones
32	Solicitud Pago Asignación
33	Solicitud de descuento por Legalización de Títulos
34	Solicitud Pago Devolución de Aranceles
35	Solicitud de Facturación y Cobro
36	Solicitud Servicios Bancarios y Financieros
37	Solicitud Información Financiera
38	Solicitud Datos de Hoja Credito Matriculados
39	Solicitud Datos de Matriculados
40	Solicitud Confirmacion datos y saldos
41	Solicitud Pago de Planillas

60	Solicitud Informacion para Control
61	Emisión de Garantias Bancarias
62	Solicitud emisión facturas a crédito
63	Solicitud ingreso de aranceles
64	Solicitud información pagos futuro
70	Solicitud Presupuesto Aprobado para Proyectos Espec.
74	Compra tercerizada útiles de oficina
75	Solicitud de depósito
76	Solicitud Suministros y Materiales
77	Reutilización Activos Fijos
78	Solicitud de Transferencia de Activos Fijos
79	Solicitud de Control Físico de Activos
83	Solicitud pago por bienes y servicios
90	Solicitud de Ajustes
92	Solicitud estados financieros
93	Solicitud Calculo Depreciación
94	Solicitud Entrega Activos Fijos
95	Solicitud becarios
99	Solicitud Transferencia de Partidas
101	Solicitud de desembolso
105	Solicitud Valoracion Gastos para proforma presupuestaria
106	Envio proforma presupuestaria para aprobacion
107	Solicitud Solicitud Avance Presupuestario y Proyecciones
108	Solicitud Liquidacion Anual y Evaluacion presupuestaria
109	Solicitud de proforma de postgrados para aprobación
110	Solicitud de Proforma Presupuestaria proximo año
111	Solicitud alcance del Cupo de Compra
112	Recepción de Bienes y Materiales
116	Solicitud Informacion vigencia de garantias de equipos
117	Informe de Casas Comerciales para mantenimiento
118	Solicitud Documentos Calificación Proveedores
119	Solicitud Cotización
120	Envio orden de compra
121	Solicitud servicio de post-venta
122	Solicitud informes estadísticos
123	Solicitud Tramite Pago
124	Solicitud autorización importación donaciones
128	Solicitud canje facturas
130	Distribución Consumo de Suministros y Materiales
132	Solicitud Cupos para Compra Tercerizada utiles oficina

Fuente: Elaboración propia

Insumos para el establecimiento del contexto estratégico e institucional, tales como organización, planificación, auditoría, gestión de seguridad, gestión de TI y gestión financiera se desarrollaron con detalle en el apartado 2.1 – Situación actual institucional.

De acuerdo al análisis de los elementos que conforman el contexto estratégico e institucional, es necesario identificar los factores externos e internos que incidan en la presencia de riesgos, de acuerdo a los objetivos estratégicos, operacionales, informativos y de cumplimiento.

La siguiente es una tabla propuesta que permita dar respuesta a la identificación de factores de ocasionen riesgo:

Tabla 2-8. Inventario de factores internos y externos en relación al riesgo

OBJETIVOS DE LA UNIVERSIDAD	TIPO DE FACTOR (Interno o Externo)	CAUSAS
ESTRATÉGICOS: - -		
OPERACIONALES: - -		
INFORMATIVOS: - -		
CUMPLIMIENTO: - -		

Fuente: Elaboración propia

b) Determinación del contexto de gestión de riesgos

Se establece los objetivos, estrategias, alcance y parámetros de las actividades donde se desarrolla el proceso de gestión de riesgos. En este apartado es necesario justificar los recursos asignados a esta gestión.

Los componentes del proceso de gestión de riesgos son:

- Políticas establecidas para la gestión del riesgo
- Metodología para evaluar la gestión del riesgo.

Con respecto a las políticas establecidas para la gestión del riesgo, éstas deben establecerse a través de la alta dirección institucional y deben abordar aspectos como la filosofía de la gestión del riesgo, metas, objetivos,

actividades y responsabilidades relativas a la gestión de riesgos de acuerdo al organigrama institucional.

Las políticas con respecto a la seguridad de la información del área financiera y sus riesgos, deben ser definidas por la Oficina de Seguridad de la Información en coordinación con la Dirección de Informática y Dirección General Financiera y aprobadas por la alta gerencia, esto es, el vicerrectorado.

Con respecto a la definición de la metodología para evaluar el riesgo, ésta puede definirse a través de la elección de una metodología existente o una metodología propia institucional, que debe estar a cargo y consensuadas por las mismas instancias que definen las políticas, con el fin de operativizar los compromisos.

c) Determinación de los criterios del riesgo

Es importante establecer los criterios que utilizará la institución para evaluar el riesgo. Esta evaluación debe reflejar los valores de la organización, objetivos y recursos y ser coherentes con la política de organización de gestión de riesgos.

Los factores que se sugiere considerar en este apartado se visualizan en la siguiente tabla:

Tabla 2-9. Determinación de los criterios del riesgo

CRITERIOS DEL RIEGO	CAUSAS	CONSECUENCIAS	PROBABILIDAD DE OCURRENCIA	PLAZO DE OCURRENCIA	CALIFICACIÓN DEL NIVEL DE RIESGO

Fuente: Elaboración propia

2.5.5.3.2 Evaluación del riesgo

La evaluación del riesgo es el proceso que integra la identificación, análisis y evaluación de un conjunto de riesgos a detalle.

El riesgo es el efecto de la incertidumbre en la consecución de los objetivos. [7].

Los criterios de riesgo pueden tener dos fuentes: aquellos derivados de la legislación estatal y aquellos establecidos por la universidad y deben ser coherentes con la política de riesgo aprobada por la institución.

2.5.5.3.2.1 Identificación de riesgos

La institución debe establecer cuáles son las posibles fuentes de riesgo, sitios de impactos, eventos que los producen, causas y consecuencias a través de un listado donde participe el personal relacionado.

El objetivo de esta fase es predecir o adelantarse a los posibles escenarios que puedan afectar el logro de los objetivos de la institución.

Para que esa fase tenga éxito es importante que se la considere en un proceso cíclico e interactivo, tomando siempre como referencia el contexto y sin dejar de lado los factores que han entorpecido la consecución de los objetivos.

A continuación se sugiere una tabla guía para identificar el riesgo, por cada uno de los procesos identificados:

Tabla 2-10. Preguntas orientadoras para identificar riesgos

PROCESO:	
PREGUNTAS ORIENTADORAS	**IDENTIFICACIÓN DE EVENTOS DE RIESGO**
¿Qué puede suceder?	
¿Cuáles son las fuentes de riesgos?	
¿Cuáles son las áreas de impacto?	
¿Cómo o por qué puede suceder?	

Fuente: Elaboración propia

2.5.5.3.2.2 Análisis de riesgo

Consiste en comprender el riesgo, sus causas y consecuencias (tangibles o intangibles) a través de información identificada previamente.

El riesgo puede ser clasificado en los siguientes:

- Riesgo de cumplimiento: Eventos que afectan al cumplimiento de requisitos de la institución.
- Riesgos estratégicos: Eventos que afectan al cumplimiento de los objetivos estratégicos de la institución.

- Riesgos financieros: Eventos que afectan al manejo de recursos financieros de la institución.
- Riesgos operativos: Eventos que afectan la operatividad de la institución.
- Riesgos tecnológicos: Eventos que se asocian con la capacidad tecnológica para satisfacer los objetivos institucionales.

A continuación se sugiere una tabla guía para analizar cada uno de los riesgos identificados por cada uno de los procesos:

Tabla 2-11. Análisis de riesgos

PROCESO:	
RIESGO:	
TIPO DE RIESGO: (Cumplimiento, Estratégico, Operativo, Financiero, Tecnológico)	

CAUSA (Recurso humano, financiero, tecnológico, procedimientos, infraestructura, factores externos…)	**EFECTO (pérdidas económicas, de información, de imagen, sanciones…)**

Fuente: Elaboración propia

2.5.5.3.2.3 Evaluación de riesgos

Su propósito es proporcionar insumos para la toma de decisiones que deben tener en cuenta el contexto, aquellos riesgos que se asumen y el entorno legal.

Para evaluar el riesgo es necesario analizar dos aspectos:

- Probabilidad: Se mide por la frecuencia en la que puede ocurrir el evento del riesgo.
- Impacto: Se mide por el grado en que la ocurrencia de evento del riesgo pueda perjudicar a la institución.

A continuación se sugiere una matriz guía para evaluar riesgo, por cada uno de los procesos identificados:

Tabla 2-12. Matriz para evaluación de riesgos

PROCESO:						
RIESGO:						
TIPO DE RIESGO: (Cumplimiento, Estratégico, Operativo, Financiero, Tecnológico)						
PROBABILIDAD	**FRECUENCIA**	**IMPACTO**				
		INSIGNIF. (Efectos mínimos)	MENOR (Bajo impacto)	MODERADO (Impacto medio)	MAYOR (Alto impacto)	CATASTRÓF. (Efectos máximos)
RARO	No se ha presentado en los últimos 5 años					
IMPROBABLE	Al menos 1 vez en los últimos 5 años					
POSIBLE	Al menos 1 vez en los últimos 2 años					
PROBABLE	Al menos 1 vez en el último año					
MUY PROBABLE	Más de una vez al año					
	ZONA DE RIESGO: Bajo: asumir riesgo Moderado bajo: Asumir o Reducir riesgo Moderado alto: Reducir el riesgo o Evitar el riesgo Alto: Evitar el riesgo o Transferir el riesgo					

Fuente: Elaboración propia

Los riesgos categorizados como altos, moderados – altos y moderados –bajos requieren acciones o controles a corto o mediano plazo.

Los riesgos categorizados como bajos requieren acciones o controles a mediano o largo plazo.

2.5.5.3.3 Tratamiento del riesgo

Consiste en seleccionar varias opciones para afectar el riesgo. Para ello es importante determinar si existen o no controles y que tan efectivos son para el riesgo que se está valorando.

Los controles pueden ser de dos tipos:

- Preventivos: Se implementar para eliminar las causas de ocurrencia del riesgo.
- Correctivos: Se implementan para modificar las consecuencias de ocurrencia del riesgo.

Para la selección más adecuada del riesgo se debe tener en cuenta:

- Equilibrio en el costo.
- Equilibrio en el esfuerzo de aplicación.

a) Opciones del tratamiento de riesgos

Las siguientes son las opciones posibles para tratar los riesgos, mismas que se reflejaron en la Tabla 9 - Matriz para evaluación de riesgos, y son:

- Asumir el riesgo: Se acepta el riesgo y se elaboran planes de contingencia para manejarlo en caso de ocurrencia.
- Reducir el riesgo: Se trabaja en el riesgo mediante la optimización de procesos y/o implementación de controles, para disminuir la probabilidad (control preventivo) o impacto (control correctivo)
- Evitar el riesgo: Se trabaja en el riesgo mediante cambios trascendentes dentro del proceso tales como mejoras, rediseño, eliminación de dicho proceso.
- Transferir el riesgo: Se trabaja en el riesgo mediante el traspaso total o parcial del mismo a otras instancias fuera de la institución. El riesgo no se elimina, sólo se transforma.

b) Elaboración de planes para el tratamiento de riesgos

El plan de tratamiento de riesgos documenta las opciones de tratamiento elegido e identifica el orden de prioridad otorgado.

El plan debe incluir: razones, responsables, acciones, recursos, métricas, información de control, cronograma.

El plan forma parte constitutiva del modelo y supone un compromiso del equipo de trabajo para la consecución de los objetivos, en la fase de ejecución del mismo.

A continuación se sugiere una tabla que permita definir el plan de tratamiento del riesgo:

Tabla 2-13. Plan de tratamiento y seguimiento de riesgos

PROCESO:						
RIESGO:						
TRATAMIENTO: (Asumir, Reducir, Evitar, Transferir)						
DESCRIPCIÓN PLAN DE TRATAMIENTO:						
INDICADOR DE CUMPLIMIENTO:						
ACTIVIDAD	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**RECURSOS**	**% APORTE AL PLAN**	**%AVANCE**
1.						
2.						
3.						

Fuente: Elaboración propia

2.5.5.3.4 Seguimiento y revisión

Es parte del proceso de gestión del riesgo. Proporciona una medida de rendimiento y comprende: aseguramiento de controles, obtención de información para mejorar la evaluación del riesgo, análisis, detección de cambios de contexto, identificación de riesgos emergentes.

La tabla 9 - Plan de tratamiento y seguimiento de riesgos, contiene el campo “% de avance” que permite hacer el seguimiento del plan ejecutándose en el tiempo. Para que el seguimiento sea efectivo, debe hacerse periódicamente.

En la Universidad este seguimiento tendría que estar a cargo de las áreas estratégicas institucionales en coordinación con la Oficina de Seguridad de Información y Auditoría, así como del responsable de la ejecución del plan.

2.5.5.3. Estructuras organizativas

Las partes interesadas en este catalizador incluyen a agentes internos y externos.

A continuación se definen los roles adaptados a la Universidad en relación a TI y al área financiera:

Tabla 2-14. Roles y estructuras PUCE en relación a TI y al área financiera

ROL/ESTRUCTURA	DEFINICIÓN
Consejo Superior	Grupo de ejecutivos de mayor cargo de la institución
Rector	Ejecutivo de más alto rango en la gerencia de la institución y de la Dirección de Informática
Vicerrector	Ejecutivo de más alto rango en la gerencia de la sedes de la Universidad y de la Oficina de Seguridad de la Información
Consejo Académico	Grupo de ejecutivos que regulan a las Direcciones Generales
Director General Financiero	Ejecutivo de mayor cargo responsable de todos los aspectos de la gestión financiera, incluyendo el riesgo financiero y cuentas confiables y precisas
Director de Informática/Sistemas	Ejecutivo de mayor cargo responsable de alinear TI con las estrategias de la institución. También es responsable de que se planifique, se consigan los recursos necesarios y se gestione la entrega de servicios y soluciones de TI para soportar los objetivos de la Universidad.
Jefe de Seguridad de la Información	Ejecutivo de mayor cargo responsable de todos los aspectos de la seguridad de la información de la institución
Auditoría Interna	Unidad de la institución adscrita al rectorado responsable de proveer auditorías internas.
Comité de supervisión	No existe Su función debería ser de responsabilidad de la dirección de programas y proyectos, incluyendo la gerencia y la supervisión de planes, asignación de recursos, entrega de beneficios y valor y la gestión de los riesgos de programas y proyectos.
Comité de riesgo institucional	No existe Su función debería ser de responsabilidad del consenso y la colaboración requerida a nivel de institución para soportar las actividades y decisiones de la gestión de riesgo.
Miembro de Seguridad de la Información	No existe Su función está atada al de Jefe de seguridad de la información. Su función debería ser una persona que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de la empresa.

Fuente: Elaboración propia

La meta de la estructura organizativa incluye la definición de principios operativos correctamente definidos.

En cuanto al ciclo de vida de la estructura organizativa, su disolución es posible y depende si ésta deja de ser coherente o resulta incompleta con el fin de la institución y sus objetivos estratégicos.

La estructura organizativa completa de la Universidad se encuentra referenciada en el apartado 2.1.1.

Es posible mejorar las estructuras organizativas considerando las modalidades prácticas respecto a la operación de la estructura, la identificación de los miembros, las funciones definidas con claridad a través de niveles de autorización, la normativa acerca de las delegaciones así como procedimiento de escalado en la toma de decisiones.

2.5.5.4. Cultura, ética y comportamiento

Son las conductas de las personas dentro de la institución.

Las partes interesadas son amplias; internamente alcanza a toda la Universidad en tanto que externamente se incluyen a los entes de control gubernamental.

Las metas de este catalizador guardan coherencia con los valores institucionales, la cultura organizacional y los límites de tolerancia que la institución define.

En relación al ciclo de vida, se pueden identificar cambios que sean necesarios y trabajar en esa implementación.

Las buenas prácticas para este catalizador dan cuenta del uso correcto de herramientas de comunicación, concientización, incentivos, reglamentos y normativas que pueden aplicarse para apuntalar los valores institucionales e individuales.

La PUCE se rige por los principios y valores ignacianos reflejados en su modelo educativo; éste es el paraguas sobre el cual se torna la cultura organizacional.

2.5.5.5. Información

Con este catalizador se mide la información relevante de la institución aunque no necesariamente coincide con la información automatizada.

Las partes interesadas pueden ser internas o externas y es recomendable diferenciar entre quienes producen la información, quienes la custodian y quienes son los consumidores de ella.

Las metas de la información se valoran en términos de calidad:

- Precisión, objetividad, credibilidad, reputación.
- Relevancia, completitud, vigencia, interpretabilidad, comprensibilidad.
- Disponibilidad, restricciones de acceso.

En cuanto al ciclo de vida la información debe cumplir las siguientes fases: planificar, diseñar, construir, usar.

2.5.5.6. Servicios, infraestructura y aplicaciones

Se refiere a las herramientas disponibles a través de TI para la institución.

Los servicios pueden ser requeridos por entes internos y externos. De la misma manera estos servicios pueden ser brindados por agentes internos o externos.

En la PUCE los servicios e infraestructura de TI son provistos por la Dirección de Informática; varios de los servicios a su vez tienen un contrato de mantenimiento tercerizado, tal es el caso de sistema financiero ERP BAAN 5.0.

Los servicios que administra TI en la Universidad han sido descritos en el apartado 2.1.4 de este documento.

En cuanto al ciclo de vida, cada uno de los servicios tiene su inicio y fin de acuerdo a las necesidades de la organización y se describen en una arquitectura de base.

Las buenas prácticas de la capacidades de servicio están relacionados con la arquitectura de base en los siguientes términos: reutilización, adquisición, simplicidad, agilidad, apertura.

2.5.5.7. Personas, habilidades y competencias

Este catalizador está relacionado con la capacidad del personal para asumir un rol dentro de los procesos de la institución.

Las partes interesadas son internas externas a través de la identificación de los roles y habilidades apropiados.

Las metas de este catalizador están en relación con la capacitación, habilidades, experiencia y conocimientos del personal con el fin de llevar con éxito las actividades dentro de los procesos asignados.

Como buenas prácticas se tiene la identificación de las necesidades de formación a cubrir, y para ello se establecen los perfiles respectivos.

En la PUCE el levantamiento de habilidades y competencias están relacionadas al cargo y éstos a su vez a funciones específicas.

CAPÍTULO 3
RESULTADOS Y DISCUSIÓN

3.1 ADAPTACIÓN DEL MODELO PROPUESTO EN UN PROCESO CRÍTICO DEL ÁREA FINANCIERA

3.1.1 SELECCIÓN DEL PROCESO CRÍTICO

En vista de que no se dispone de un insumo formal de levantamiento integral de procesos de la Dirección General Financiera y que no es objeto de este trabajo hacerlo, se acudió a la entrevista como herramienta para levantamiento de información. Esta entrevista se hizo de manera aleatoria a siete autoridades institucionales (académicos y administrativos) y tres usuarios operativos del área financiera que mostraron su interés en contribuir con este trabajo.

El resultado de la entrevista realizada arrojó dos procesos financieros críticos:

Tabla 3-1. Identificación de procesos críticos financieros a través de informantes

PROCESO CRÍTICO FINANCIERO	SUSTENTACIÓN
Procesos de matrículas	Es el proceso a través del cual se recauda aproximadamente el 70% de los ingresos de la PUCE y sobre la que se ramifican una serie de procesos financieros que conlleva la distribución presupuestaria real en relación a dichos ingresos
Evaluación presupuestaria	Es el proceso que permite ejecutar la planeación estratégica. Permite evaluar si la ejecución presupuestaria se llevó de acuerdo a lo autorizado y a las necesidades reales en la vida de la Universidad.

Fuente: Elaboración propia

A continuación se describe a detalle los procesos identificados:

- **Proceso de Matrículas.-**

  En términos generales, por cada período académico (semestre), la PUCE hace una evaluación de este proceso con los principales actores involucrados, esto es, Dirección General Financiera con la Dirección de Tesorería, Dirección General de Estudiantes, Dirección General Académica y Auditoría Interna.

  El resultado de esta revisión, cuya documentación está a cargo de la unidad de Auditoria Interna arroja las principales dificultades del proceso en varios aspectos: calidad y oportunidad de información, calendario académico, disponibilidad de los sistemas académico y financiero,

respuesta de los bancos con la recaudación externa, entre los principales aspectos.

En dichos informes se hace referencia leve a la integridad y debilidades de seguridad originadas en el sistema académico básicamente. Es una preocupación de la Directora General Financiera contar con mayor información sobre seguridad de la información de su área, toda vez que indica que desconoce si existen normativas o procedimientos formales que garanticen minimizar las vulnerabilidades del área financiera en lo que se refiere a sus procesos internos en combinación con su herramientas tecnológica, ERP BAAN 5.0.

El proceso de matrículas aparece en la tabla de procesos internos del área financiera documentados en BAAN, del apartado 2.3.5.2.1- Identificación de procesos, documentada como TE6001 - Cobro de matrículas en tesorería.

- **Proceso de evaluación presupuestaria.-**

  Con respecto al segundo proceso crítico, se hizo una entrevista a profundidad con el representante de los profesores ante el Consejo Superior, máximo organismo institucional, especialista en finanzas y conocedor de los procesos esenciales de la Universidad. Indicó que a su juicio, el Consejo Superior no estaría cumpliendo con este proceso toda vez que carece de insumos para hacerlo y la poca información se la recibe demasiado tarde para poder tomar correctivos a tiempo, lo cual no permite a la universidad tomar acciones sobre su administración financiera.

  El proceso de Evaluación Presupuestaria aparece en la tabla de procesos internos del área financiera documentados en BAAN, del apartado 2.3.5.2.1- Identificación de procesos, como el proceso PR4200 – Evaluación Presupuestaria.

Por la relación del proceso con el gobierno de la Universidad para toma de decisiones, se seleccionó el proceso de Evaluación Presupuestaria por parte del Consejo Superior, identificado para aplicar el modelo MGSI-PUCE-DGF propuesto, específicamente en la Meta del Catalizador: procesos y gestión del riesgo que se apoya en la norma ISO/IEC 31000.

3.1.2 PROCESO DE EVALUACIÓN PRESUPUESTARIA

La evaluación presupuestaria puede definirse como el conjunto de procesos de análisis para determinar, periódicamente, los avances financieros obtenidos a un momento dado, y su comparación con el presupuesto inicial y modificado, entendiendo su incidencia en el logro de los objetivos institucionales.

Los objetivos de la evaluación presupuestaria para la Universidad pueden enunciarse así:

- Determinar el grado de eficacia en la ejecución presupuestaria de los ingresos y gastos en relación con los proyectos aprobados.
- Determinar el grado de eficiencia en los proyectos, con relación a la ejecución presupuestaria de los gastos realizados.
- Fundamentar y determinar las causas de las variaciones del presupuesto comparándolas con las estimaciones.
- Realizar un análisis general de la gestión presupuestaria en torno a la información que brinda a las unidades internas y entidades externas.
- Identificar medidas correctivas para mejorar la función presupuestaria.

Las etapas de la Evaluación Presupuestaria a desarrollarse secuencialmente son:

- Etapa 1: Análisis de la gestión presupuestaria en términos de eficacia y eficiencia.
- Etapa 2: Fundamentación de las variaciones del presupuesto.
- Etapa 3: Identificación de las medidas correctivas internas.

El Consejo Superior es la instancia que solicita a la Dirección General Financiera, los informes de ejecución y evaluación presupuestaria y esta a su vez solicita a la Dirección de Presupuestos la preparación del informe solicitado.

Dentro de la Dirección de Presupuestos, se puede visualizar en la siguiente ilustración, la relación con las unidades internas y externas a esta dirección, así como los ciclos de requerimiento y respuesta propios:

Ilustración 3-1. Dir. Presupuestos - Ciclos de requerimiento y respuesta

1	Solicitud Uso Presupuesto
2	Solicitud Compra de Bienes y Servicios
4	Solicitud Distribución de gastos
10	Solicitud disponibilidad de fondos
11	Solicitud de reportes y documentos para conciliacion
14	Solicitud Informes de Saldos y Liquidaciones
15	Solicitud Elaboración Proformas Maestrias y Postgrados
16	Solicitud presupuesto educación continua
17	Solicitud Elaboración Proformas para Proyectos Financ. Externo
19	Solicitud Elaboracion proformas proyectos con financ. PUCE
20	Solicitud notificacion de Postgrados Maestrias y Carreras
22	Solicitud Valor Bonificacion para Becarios
23	Solicitud listado estudiantes en entrenamiento
24	Solicitud Informacion Financiera para Aranceles
29	Solicitud Informacion Subvención Estado
60	Solicitud Información para Control
69	Solicitud Información de ingresos mensuales
70	Solicitud Presupuesto Aprobado para Proyectos Especificos
71	Solicitud Reporte Ingresos Proyectos Autofinanciados y Maestrias
72	Solicitud Informacion Proyectos Autofinanciados y maestrias
73	Proyección de ingresos y Egresos
74	Compra tercerizada útiles de oficina

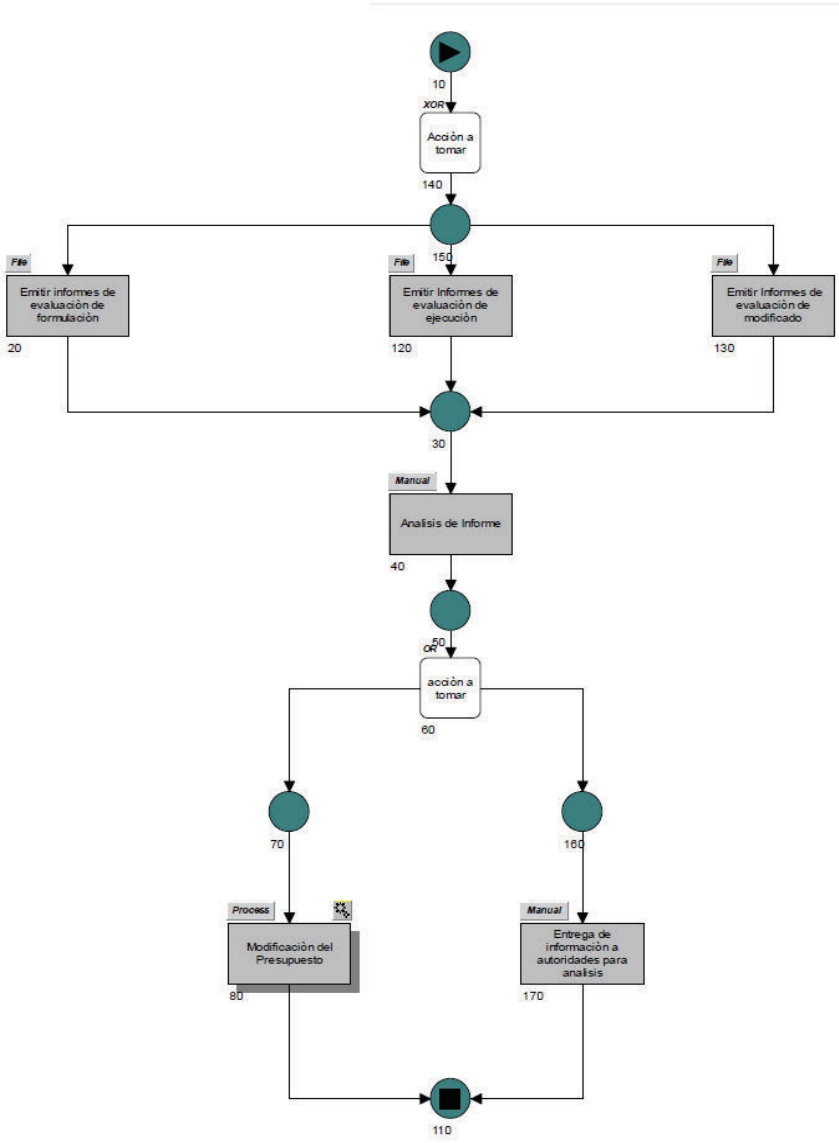
76	Solicitud de suministros y materiales
77	Reutilización de Activos Fijos
78	Solicitud de transferencia de Activos Fijos
79	Solicitud de control fisico de activos
89	Solicitud Elaboraciòn Obligaciòn presupuestaria
90	Solicitud de Ajustes
91	Sollcitud de Documentacion Contable
94	Solicitud entrega activos fijos
99	Solicitud Transferencia de Partidas de Operación
100	Solicitud Especificaciones de Gasto e Inversion
101	Solicitud de desembolso
102	Solicitud cruce información compromisos presupuestarios
103	Solicitud ajuste a desponibilidad de fondos
104	Solicitud Valoracion de Requerimientos
105	Solicitud Valoracion Gastos para proforma presupuestaria
106	Envio proforma presupuestaria para aprobacion
107	Solicitud de Avance Presupuestarios y Proyecciones
108	Solicitud Liquidacion Anual y Evaluacion presupuestaria
109	Solicitud de proformas de postgrados y maestrias para aprob.
110	Solicitud de Proforma Presupuestaria proximo año
111	Solicitud alcance del Cupo de Compra
130	Distribución Consumo de Suministros y Materiales
132	Solicitud Cupos para Compra Tercerizada utiles de oficina

Fuente: DGF - Modelo de Control Financiero. Proy. Hacia el Cambio

Relacionando la ilustración anterior con el proceso seleccionado, Evaluación presupuestaria, es posible observar que aparece en el punto 108 – Solicitud de liquidación anual y evaluación presupuestaria que es solicitado por el gobierno de la PUCE, y que corresponde al Consejo Superior.

El diagrama de flujo que se presenta a continuación fue proporcionado por la Dirección de Presupuestos y responde a la concepción de este proceso desde el punto de vista interno y en relación con el sistema financiero utilizado.

Ilustración 3-2. PR4200 – Proceso de evaluación presupuestaria



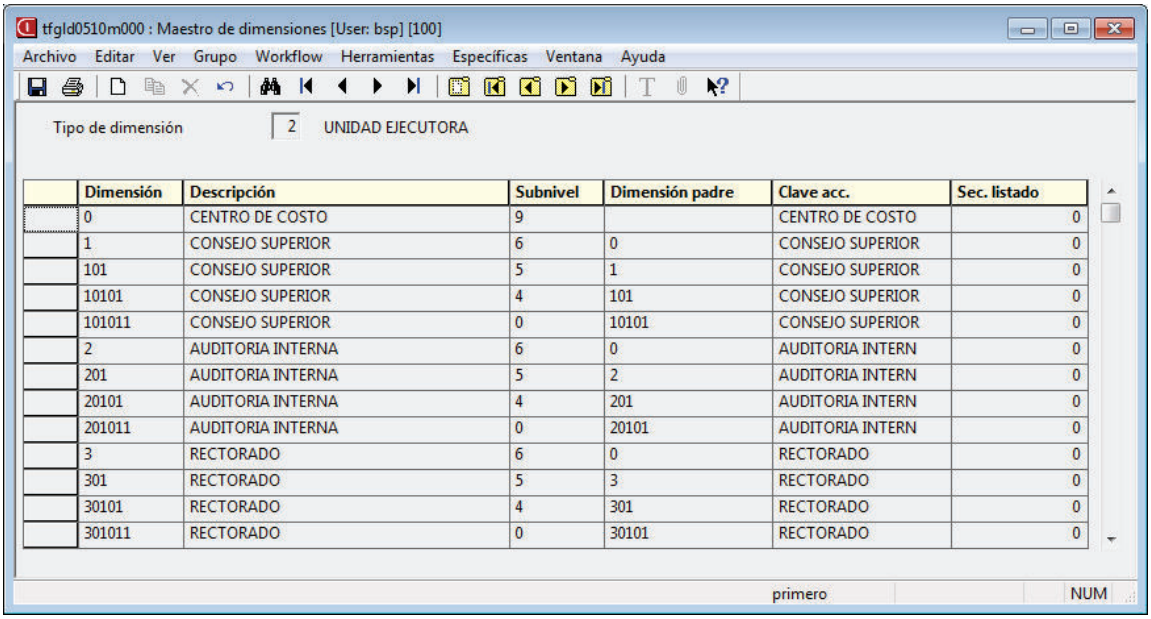
Fuente: PUCE ERP BAAN 5.0 – DEM

Haciendo una revisión del diagrama anterior se puede determinar que en el proceso de evaluación presupuestaria considera como acción inicial emitir un informe que después de ser analizado puede ser modificado a través de afectaciones transaccionales en el sistema o puede ser entregado a las autoridades solicitantes.

El subproceso de modificación presupuestaria parte de una comprensión sobre la definición del concepto de Dimensiones con el que BAAN se maneja.

En el maestro de dimensiones se establece la estructura contable-presupuestaria que permite la clasificación de la información financiera en la Universidad. Estas dimensiones son establecidas por la Dirección General Financiera y su parametrización puede variar de un periodo a otro:

Ilustración 3-3. BAAN – Presupuestos – Maestro de dimensiones

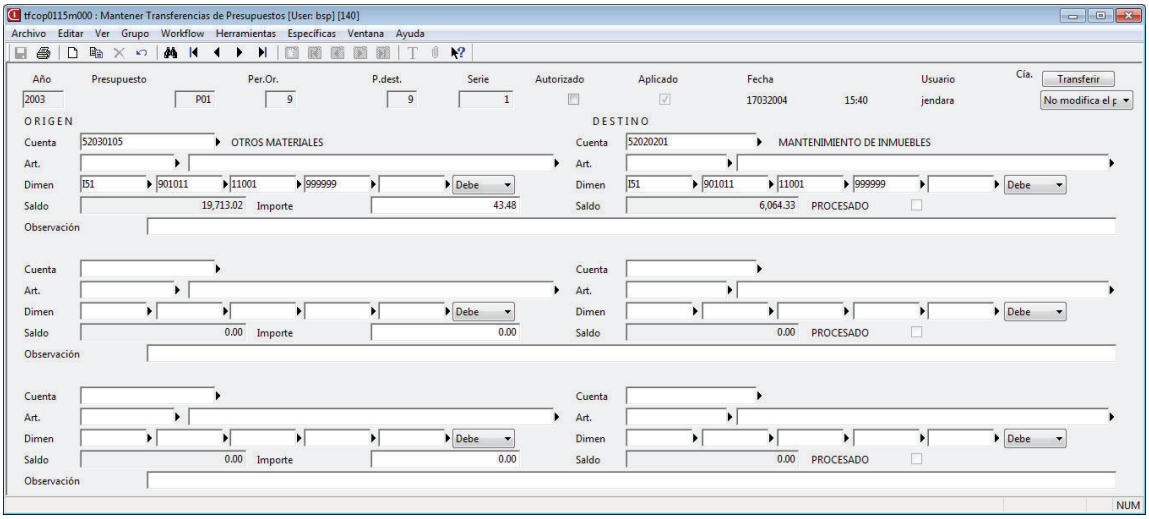


Dimensión	Descripción	Subnivel	Dimensión padre	Clave acc.	Sec. listado
0	CENTRO DE COSTO	9		CENTRO DE COSTO	0
1	CONSEJO SUPERIOR	6	0	CONSEJO SUPERIOR	0
101	CONSEJO SUPERIOR	5	1	CONSEJO SUPERIOR	0
10101	CONSEJO SUPERIOR	4	101	CONSEJO SUPERIOR	0
101011	CONSEJO SUPERIOR	0	10101	CONSEJO SUPERIOR	0
2	AUDITORIA INTERNA	6	0	AUDITORIA INTERN	0
201	AUDITORIA INTERNA	5	2	AUDITORIA INTERN	0
20101	AUDITORIA INTERNA	4	201	AUDITORIA INTERN	0
201011	AUDITORIA INTERNA	0	20101	AUDITORIA INTERN	0
3	RECTORADO	6	0	RECTORADO	0
301	RECTORADO	5	3	RECTORADO	0
30101	RECTORADO	4	301	RECTORADO	0
301011	RECTORADO	0	30101	RECTORADO	0

Fuente: BAAN 5.0 PUCE- Presupuestos

La modificación presupuestaria propiamente, a cada una de las dimensiones presupuestarias se hace a través de transferencias entre partidas mediantes las cuales se compensan las cuentas cuando las unidades ejecutoras hacen uso de su presupuesto. En la siguiente ilustración se puede observar la sesión asociada a esta parte del proceso:

Ilustración 3-4. BAAN – Presupuestos – Mantener transferencia de presupuestos



Fuente: BAAN 5.0 PUCE- Presupuestos

Para poder entender posteriormente el nivel de riesgo del proceso seleccionado, es importante analizar el proceso de madurez de los procesos EDM03-Asegurar la optimización del riesgo y APO13-Definir, operar y supervisar un sistema para la gestión de la seguridad de la información determinados desde la perspectiva de TI, *Anexo 4 y Anexo 5.*

A continuación se presenta una tabla que condensa el nivel de madurez del proceso EDM03-Asegurar la optimización del riesgo [21]:

Tabla 3-2. Nivel de madurez del proceso EDM03 – Asegurar la optimización del riesgo

PROCESO: EDM03 – Asegurar la optimización del riesgo					
PROPÓSITO: Cumplir con los requisitos actuales y futuros de la empresa de tener estables, rentables, integrados y estandarizados los sistemas de aplicación, recursos y capacidades					
N.M	**CRITERIOS DE MADUREZ DEL PROCESO**	**NIVEL DE MEDICIÓN**			
		N	**P**	**L**	**F**
		0% A 15%	**>15 % al 50%**	**>50 % al 85%**	**>85% al 100%**
N1 (70%)	**EDM03-01** – Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con TI son conocidos. **VALORACIÓN:** Los riesgos han sido identificados por la Oficina de Seguridad de Información. La Dirección de Informática conoce varios riesgos a los que se encuentran expuestos.			65%	
	EDM03-02 – La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente. **VALORACIÓN:** Varios riesgos críticos han sido mitigados.			52%	
	EDM03-03- Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado. **VALORACIÓN:** Se ha mantenido un buen control de riesgos aunque se han producido eventualidades inesperadas.				93%
N2 (31%)	**A)** Los objetivos de desempeño del proceso son identificados **B)** El desempeño del proceso está planeado y monitoreado **C)** El desempeño del proceso está ajustado para cumplir los planes. **D)** Los responsables está definidos **E)** Los recursos e información necesaria están identificados, disponibles, asignados y utilizados **F)** Las interfaces entre las partes interesadas son gestionadas una comunicación efectiva y clara asignación de responsabilidades **VALORACIÓN:** La Oficina de Seguridad de Información tiene identificados los objetivos de este proceso y es responsable del mismo conjuntamente con la Dirección de Informática. Hay una debilidad en la comunicación entre las partes. No se cumplen B, C y F.		42%		
	A) Los requerimientos para los productos de trabajo del proceso están definidos. **B)** Los requerimientos de documentación y control de los productos de trabajo están definidos. **C**) Los productos de trabajo están adecuadamente identificados, documentados y controlados. **D)** Los productos de trabajo son revisados de acuerdo a un plan previsto y ajustados si es necesario para cumplir los requerimientos. **VALORACIÓN:** La Oficina de Seguridad de Información ha elaborado cierta documentación necesaria para el desenvolvimiento adecuado de este proceso. No se cumplen A,C y D		20%		
NIVEL DE MADUREZ: 1					

Fuente: Elaboración propia

Tabla 3-3. Nivel de madurez del proceso APO13 – Definir, operar y supervisar un sistema para la gestión de seguridad de información.

PROCESO: APO03 – Gestionar la seguridad					
PROPÓSITO: Cumplir con los requisitos de la empresa de asegurar el alineamiento de los servicios de TI clave con las necesidades el negocio.					
N.M	**CRITERIOS DE MADUREZ DEL PROCESO**	**NIVEL DE MEDICIÓN**			
		N	**P**	**L**	**F**
		0% A 15%	**>15 % al 50%**	**>50 % al 85%**	**>85% al 100%**
N1 (92%)	**APO13-01** – Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa. **VALORACIÓN:** Se definió la Oficina de Seguridad de Información que es responsable de gestionar la seguridad de TI conjuntamente con la Dirección de Informática.				90%
	APO13-02 – Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad. **VALORACIÓN:** Existe un plan difundido en toda la institución.				93%
	APO13-03 – Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en todoa la empresa **VALORACIÓN:** Se ha implementado la soluciones de seguridad de la información de manera consistente.				92%
N2 (17%)	**2.1 GESTIÓN DEL DESEMPEÑO** **A)** Los objetivos de desempeño del proceso son identificados **B)** El desempeño del proceso está planeado y monitoreado **C)** El desempeño del proceso está ajustado para cumplir los planes. **D)** Los responsables está definidos **E)** Los recursos e información necesaria están identificados, disponibles, asignados y utilizados **F)** Las interfaces entre las partes interesadas son gestionadas una comunicación efectiva y clara asignación de responsabilidades **VALORACIÓN:** El desarrollo del proceso se encuentra en fase preliminar. No se cumplen A, B y C.		33%		
	2.2 GESTIÓN DEL PRODUCTO DEL TRABAJO **A)** Los requerimientos para los productos de trabajo del proceso están definidos. **B)** Los requerimientos de documentación y control de los productos de trabajo están definidos. **C**) Los productos de trabajo están adecuadamente identificados, documentados y controlados. **D)** Los productos de trabajo son revisados de acuerdo a un plan previsto y ajustados si es necesario para cumplir los requerimientos. **VALORACIÓN:** La Oficina de Seguridad de Información ha elaborado cierta documentación necesaria para el desenvolvimiento adecuado de este proceso. No se cumplen A, B, C y D	0%			
NIVEL DE MADUREZ: 1					

Fuente: Elaboración propia

La tabla anterior condensa el nivel de madurez del proceso APO13-Definir, operar y supervisar un sistema para la gestión de la seguridad de la información [21]:

De la investigación anterior que se condensó en las dos tablas anteriores, se desprende que los procesos de TI: EDM03-Asegurar la optimización del riesgo y APO13-Definir, operar y supervisar un sistema para la gestión de la seguridad de la información alcanza en parcialmente su madurez en el nivel 1; esto quiere decir que dichos procesos se encuentran en ejecución.

3.1.3 EVALUACIÓN DEL RIESGO

En términos generales, el proceso de evaluación presupuestaria se basa en el procesamiento de grandes volúmenes de información por cada una de las unidades administrativas y docentes de la Universidad y está a cargo de la Dirección de Presupuestos. Para la consecución de este objetivo, se toma como insumos iniciales:

- El presupuesto aprobado por el Consejo Superior para el año fiscal.
- Los proyectos, partidas y subpartidas formulados por cada una de las unidades administrativas y académicas.
- Los proyectos, partidas y subpartidas modificados por cada una de las unidades administrativas y académicas.
- Los proyectos, partidas y subpartidas ejecutados por cada una de las unidades administrativas y académicas.

La información proviene del sistema ERP BAAN 5.0 implementado, de hojas electrónicas de apoyo y de documentación de respaldo y es procesada en hojas electrónicas complejas y extensas que permiten hacer agrupaciones y filtros de información que no son posibles de hacer en dicho sistema.

Cuando la información ha sido condensada por los analistas de presupuestos a cargo, la directora de presupuestos analiza el informe y lo sustenta con notas explicativas.

Este informe es revisado por la directora general financiera y envía el informe al Consejo Superior.

La frecuencia de pedidos de evaluación presupuestaria por parte del Consejo Superior es anual como parte del cierre del periodo.

3.1.3.1 Identificación de riesgos

Tomando como referencia el contexto de la Universidad. Se identifican a través de la entrevista, los siguientes factores que han incidido en la consecución del proceso de evaluación presupuestaria:

Tabla 3-4. Preguntas orientadoras para identificar riesgos en el proceso crítico seleccionado

PROCESO:	**Evaluación presupuestaria**
PREGUNTAS ORIENTADORAS	**IDENTIFICACIÓN DE EVENTOS DE RIESGO**
¿Qué puede suceder?	• Falta de acciones preventivas y correctivas en la ejecución presupuestaria • Riesgo financiero institucional • Pérdida de información para toma de decisiones • Divulgación de información confidencial
¿Cuáles son las fuentes de riesgos?	• Personal involucrado en el procesamiento de información • Autoridades institucionales • Vulnerabilidad de información • Vulnerabilidad en los sistemas de información • Frecuencia baja de evaluaciones del presupuesto institucional
¿Cuáles son las áreas de impacto?	• Recursos institucionales • Planes operativos institucionales • Planes de mejora institucionales
¿Cómo o por qué puede suceder?	• Automatización limitada para obtener información de análisis • Errores en el procesamiento de información • Falta de controles en la ejecución presupuestaria • Existencia mínima de pautas metodológicas para evaluación presupuestaria • Documentación incompleta del proceso • Exceso de permisos abiertos para modificar el presupuesto • Permisos con relación mínima en relación con las funciones y cargos del personal

Fuente: Elaboración propia

3.1.3.2 Análisis de riesgos

A continuación se hace un análisis de los riesgos identificados en el proceso de evaluación presupuestaria, sus principales causas y consecuencias a través de información identificada previamente.

Tabla 3-5. Análisis del riesgo financiero institucional

PROCESO:	**Evaluación presupuestaria**
RIESGO:	**Riesgo financiero institucional**
TIPO DE RIESGO:	**Financiero**
CAUSA	**EFECTO**
Recurso financieros incorrectamente asignados	Pérdidas económicas

Fuente: Elaboración propia

De la tabla anterior se desprende que una incorrecta asignación de recursos eleva el riesgo financiero de la institución y pueden ocasionarse pérdidas económicas por ese motivo.

Tabla 3-6. Análisis del riesgo de toma de acciones preventivas y correctivas

PROCESO:	**Evaluación presupuestaria**
RIESGO:	**Falta de acciones preventivas y correctivas en la ejecución presupuestaria**
TIPO DE RIESGO:	**Cumplimiento**
CAUSA	**EFECTO**
• Procedimientos no adecuados para extraer información financiera para toma de decisiones. • Falta de calidad de información financiera	• No cumplimiento de los objetivos institucionales anuales identificados a través de POAs y PEDIs. • Ejecución presupuestaria deficiente. • Evaluación presupuestaria tardía o incompleta

Fuente: Elaboración propia

De la tabla anterior se desprende que la falta de procedimientos adecuados para extraer información de calidad, eleva el riesgo de no poder ejecutar acciones preventivas y correctivas presupuestarias en la institución y puede ocasionarse principalmente el incumplimiento de los objetivos institucionales.

Tabla 3-7. Análisis del riesgo de acceso no controlado a la información confidencial

PROCESO:	**Evaluación presupuestaria**
RIESGO:	**Acceso no controlado a la información confidencial**
TIPO DE RIESGO:	**Tecnológico**
CAUSA	**EFECTO**
• Exceso de permisos de acceso al sistema ERP BAAN 5.0 a los analistas de presupuestos. • Respaldo de archivos de análisis en repositorios comunes de información en computadores compartidos y espacios de servidor.	• Vulnerabilidad de acceso a la información presupuestaria por instancias no autorizadas • Divulgación de información no autorizada a personal interno y externo de la institución.

Fuente: Elaboración propia

De la tabla anterior se desprende que la falta de control de los permisos de acceso a la información financiera en sistemas y archivos, eleva el riesgo de acceso no controlado a la información confidencial financiera y puede ocasionarse principalmente divulgación no autorizada de información sensible.

Tabla 3-8. Análisis del riesgo de pérdida de información para toma de decisiones

PROCESO:	**Evaluación presupuestaria**
RIESGO:	**Pérdida de información para toma de decisiones**
TIPO DE RIESGO:	**Operativo – tecnológico.**

CAUSA	**EFECTO**
• Registros incompletos dentro del sistema. • Errores en la interpretación de las instrucciones de modificación y ejecución presupuestaria	• Calidad de información deficiente. • Falta de coherencia entre los registros presupuestarios y contables.

Fuente: Elaboración propia

De la tabla anterior se desprende que la falta de control y coherencia en el registro de datos dentro de los sistemas, eleva el riesgo de perder información para toma de decisiones y puede ocasionar principalmente que la calidad de información sea deficiente e incoherente con respecto a las transacciones contables.

3.1.3.3 Evaluación de riesgos

A continuación se evalúan los riesgos identificados en la sección 3.1.3.2 – Análisis de riesgos, con la finalidad de valorar los mismos en términos de probabilidad y de impacto, para poder determinar posteriormente su tratamiento.

Tabla 3-9. Matriz para evaluación del riesgo financiero institucional

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Riesgo financiero institucional**					
TIPO DE RIESGO:	**Financiero**					
PROBABILIDAD	**FRECUENCIA**	**IMPACTO**				
		INSIGNIF. (Efectos mínimos)	MENOR (Bajo impacto)	MODERADO (Impacto medio)	MAYOR (Alto impacto)	CATASTRÓF. (Efectos máximos)
RARO	No se ha presentado en los últimos 5 años					
IMPROBABLE	Al menos 1 vez en los últimos 5 años					**X**
POSIBLE	Al menos 1 vez en los últimos 2 años					
PROBABLE	Al menos 1 vez en el último año					
MUY PROBABLE	Más de una vez al año					

Fuente: Elaboración propia

De la tabla anterior se desprende que es improbable que el riesgo financiero institucional ocurra, y que cuando llega a ocurrir es catastrófico para la universidad.

Tabla 3-10. Matriz para evaluación del riesgo de toma de acciones preventivas y correctivas

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Falta de acciones preventivas y correctivas en la ejecución presupuestaria**					
TIPO DE RIESGO:	**Cumplimiento**					
PROBABILIDAD	**FRECUENCIA**	**IMPACTO**				
		INSIGNIF. (Efectos mínimos)	MENOR (Bajo impacto)	MODERADO (Impacto medio)	MAYOR (Alto impacto)	CATASTRÓF. (Efectos máximos)
RARO	No se ha presentado en los últimos 5 años					
IMPROBABLE	Al menos 1 vez en los últimos 5 años					
POSIBLE	Al menos 1 vez en los últimos 2 años					
PROBABLE	Al menos 1 vez en el último año					
MUY PROBABLE	Más de una vez al año					**X**

Fuente: Elaboración propia

De la tabla anterior se desprende que es muy probable que la falta de acciones preventivas y correctivas en la ejecución presupuestaria ocurra, y que cuando llega a ocurrir es catastrófico para la universidad.

Tabla 3-11. Matriz para evaluación del riesgo de acceso no controlado a la información confidencial

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Acceso no controlado a la información confidencial**					
TIPO DE RIESGO:	**Tecnológico**					
PROBABILIDAD	**FRECUENCIA**	**IMPACTO**				
		INSIGNIF. (Efectos mínimos)	MENOR (Bajo impacto)	MODERADO (Impacto medio)	MAYOR (Alto impacto)	CATASTRÓF. (Efectos máximos)
RARO	No se ha presentado en los últimos 5 años					
IMPROBABLE	Al menos 1 vez en los últimos 5 años					
POSIBLE	Al menos 1 vez en los últimos 2 años					
PROBABLE	Al menos 1 vez en el último año				**X**	
MUY PROBABLE	Más de una vez al año					

Fuente: Elaboración propia

De la tabla anterior se desprende que es probable que el acceso no controlado a la información confidencial ocurra, y que cuando llega a ocurrir su impacto es mayor para la universidad.

Tabla 3-12. Matriz para evaluación del riesgo de pérdida de información para

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Pérdida de información para toma de decisiones**					
TIPO DE RIESGO:	**Operativo – tecnológico.**					
PROBABILIDAD	**FRECUENCIA**	**IMPACTO**				
		INSIGNIF. (Efectos mínimos)	MENOR (Bajo impacto)	MODERADO (Impacto medio)	MAYOR (Alto impacto)	CATASTRÓF. (Efectos máximos)
RARO	No se ha presentado en los últimos 5 años					
IMPROBABLE	Al menos 1 vez en los últimos 5 años					
POSIBLE	Al menos 1 vez en los últimos 2 años					
PROBABLE	Al menos 1 vez en el último año				**X**	
MUY PROBABLE	Más de una vez al año					

Fuente: Elaboración propia

De la tabla anterior se desprende que es probable que la pérdida de información para la toma de decisiones ocurra, y que cuando llega a ocurrir su impacto es mayor para la universidad.

De acuerdo a la Matriz de cumplimiento de Objetivos de los procesos AP013 - Gestión de la Seguridad y EDM03 – Asegurar la optimización del riesgo [21] cuyo detalle se encuentra en el *Anexo 3*, se hacen las siguientes reflexiones:

- Apenas el 10% de los proyectos de la institución consideran el riesgo de TI.
- El nivel de alineamiento entre el riesgo de TI y el riesgo de negocio es del 70%.
- La frecuencia de refresco de la evaluación de factores de riesgo se hace anualmente, por ello se considera que esta métrica se ha cumplido en un 50%.
- Los incidentes de seguridad son varios pero se han mitigado el 80% de ellos.
- El 85% de los servicios de TI están alineados conforme al plan de seguridad.

De este análisis se desprende que la institución como tal está lejos de comprender la importancia de considerar el riesgo en sus operaciones, y que TI tiene una idea más cercana de su importancia sin embargo aún le falta trabajar al respecto.

3.1.4 TRATAMIENTO, SEGUIMIENTO Y REVISIÓN DEL RIESGO

A continuación se define el plan de tratamiento del riesgo del proceso de evaluación presupuestaria:

Tabla 3-13. Plan de tratamiento y seguimiento del riesgo financiero institucional del proceso de evaluación presupuestaria

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Tipo financiero - Riesgo financiero institucional**					
TRATAMIENTO:	Reducir el riesgo					
DESCRIPCIÓN PLAN DE TRATAMIENTO:	Mejorar la asignación de recursos financieros a los programas, planes y proyectos que se identifiquen como prioritarios para el cumplimiento de los objetivos institucionales.					
INDICADOR DE CUMPLIMIENTO:	% de proyectos prioritarios culminados					
ACTIVIDAD	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**RECURSOS**	**% APORTE AL PLAN**	**%AVANCE**
1.Identificarlos POAs institucionales anuales prioritarios	Dirección General Académica Dirección General Administrativa Dirección General de Estudiantes Dirección General Financiera Dirección de Informática				20%	
2.Establecer la prioridad de los POAs anuales en función de los objetivos estratégicos de la PUCE	Consejo Superior				10%	
3.Asignar presupuesto para la ejecución de los POAs identificados	Consejo Superior				10%	
4.Evaluar periódicamente la ejecución de los POAs en función de la asignación presupuestaria	Consejo Superior				40%	
5. Redefinir los POAs prioritarios en base a la evaluación	Consejo Superior				20%	
					100%	

Fuente: Elaboración propia

De la tabla anterior se desprende que la actividad más relevante para reducir el riesgo financiero es evaluar periódicamente la ejecución de los POAs en función de la asignación presupuestaria por parte del Consejo Superior.

Tabla 3-14. Plan de tratamiento y seguimiento del riesgo de toma de acciones preventivas y correctivas del proceso de evaluación presupuestaria

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Tipo cumplimiento - Falta de acciones preventivas y correctivas en la ejecución presupuestaria**					
TRATAMIENTO:	Evitar el riesgo					
DESCRIPCIÓN PLAN DE TRATAMIENTO:	Mejorar la periodicidad y calidad de información entregada al Consejo Superior para la toma de decisiones y la consecución de los objetivos institucionales.					
INDICADOR DE CUMPLIMIENTO:	% de acciones preventivas y correctivas en la ejecución presupuestaria como resultado de la evaluación presupuestaria					
ACTIVIDAD	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**RECURSOS**	**% APORTE AL PLAN**	**%AVANCE**
1. Evaluar periódicamente la ejecución presupuestaria en base a la información operativa	Dirección de Presupuestos				10%	
2. Proponer acciones preventivas y correctivas en base a la evaluación	Dirección General Financiera				30%	
2. Enviar el resultado del análisis al Consejo superior para toma de decisiones	Dirección General Financiera				5%	
3. Evaluar periódicamente la ejecución de los POAs en función de la asignación presupuestaria	Consejo Superior				25%	
4. Autorizar acciones preventivas y correctivas en base a la evaluación realizada por el Consejo Superior	Consejo Superior				10%	
5. Ejecutar las acciones preventivas y correctivas aprobadas	Dirección General Académica Dirección General Administrativa Dirección General de Estudiantes Dirección General Financiera Dirección de Informática				20%	
					100%	

Fuente: Elaboración propia

De la tabla anterior se desprende que la actividad más relevante para evitar el riesgo de la falta de acciones preventivas y correctivas en la ejecución presupuestaria es proponer acciones preventivas y correctivas en base a la evaluación por parte de la Dirección General Financiera.

Tabla 3-15. Plan de tratamiento y seguimiento del riesgo de acceso no controlado a la información confidencial del proceso de evaluación presupuestaria

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Tipo tecnológico - Acceso no controlado a la información confidencial**					
TRATAMIENTO:	Evitar el riesgo					
DESCRIPCIÓN PLAN DE TRATAMIENTO:	Mejorar el control de acceso a la información presupuestaria de acuerdo al organigrama institucional y funciones del personal del área financiera y de gobierno.					
INDICADOR DE CUMPLIMIENTO:	% roles y permisos levantados con respecto a los cargos y funciones del personal administrativo y autoridades de gobierno.					
ACTIVIDAD	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**RECURSOS**	**% APORTE AL PLAN**	**%AVANCE**
1. Identificar y documentar los procesos institucionales	Dirección General Administrativa Oficina de Seguridad de Información				20%	
2.Identificar funciones y cargos para ejecutar los procesos	Dirección General Administrativa Dirección de Recursos Humanos Oficina de Seguridad de Información				5%	
3.Implementar restructuración en procesos y categorización de cargos	Dirección General Administrativa				10%	
4. Identificar los activos de información por cada sistema o repositorio institucional	Oficina de Seguridad de Información Dirección de Informática				25%	
5. Identificar permisos y roles por cada activo de información	Oficina de Seguridad de Información Dirección de Informática				10%	
6. Implementar el esquema de seguridad de información	Oficina de Seguridad de Información Dirección de Informática				30%	

Fuente: Elaboración propia

De la tabla anterior se desprende que la actividad más relevante para evitar el riesgo de acceso no controlado a la información confidencial es implementar el esquema de seguridad de información por parte de la Oficina de Seguridad de Información y la Dirección de Informática.

Tabla 3-16. Plan de tratamiento y seguimiento del riesgo de pérdida de información para toma de decisiones del proceso de evaluación presupuestaria

PROCESO:	**Evaluación presupuestaria**					
RIESGO:	**Tipo operativo – tecnológico - Pérdida de información para toma de decisiones**					
TRATAMIENTO:	Evitar el riesgo					
DESCRIPCIÓN PLAN DE TRATAMIENTO:	Mejorar la calidad del registro de datos en el sistema financiero, eliminando herramientas alternas de registro.					
INDICADOR DE CUMPLIMIENTO:	% de datos automatizados dentro del sistema financiero.					
ACTIVIDAD	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**	**RECURSOS**	**% APORTE AL PLAN**	**%AVANCE**
1. Identificar los activos de información por cada sistema o repositorio del área financiera y de unidades relacionadas	Oficina de Seguridad de Información Dirección de Informática Dirección General Financiera				10%	
2.Identificar la vulnerabilidad de los sistemas y repositorios de información	Oficina de Seguridad de Información Dirección de Informática Dirección General Financiera				20%	
3. Integrar la información vulnerable dentro del sistema financiero minimizando la interacción manual	Dirección de Informática				30%	
4. Mejorar los controles y calidad de registro de información y de acceso a la información de los sistemas	Oficina de Seguridad de Información Dirección de Informática Dirección General Financiera				40%	
					100%	

Fuente: Elaboración propia

De la tabla anterior se desprende que la actividad más relevante para evitar el riesgo de pérdida de información para toma de decisiones es mejorar los controles y calidad de registro de información y de acceso a la información de los sistemas por parte de la Oficina de Seguridad de Información, la Dirección de Informática y la Dirección General Financiera.

Dos de los riesgos identificados en el proceso de evaluación financiera, están relacionados con TI y son de riesgo alto. Estos son:

- Acceso no controlado a la información confidencial.
- Pérdida de información para toma de decisiones.

A continuación se presenta una matriz de relación entre los riesgos de tipo tecnológico del proceso de evaluación presupuestaria versus los procesos de TI relacionados con la gestión financiera seleccionados para este modelo:

Tabla 3-17. Relación proceso críticos financiero versus procesos de TI relacionados

<table>
<tr><td colspan="2"></td><td colspan="2">PROCESOS DE TI RELACIONADOS CON LA GESTIÓN FINANCIERA</td></tr>
<tr><td colspan="2">PROCESO CRÍTICO DEL ÁREA FINANCIERA</td><td>AP013 - Gestión de la Seguridad</td><td>EDM03 – Asegurar la optimización del riesgo</td></tr>
<tr><td colspan="2">Evaluación presupuestaria</td><td colspan="2">Alcanza totalmente el Nivel 1 de riesgo</td></tr>
<tr><td>Acceso no controlado a la información confidencial</td><td rowspan="2">Alcanza parcialmente el Nivel 1 de riesgo</td><td colspan="2" rowspan="2">Oficina de Seguridad de la Información
Dirección de Informática
Dirección General Financiera</td></tr>
<tr><td>Pérdida de información para toma de decisiones</td></tr>
</table>

Fuente: Elaboración propia

De la tabla anterior se puede deducir el proceso de evaluación presupuestaria tiene relación con los procesos de TI identificados en relación con el área financiera [21] Sin embargo, el nivel de riesgo de dichos procesos de TI evaluados en el trabajo referenciado son optimistas con respecto a los resultados de este trabajo. Para que la Dirección de Informática alcance totalmente el nivel 1 de riesgo, los procesos de gobierno relacionado tendrían que alcanzar en su gran mayoría este nivel. Con la información analizada no es posible determinar si esa es la tendencia.

Para tratar los riesgos identificados y mejorar la coherencia en la valoración de riesgos, se proponen adicionalmente las siguientes acciones de mejora:

- Capacitar a los directivos de la institución para entender la importancia de considerar los riesgos de TI en los proyectos de la institución.
- Involucrar a TI en la gestión estratégica de la institución con el fin de maximizar el nivel de alineamiento entre el riesgo de TI y el riesgo de negocio.
- Generar políticas e implantar un rol específico que periódicamente tenga a cargo evaluar los factores de riesgo.
- Atender la totalidad de los incidentes de seguridad registrados.
- Minimizar los controles en las áreas afectadas, ejecutando acciones preventivas.
- Alinear los servicios de TI conforme al plan de seguridad, a través de un trabajo conjunto entre la Oficina de Seguridad de Información y la Dirección de Informática.

3.2 DETERMINACIÓN DEL APORTE DEL MODELO

Este modelo propuesto es una adaptación de COBIT 5 e ISO 31000 enfocado al área financiera de la PUCE. Se han dado lineamientos amplios de tal manera que pueda abordar cualquier proceso identificado en contraste con los procesos de gestión de TI.

El Modelo de Gestión de Seguridad de Información, MGSI-PUCE-DGF, está organizado a través de fases que respetan la terminología de metas de COBIT 5.0.

Se convierte en un aporte útil para la Universidad primeramente, porque no existe vigente ningún modelo de seguridad de información en marcha, lo que facilitaría una implementación o aplicación de las políticas de seguridad de información existentes en los términos indicados en la sección 2.1.3 - Gestión de la Seguridad de la Información, y luego, para la Dirección General Financiera, en varias aristas:

- Concientizar en la importancia de asegurar la información financiera en términos de confidencialidad, integridad y disponibilidad. La relación entre los objetivos institucionales y las gestiones de las unidades de informática de las empresas deben estar vinculadas. Una de las funciones del área de TI es responder a la razón misma de la institución mediante un conjunto de herramientas y estrategias que permitan minimizar o anular los factores que pudieran afectar su normal funcionamiento.
- Forzar la identificación y documentación de los procesos internos del área financiera, toda vez que para este trabajo ese insumo resultó faltante y por lo cual se tuvo que partir de información de base poco documentada. No conocer a ciencia cierta los procesos internos de la institución hace muy difícil lograr resultados con eficacia y eficiencia. La determinación de cuellos de botella, falta de controles o fallo en operaciones se tornan complejas de entender y por tanto de abordar.
- Medir los riesgos a los que está expuesto el resultado de los procesos del área financiera y que afectan significativamente a los logros institucionales. Minimizando el riesgo y mejorando los niveles de seguridad dentro del área financiera de la PUCE en trabajo coordinado con la Dirección de Informática y Oficina de Seguridad de Información, es posible hablar en términos de seguridad de la información.

3.3 PROPUESTA DE ESTRATEGIAS DE IMPLEMENTACIÓN DEL MODELO

Para la implementación del modelo propuesto, se requiere en primera instancia, un cambio institucional que permita básicamente:

- Entender la razón de ser de la institución.
- Identificar las fortalezas y debilidades institucionales en función de sus objetivos.
- Concientizar acerca de la importancia de la seguridad de la información.

Con una base institucional fortalecida, comprometida y consciente de su situación actual al respecto de seguridad de información, y en función de los objetivos de calidad planteados, sería posible implementar el modelo para lo cual se sugiere la siguiente estrategia en forma de fases a manera de ciclo de vida:

Ilustración 3-5. Estrategia de implementación de MGSI-PUCE-DGF

Fuente: Elaboración propia

En la ilustración anterior se puede observar que se han contemplado 5 fases, y que ellas tienden a ser cíclicas, tomando como primicia los principios de calidad que conllevan una revisión permanente de cualquier institución.

Antes de pensar en la implementación de un modelo es necesario definir los objetivos y los resultados esperados y para ello es importante el compromiso y comprensión de las autoridades institucionales, así como contar con un paraguas de levantamiento de información del políticas y procesos para poder llegar a nivel de detalle en la misma institución.

Dado que en la PUCE el levantamiento de procesos a nivel de detalle aún no es un insumo con el que se pueda contar, y que de una u otra manera, existen políticas sobre las cuales opera la Universidad, esta propuesta hace énfasis en el

levantamiento de procesos, dejando la identificación de políticas como parte del modelo MGSI-PUCE-DGF.

A continuación se explica a detalle cada una de estas fases propuestas:

Fase 1: Conocimiento institucional

- Compromiso de la alta dirección
- Expectativas de los miembros de la comunidad
- Realización del Diagnóstico inicial
    - Identificación de las Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) de la institución

Fase 2: Levantamiento de procesos institucionales

En esta fase se propone hacer un levantamiento y optimización integral de procesos que sirva como punto de partida. Si la optimización no fuera posible, al menos se requiere un levantamiento de los procesos internos para lo cual se pueden distinguir tres dimensiones como los sugiere la metodología corporativa, Gestión de Procesos de Negocio (BPM) y que se alinea de manera natural con COBIT 5.0:

- Dimensión de Negocio.
- Dimensión de Proceso.
- Dimensión de Gestión.-
    - Diseño y construcción de procesos
    - Simulación de procesos
    - Ejecución de procesos modelizados
    - Monitorización de procesos
    - Optimización de procesos

Fase 3: Implementación del modelo MGSI-PUCE-DGF en el área financiera

En esta fase se espera la intervención directa de la Oficina de Seguridad de la Información como líder de implementación y unidad ejecutora, Auditoría Interna validando la consecución de cada meta, la Dirección General Financiera como unidad responsable de proporcionar información e implementar el modelo, y la Dirección de Informática como unidad estratégica de apoyo a los objetivos de la Dirección Financiera y como unidad proveedora de información.

- Meta 1: Motivo de las partes interesadas
- Meta 2: Necesidades de las partes interesadas
- Meta 3: Metas institucionales para los procesos financieros
- Meta 4: Metas relacionadas con TI

- Meta 5: Meta de los catalizadores

Fase 4: Evaluación de los resultados

Ejecución de auditorías periódicas

Fase 5: Optimización de los hallazgos

Ejecución de las recomendaciones de auditoria

CAPÍTULO 4
CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Los objetivos específicos planteados para la consecución de este trabajo se han cumplido. A continuación se detallan las conclusiones que se pueden generar a partir de la realización de dicho trabajo:

- La determinación de los procesos críticos en la Dirección General Financiera de la PUCE, se llevó a cabo en la sección 2.2–Determinación de los procesos críticos. La falta de un levantamiento formal de procesos y procedimientos ha demorado la realización de este trabajo y se ha debido utilizar otras técnicas complementarias de levantamiento de información para poder establecer una base. Los hallazgos más relevantes en el pilotaje están relacionados con la falta de políticas y de documentación de procesos internos.
- La identificación de las vulnerabilidades internas y externas se indican en el apartado 2.3– Identificación de riesgos, las mismas que sirvieron de antesala para determinar los riesgos más importantes para el área financiera en función de los recursos de TI. Se hizo un contraste entre las vulnerabilidades y riesgos en torno al rol de a Oficina de Seguridad de Información y las funciones asociadas a ellos que se encuentran en fase de planeación.
- Se ha desarrollado el modelo de gestión de seguridad de información, MGSI-PUCE-DGF adaptando COBIT 5.0 y acoplando ISO 31000 en el tratamiento de procesos e identificación del riesgo en el área de Dirección General Financiera en relación con los procesos del área de TI de la PUCE. El modelo propuesto tiene por finalidad proporcionar un instrumento de base que permita orientar a la Dirección General Financiera, a la Oficina de Seguridad de la Información y a la Dirección de Informática, mejorar la seguridad de la información en los procesos críticos financieros. Este desarrollo se evidencia en el apartado 2.5 – Desarrollo de propuesta del modelo de gestión de seguridad de la información MGSI-PUCE-DGF.
- De acuerdo al levantamiento de información realizado y documentado se pudo determinar que actualmente en la PUCE no existe implementado un modelo de seguridad de información financiera; la cultura organizacional, los sistemas, las políticas aprobadas aún están lejos de llegar a llegar a este nivel de detalle, y por ello se han determinado estrategias de implementación del modelo propuesto en la PUCE, a través del desarrollo de 5 fases, tomando como base el aporte que el modelo brinda (apartado

3.2- Determinación del aporte del modelo) y aterrizando el análisis realizado en la medida que se ha desarrollado el trabajo y que ha sido condensado en el apartado 3.3 – Propuesta de estrategias de implementación del modelo.

4.2 RECOMENDACIONES

A continuación se presentan algunas recomendaciones pertinentes de implementarse en la universidad a partir del desarrollo de este trabajo:

- La Oficina de Seguridad de Información ha desarrollado la *Política Detallada y Normas de Seguridad Lógica de la Información procesada con Sistemas Informáticos*, la misma que aún no entra en vigencia. Para efectos de este trabajo, hubiera resultado conveniente su implementación toda vez que la misma se enfoca en normar la recolección, transmisión, almacenamiento, proceso y distribución de información por medio de sistemas informáticos institucionales, con el objetivo de proteger la información y evitar suspensión e servicios, mal uso de la información y alteraciones.
- Para que el modelo pueda ser implementado, es imprescindible contar con los insumos realizados de manera completa.
- Es necesario que la PUCE implemente un modelo de gestión de seguridad de información institucional como parte de la planificación estratégica a través de un objetivo estratégico puntual, que permita a su vez la generación de varios proyectos alineados, entre los cuales debe constar un POA dentro del área de TI en coordinación con el área financiera para mejorar los procesos críticos en función de la seguridad de información; para ello es necesario la concientización y compromiso de la alta gerencia, así como un POA que permita analizar y revisar funciones y roles del gobierno corporativo con el fin de elevar la gestión de TI de apoyo a estratégicas.
- La gestión financiera debe estar sustentada en sistemas sólidos y eficaces de información y de gestión que hagan posible que los procesos se lleven con calidad al servicio de la educación. Un Sistema de Gestión de Calidad (SGC) implementado pondría orden en la manera como la universidad dirige y controla las actividades relacionadas con la vida institucional en relación con la calidad requerida. La incorporación del modelo de gestión de seguridad de información permitiría fortalecer dicho sistema.

REFERENCIAS BIBLIOGRÁFICAS

[1] CINDA, «MANUAL GESTIÓN ESTRATÉGICA UNIVERSITARIA: PROCESOS ADMINISTRATIVOS Y FINANCIEROS,» 1999. [En línea]. Available: http://www.academia.edu/5251841/MANUAL_GESTI%C3%93N_ESTRAT%C3%89GICA_UNIVERSITARIA_PROCESOS_ADMINISTRATIVOS_Y_FINANCIEROS_.

[2] SOX, «El impacto a más de cinco años de su aplicación,» 2002. [En línea]. Available: https://www.deloitte.com/view/es_CL/cl/ideas-y-perspectivas/sarbanes-oxley/.

[3] ISACA, «COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa,» 2012. [En línea]. Available: http://www.isaca.org/cobit/Pages/Thankyou.aspx.

[4] OCTAVE, «OCTAVE Method Implementation Guide Version 2.0 Volume 1y2,» 2011. [En línea]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=51558.

[5] MAGERIT, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método,» 2014. [En línea]. Available: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf.

[6] ISO, «ISO 31000-2009 La gestión de riesgos – Principios y directrices,» 2009. [En línea]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=43170.

[7] ITIL, «ITIL V.3 Manual íntegro,» 2013. [En línea]. Available: http://www.biable.es/wp-content/uploads/Recursosdescargables/Manual-ITIL.pdf.

[8] COSO, «Perspectivas para el nuevo marco de controles interno,» 2010. [En línea]. Available: http://vcdi.gob.bo/archivopaps/91570084-Proposed-Revisions-to-the-COSO-Framework-Spanish.pdf.

[9] ISO, «ISO 27000-2014 Information security management systems -- Overview and vocabulary,» 2014. [En línea]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411.

[10] PUCE, «Estatuto,» [En línea].

[11] PUCE, «Plan Estratégico de Desarrollo Institucional 2008-2013,» 2013.

[12] PUCE, «Plan estratégico de desarrollo institucional 2014-2018,» Quito, 2014.

[13] OSI-PGSI, «PUCE - Política general y normativa de seguridad de la información V1.0,» 2010.

[14] OSI-PDUF, «PUCE - Política detallada de usuario final para la seguridad de la información V1.0,» Quito, 2012.

[15] OSI-PNSL, «PUCE - Política detallada y normas de seguridad lógica de la información procesada con SI,» 2011.

[16] Verdezoto y Niama, Tesis - Evaluación técnica a los procesos de alta criticidad en la DI de la PUCE utlizando COBIT 5, Sangolquí: ESPE, 2014.

[17] PUCE-DI, «Informe de proyectos y principales actividades realizadas de julio a diciembre del 2014,» 2014.

[18] PUCE, «SINAPUCE. Presupuesto, servicio e infraestructura,» 2015. [En línea]. Available: http://es.calameo.com/read/000027008cec7d1637c02.

[19] DGF, «Proyecto Hacia el cambio - Contrato interno,» 2002.

[20] PUCE, «PORTAL WEB,» [En línea]. Available: http://www.puce.edu.ec/portal/content/Pontificia%20Universidad%20Cat%C3%B3lica%20del%20Ecuador/0?link=oln266n.redirect.

[21] DGF, «BLUE PRINT,» Quito, 2003.

[22] DGF, «DGF - Modelo de Control Financiero. Proy. Hacia el Cambio,» Quito, 2002.

[23] Fluidsignal, 2007. [En línea]. Available: http://www.slideshare.net/fluidsignal/analisis-de-riesgo-informatico-con-octave.

[24] Econocom-Osiatis, «ITIL-Gestión de Servicios TI,» [En línea]. Available: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php.

[25] «Experiencias de auditoría informática - Modelo COSO,» 2013. [En línea]. Available: https://chauditoriaucaldas1700711839.wordpress.com/2013/11/27/modelo-coso/.

[26] ISO27000.ES, «El portal de ISO 27001 en Español,» [En línea]. Available: http://www.iso27000.es/otros.html.

[27] PUCE-ORGANIGRAMA, «PUCE-ORGANIGRAMA ESTRUCTURAL,» [En línea]. Available: http://www.puce.edu.ec/documentos/Organigrama_may2013.pdf.

[28] PinkElephant, «COBIT,» 2012. [En línea]. Available: http://www.pinkelephant.com/uploadedFiles/Content/es-mx/Products/PinkPublication/FAQ-COBIT-V8.pdf.

[29] ISACA, «COBIT® Assessment Programme (PAM) Tool Kit: Using COBIT 5,» 2012. [En línea]. Available: http://www.isaca.org/cobit/Pages/Thankyou.aspx.

ANEXOS

ANEXO 1: PEDI PUCE 2014-2018

ANEXO 2: PROCESO CRÍTICOS DIRECCIÓN DE INFORMÁTICA PUCE

ANEXO 3: MATRIZ DE CUMPLIMIENTO DE OBJETOS DE PROCESO CRÍTICOS DIRECCIÓN DE INFORMÁTICA PUCE

ANEXO 4: NIVEL DE MADUREZ DEL PROCESO EDM03 – ASEGURAR LA OPTIMIZACIÓN DEL RIESGO

ANEXO 5: NIVEL DE MADUREZ DEL PROCESO APO13 – GESTIONAR LA SEGURIDAD

ANEXO 1: PEDI PUCE 2014-2018

Fuente: PUCE, Plan estratégico de desarrollo institucional 2014-2018

LEYENDA »
Objetivos estratégicos | Objetivos tácticos | Estrategias

ID	NOMBRE
OE 1	En los próximos 5 años, ofrecer a la sociedad profesionales integrales: conscientes, competentes, compasivos y comprometidos en el conocimiento de nuestra realidad, a través del fortalecimiento académico, investigativo y de vinculación con la colectividad
OT 1.1	Consolidar en los siguientes 5 años el modelo educativo de la PUCE como sustento del quehacer académico del SINAPUCE
E 1.1.1	Articular los programas académicos de pre y posgrado al modelo educativo de la PUCE en todo el SINAPUCE
E 1.1.2	Optimizar el proceso de gestión académica de pre y posgrado en el SINAPUCE
OT 1.2	Incrementar en los siguientes 2 años la producción científica del SINAPUCE, con trabajos y publicaciones que se articulen a las necesidades país, y que sean reconocidas nacional e internacionalmente en el medio académico y productivo
E 1.2.1	Implementar un proceso de producción científica estandarizado en cada unidad académica del SINAPUCE
E 1.2.2	Implementar un proceso de gestión editorial en todo el SINAPUCE
E 1.2.3	Gestionar el seguimiento de la investigación en el SINAPUCE
OT 1.3	Incrementar en los siguientes 2 años la participación de la comunidad universitaria en los procesos de: acción social, pasantías, prácticas pre profesionales y servicios de extensión del sistema de vinculación con la colectividad del SINAPUCE
E 1.3.1	Articular los procesos de vinculación con la colectividad identificados en el SINAPUCE
OE 2	En los próximos 5 años, perfeccionar el sistema de gestión integral del SINAPUCE a través de la implementación de buenas prácticas de gestión de infraestructura física, tecnológica, educativa y financiera, que apoyen de manera transversal y eficiente a la comunidad universitaria en sus tareas fundamentales
OT 2.1	Gestionar en los próximos 2 años la insfraestructura física, tecnológica y educativa del SINAPUCE de tal manera que cumpla eficientemente con estándares nacionales e internacionales
E 2.1.1	Adecuar la infraestructura física, tecnológica y educativa en función de los objetivos estratégicos en todo el SINAPUCE
OT 2.2	Invertir en los siguientes 5 años eficientemente los recursos financieros en las áreas estratégicas del SINAPUCE
E 2.2.1	Rediseñar los procesos financieros de soporte en función de las áreas estratégicas del SINAPUCE
OE 3	Implementar en los próximos 5 años un sistema de gestión administrativa y laboral que asegure la eficiencia en el desempeño del talento humano del SINAPUCE, a través del fortalecimiento de competencias, desarrollo profesional y seguimiento continuo que propendan al desarrollo institucional
OT 3.1	Desarrollar en los siguientes 5 años una nueva estructura funcional del SINAPUCE, a través de la reorganización de procesos y talento humano para alcanzar los objetivos misionales
E 3.1.1	Implementar un modelo para la organización del trabajo dentro del SINAPUCE
OT 3.2	Optimizar en los siguientes 2 años el desempeño del talento humano a través de una adecuada selección, capacitación, evaluación y desarrollo profesional que aporte en los diferentes ámbitos misionales y de soporte del SINAPUCE
E 3.2.1	Implementar un programa de mejoramiento de competencias del talento humano en el SINAPUCE
E 3.2.2	Articular subprocesos de talento humano a las áreas estratégicas del SINAPUCE
OT 3.3	Promover en los próximos 5 años un ambiente de bienestar que contribuya al desarrollo integral de la comunidad universitaria del SINAPUCE
E 3.3.1	Convertir los campus del SINAPUCE en campus seguros, saludables y sostenibles
OE 4	Para el año 2018, implementar estándares de evaluación y acreditación nacional e internacional, haciendo uso de las mejores metodologías de gestión universitaria, en búsqueda del mejoramiento y crecimiento continuo del SINAPUCE
OT 4.1	Desarrollar en los próximos 5 años en el SINAPUCE carreras y programas pertinentes a la realidad nacional
E 4.1.1	Investigar y desarrollar nuevos carreras y programas académicos para el SINAPUCE
OT 4.2	Diseñar e implementar en los proximos 5 años un sistema de mejoramiento continuo que asegure el cumplimiento de los objetivos institucionales del SINAPUCE
E 4.2.1	Gestionar la organización, métodos, procesos de planificación y control del SINAPUCE
E 4.2.2	Elaborar un marco juridico técnico para el mejoramiento de las áreas estratégicas del SINAPUCE
OT 4.3	Lograr en los próximos 5 años que la comunicación interna y externa del SINAPUCE sea eficaz
E 4.3.1	Articular las relaciones públicas y la comunicación interna y externa a las áreas estratégicas del SINAPUCE
OT 4.4	En los próximos 5 años aprovechar la cooperación nacional e internacional para la consecución de los objetivos del SINAPUCE

ANEXO 2: PROCESO CRÍTICOS DIRECCIÓN DE INFORMÁTICA PUCE

Fuente: Verdezoto y Niama, Evaluación técnica a los procesos de alta criticidad en la DI de la PUCE utilizando COBIT 5

PROCESO:	EDM03	Asegurar la Optimización del Riesgo
DESCRIPCIÓN:	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	
PROPÓSITO:	Asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.	

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	5	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	2	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	5	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	4	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	4	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	5	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	5	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	4	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	1	IT	Otro interno	tercero	No del todo definido	No sabe
	CRITICIDAD	38.750					

PROCESO:	APO11	Gestionar la Calidad
DESCRIPCIÓN:	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	
PROPÓSITO:	Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.	

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	4	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	4	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	5	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	4	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	5	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	5	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	5	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	5	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	4	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	39.125					

PROCESO:	APO12	Gestionar el Riesgo	
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.		

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	4	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	3	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	3	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	3	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	3	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	5	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	4	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	3	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	2	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	28.250					

PROCESO:	APO13	Gestionar la Seguridad	
DESCRIPCIÓN:	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.		
PROPÓSITO:	Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.		

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	5	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	3	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	3	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	3	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	4	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	5	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	5	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	3	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	1	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	36.875					

PROCESO:	BAI01	Gestión de Programas y Proyectos	
DESCRIPCIÓN:	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.		
PROPÓSITO:	Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.		

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	3	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	2	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	4	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	3	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	4	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	5	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	5	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	4	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	1	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	29.500					

PROCESO:	BAI06	Gestionar los Cambios	
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.		

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	4	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	2	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	3	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	2	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	2	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	3	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	5	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	3	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	1	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	25.125					

PROCESO:	DSS05	Gestionar Servicios de Seguridad
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.	
PROPÓSITO:	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	4	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	2	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	3	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	2	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	2	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	5	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	4	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	2	Continuamente monitoreadas y mitigadas	Regularmente monitoreadas y muchas bajo control	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
10	¿Quién lo realiza?	1	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	21.125					

PROCESO:	DSS06	Gestionar Controles de Proceso de Negocio
DESCRIPCIÓN:	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	
PROPÓSITO:	Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.	

No.	PREGUNTA	VALOR	1	2	3	4	5
1	¿Qué tan importante es el proceso para el éxito de la empresa?	4	No es importante	Se puede obviar	Facilita las cosas	Muy significativo	Crítico
2	¿El proceso se desempeña bien?	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	¿Está claro quién debe responder por los resultados finales?	4	Sí, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma acción	Alguien lo asume así	No está totalmente claro
4	¿El proceso se lleva a cabo formalmente?	3	Todos los aspectos están documentados y son repetibles	Todos los aspectos son repetibles, sin formalidad documentada	Algunos aspectos son repetibles y están documentados	Algunos aspectos son repetibles, sin formalidad	Definitivamente no
5	¿Está claro quién debe responder por el proceso?	4	Todo el mundo lo conoce y el responsable lo acepta	Mucha gente lo sabe y el responsable lo acepta en buena medida	Alguien lo sabe; el responsable acepta parcialmente	Alguien lo sabe; el responsable lo sabe pero no toma acción	Nadie sabe
6	¿El proceso tiene una dirección y unos objetivos claros?	4	Los objetivos están integrados en los indicadores de desempeño	Se conocen, pero no están ligados con indicadores	Documentado pero no ha habido la necesaria divulgación	Conocidos por la alta dirección, no documentados ni divulgados	No del todo
7	¿El proceso es medido?	3	Las mediciones existen y están integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad, no se liga con objetivos	Algunas medidas de efectividad	Algunas medidas financieras	No del todo
8	¿El proceso es auditado?	4	Basado en riesgos y los resultados siempre reciben acción	Parte del plan está basado en riesgos y los resultados regularmente reciben acción	La regularidad y los resultados ocasionalmente reciben acción	*Ad hoc*	No del todo
9	¿El proceso tiene debilidades de control conocidas?	4	Continuamente monitoreadas y	Regularmente monitoreadas y muchas	Reconocidas, pero aun no tratadas	Hay conciencia de que hay que hacer algo al	No se sabe acerca de las
10	¿Quién lo realiza?	1	IT	Otro interno	Tercero	No del todo definido	No sabe
	CRITICIDAD	24.875					

ANEXO 3: MATRIZ DE CUMPLIMIENTO DE OBJETOS DE PROCESO CRÍTICOS DIRECCIÓN DE INFORMÁTICA PUCE

Fuente: Verdezoto y Niama, Evaluación técnica a los procesos de alta criticidad en la DI de la PUCE utlizando COBIT 5

EDM03	Asegurar la Optimización del Riesgo			
	Propósito	Cumplir con el requerimiento de la empresa de tener estables, rentables, integrados y estandarizados los sistemas de aplicación, recursos y capacidades que cumplen con los requisitos actuales y futuros de la empresa.		
	Criterios	**Métricas Relacionadas**	**Cumple %**	**Comentarios**
PA 1.1 El proceso alcanza su propósito.	EDM03-01 Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	Nivel de alineamiento entre riesgo TI y riesgo de negocio	70%	El negocio es la educación por lo que los riesgos que conciernen a los sistemas están alineados con el negocio
		Número de potenciales riesgos TI identificados y gestionados	75%	Se ha gestionado con implementación de IDS, Firewall, Certificados, etc.
		Frecuencia de refresco de la evaluación de los factores de riesgo	50%	Se realiza anualmente, aunque debería también realizarse cuando se produce algún cambio importante
	EDM03-02 La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	Porcentaje de proyectos de la empresa que consideran el riesgo TI	10%	Los riegos de TI casi no son tomados en cuenta en los proyectos de la institución
		Porcentaje de planes de acción de riesgo TI ejecutados en tiempo	70%	Se ha implementado a tiempo herramientas para disminuir los riesgos que pueden afectar a la institución
		Porcentaje de riesgos críticos que han sido eficazmente mitigados	75%	Se han implementado las medidas necesarias para su mitigación
	EDM03-03 Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado.	Nivel de impacto empresarial inesperado	90%	Se han producido muy pocos incidentes inesperados
		Porcentaje de riesgos TI que exceden el riesgo empresarial tolerado	95%	El porcentaje de riesgos que exceden el nivel tolerado es bajo y se debe a causas inesperadas

APO13	Gestionar la Seguridad			
	Propósito	Cumplir con los requisitos de la empresa de asegurar el alineamiento de los servicios TI clave con las necesidades del negocio.		
	Criterios	**Métricas Relacionadas**	**Cumple %**	**Comentarios**
PA 1.1 El proceso alcanza su propósito.	APO13-01 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	100%	Existe la oficina de seguridad que se encarga de la gestión de seguridad
		Número de incidentes relacionados con la seguridad	80%	Hay gran cantidad de incidentes de seguridad pero la mayoría se encuentran mitigados
	APO13-02 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	95%	Se realizó una encuesta
		Número de soluciones de seguridad que se desvían del plan	90%	Las soluciones implementadas van de acuerdo al plan
		Número de soluciones de seguridad que se desvían de la arquitectura de la empresa	95%	Las soluciones que se han dado, son tomando en cuenta la arquitectura de la institución
	APO13-03 Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	Número de servicios con alineamiento confirmado al plan de seguridad	85%	Se han alineado al plan de seguridad existente la mayoría de servicios, los que faltan que son un 15% son recientes
		Número de incidentes de seguridad causados por la no observancia del plan de seguridad	100%	No se ha producido ningún incidente
		Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad	90%	Las que se han desarrollado son las que están en el plan de seguridad y otras

ANEXO 4: NIVEL DE MADUREZ DEL PROCESO EDM03 – ASEGURAR LA OPTIMIZACIÓN DEL RIESGO

Fuente: Verdezoto y Niama, Evaluación técnica a los procesos de alta criticidad en la DI de la PUCE utilizando COBIT 5

Tabla 81 Madurez EDM03 Asegurar la Optimización del Riesgo

Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
EDM03		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Puntuación de los Criterios		L (70%)	P (42%)	P (20%)						
Nivel de Madurez Conseguido		1								

N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%

EDM03	Asegurar la Optimización del Riesgo							
	Propósito	Cumplir con los requisitos actuales y futuros de la empresa de tener estables, rentables, integrados y estandarizados los sistemas de aplicación, recursos y capacidades.						
	Evaluar si se consiguen los siguientes resultados.	Criterios	Cumple con los Criterios S/N	Comentarios	No Alcanzados (0-15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzado (85-100%)
Nivel 0 Incompleto	El proceso no se ha implementado, o no ha logrado conseguir su propósito.	En este nivel, hay poca o ninguna evidencia del cumplimiento del propósito del proceso.						
Nivel 1 Ejecutado	PA 1.1 El proceso alcanza su propósito.	Los siguientes resultados del proceso se están cumpliendo:	Valoración General del Proceso					
		EDM03-01 Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	S	Los riesgos han sido identificados por la oficina de seguridad, la DI conoce varios riesgos a los que se encuentran expuestos			65%	
		EDM03-02 La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	S	Varios riesgos críticos han sido mitigados			52%	
		EDM03-03 Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado.	S	Se ha mantenido un buen control de riesgos aunque se han producido eventualidades inesperadas				93%

Tabla 81 Madurez EDM03 Asegurar la Optimización del Riesgo

Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
EDM03		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Puntuación de los Criterios		L (70%)	P (42%)	P (20%)						
Nivel de Madurez Conseguido		1								

N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%

EDM03	Asegurar la Optimización del Riesgo							
	Propósito	Cumplir con los requisitos actuales y futuros de la empresa de tener estables, rentables, integrados y estandarizados los sistemas de aplicación, recursos y capacidades.						
	Evaluar si se consiguen los siguientes resultados.	Criterios	Cumple con los Criterios S/N	Comentarios	No Alcanzados (0-15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzado (85-100%)
Nivel 2 Gestionado	PA 2.1 Gestión del Desempeño - Una medida del grado en que se gestiona el desempeño del proceso.	Como resultado de la plena consecución de este atributo: a) Los objetivos de desempeño del proceso son identificados.	S	La oficina de seguridad tiene identificados los objetivos de este proceso y es responsable del mismo conjuntamente con la DI, esta oficina tiene identificados los recursos que necesita pero hay una debilidad en la comunicación con la DI		42%		
		b) El desempeño del proceso está planeado y monitoreado.	N					
		c) El desempeño del proceso está ajustado para cumplir los planes.	N					
		d) Los responsables y las autoridades encargados del proceso están definidos, asignados y comunicados.	S					
		e) Los recursos e información necesaria para ejecutar el proceso están identificados, disponibles, asignados y utilizados.	S					
		f) Las interfaces entre las partes interesadas son gestionadas para garantizar una comunicación efectiva y una clara asignación de responsabilidades.	N					
	PA 2.2 Gestión del Producto del Trabajo - Una medida del grado en la que los productos de trabajo proporcionados por	Como resultado de la plena consecución de este atributo: a) Los requerimientos para los productos de trabajo del proceso están definidos.	N	La oficina de seguridad ha elaborado cierta documentación necesaria para el desenvolvimiento		20%		
		b) Los requerimientos de documentación y control de los productos de trabajo están definidos.	S					
		c) Los productos de trabajo están adecuadamente identificados, documentados y controlados.	N					
		d) Los productos de trabajo son revisados de acuerdo a un plan previsto y ajustados si es necesario para cumplir con los requerimientos.	N					

ANEXO 5: NIVEL DE MADUREZ DEL PROCESO APO13 – GESTIONAR LA SEGURIDAD

Fuente: Verdezoto y Niama, Tesis - Evaluación técnica a los procesos de alta criticidad en la DI de la PUCE utlizando COBIT 5, Sangolquí: ESPE, 2014

Tabla 85 Madurez APO13 Gestionar la Seguridad

Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
APO13		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Puntuación de los Criterios		F (92%)	P (33%)	N (0%)						
Nivel de Madurez Conseguido		1								

N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%

APO13	Gestionar la Seguridad						
	Propósito	Cumplir con los requisitos de la empresa de asegurar el alineamiento de los servicios TI clave con las necesidades del negocio.					
	Evaluar si se consiguen los siguientes resultados.	Criterios	Cumple con los Criterios S/N	Comentarios	No Alcanzados (0-15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzado (85-100%)
Nivel 0 Incompleto	El proceso no se ha implementado, o no ha logrado conseguir su propósito.	En este nivel, hay poca o ninguna evidencia del cumplimiento del propósito del proceso.						
Nivel 1 Ejecutado	PA 1.1 El proceso alcanza su propósito.	Los siguientes resultados del proceso se están cumpliendo:	Valoración General del Proceso					
		APO13-01 Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	S	Se definió la oficina de seguridad que es la responsable de gestionar la seguridad de TI conjuntamente con la Dirección de Informática				90%
		APO13-02 Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	S	Existe un plan de seguridad difundido en toda la institución				93%
		APO13-03 Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	S	Se han implementado las soluciones de seguridad de la información de manera consistente				92%
Nivel 2 Gestionado	PA 2.1 Gestión del Desempeño - Una medida del grado en que se gestiona el desempeño del proceso.	Como resultado de la plena consecución de este atributo:						
		a) Los objetivos de desempeño del proceso son identificados.	N					
		b) El desempeño del proceso está planeado y monitoreado.	N					
		c) El desempeño del proceso está ajustado para cumplir los planes.	N	El desarrollo del proceso se encuentra en fase preliminar		33%		
		d) Los responsables y las autoridades encargados del proceso están definidos, asignados y comunicados.	S					

APO13	Gestionar la Seguridad							
	Propósito	Cumplir con los requisitos de la empresa de asegurar el alineamiento de los servicios TI clave con las necesidades del negocio.						
	Evaluar si se consiguen los siguientes resultados.	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	No Alcanzados (0-15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzado (85-100%)
		e) Los recursos e información necesaria para ejecutar el proceso están identificados, disponibles, asignados y utilizados.	S					
		f) Las interfaces entre las partes interesadas son gestionadas para garantizar una comunicación efectiva y una clara asignación de responsabilidades.	N					
	PA 2.2 Gestión del Producto del Trabajo - Una medida del grado en la que los productos de trabajo proporcionados por el proceso son bien manejados. Los productos de trabajo (o salidas del proceso) se definen y controlan.	Como resultado de la plena consecución de este atributo:						
		a) Los requerimientos para los productos de trabajo del proceso están definidos.	N					
		b) Los requerimientos de documentación y control de los productos de trabajo están definidos.	N		0%			
		c) Los productos de trabajo están adecuadamente identificados, documentados y controlados.	N					
		d) Los productos de trabajo son revisados de acuerdo a un plan previsto y ajustados si es necesario para cumplir con los requerimientos.	N					