Modelo de medición bajo la metodología ajustada PAM de la implementación del Capítulo IV Título I Parte I de la circular básica Jurídica 29 de 2014 de la superintendencia financiera mapeado bajo el modelo COSO y COBIT 5.

Sergio Giraldo Henao.
Junio 2017.

Universidad del Norte.
Atlántico.
Trabajo de grado II

Abstract

El propósito de este trabajo consiste en presentar un modelo de medición estándar para la implementación de los elementos de sistema de control interno referente a las tecnologías de información dentro de la circular jurídica 29 de la superintendencia financiera de Colombia (SFC), de modo que sea posible medir y comparar el grado de implementación de prácticas de gobiernos en las diversas entidades supervisadas por la SFC o quienes decidan acoplarse a lo solicitado por la circular.

Tabla de Contenidos

Contents

Capítulo 1
Formulación del Problema

Antecedentes

El Gobierno de TI, sistemas robustos de control interno y su implementación en los ambientes productivos de la empresas colombianas, se ha convertido al igual que en el resto del mundo en un punto crítico para establecer ventajas competitivas en la industria. A nivel del sector financiero Colombiano, y las entidades que por ende son vigiladas por la Superintendencia Financiera de Colombia (SFC) la implementación de esquemas de Gobierno de TI no es solo una propuesta, sino también en alguno de sus aspectos requerimientos explícitos del regulador, los cuales deben ser cumplidos por todas las entidades vigiladas.

En este ámbito cabe señalar que en Colombia existe la Circular Básica Jurídica 29 del 2014 (C.E 29/14) la cual establece lineamientos frente a diferentes aspectos que los entes vigilados deben cumplir, entre ellos se encuentra el Capítulo 5, el cual trata sobre el sistema de control interno, el cual se encuentra alienado con las buenas prácticas de COSO.

A nivel de TI la CE 29/14 establece linimentos frente a temas como:

- Plan estratégico de tecnología.
- Infraestructura de tecnología.
- Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
- Administración de proyectos de sistemas.
- Administración de la calidad.
- Adquisición de tecnología.
- Adquisición y mantenimiento de software de aplicación.
- Instalación y acreditación de sistemas.
- Administración de cambios.
- Administración de servicios con terceros.
- Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
- Continuidad del negocio.
- Seguridad de los sistemas.
- Educación y entrenamiento de usuarios.
- Administración de los datos.
- Administración de instalaciones.
- Administración de operaciones de tecnología.
- Documentación.

Todos estos puntos son evaluados con periodicidad por quienes hacen las veces de revisores fiscales de las entidades, quienes basado en buenas prácticas y marcos de referencia (COSO, COBIT, etc) generan informes de cumplimiento (cumple, no cumple)

para las organizaciones supervisadas lo cual no permite visualizar a nivel de industria el grado de implementación de las buenas practicas bajo metodologías de madures como el "Process Assessment Model" (PAM).

Planteamiento del problema

El grado de implementación de buenas prácticas en los puntos planteados en la CE 29/2014 de la SFC, es un tema que aunque es evaluado por el regulador, es medido en 2 puntos: cumple o no cumple, lo cual no permite realizar ejercicios de Benchmarking u Open Innovation en el sector, esto representa un costo de oportunidad desperdiciado para el sector financiero de Colombia, si bien la misma regulación previene o desestimula el hecho de compartir abiertamente las prácticas empresariales, la oportunidad de implementar esquemas de innovación abierta o comparativa mediante el uso de reportes detallados sobre el nivel de implementación o buenas practicas referentes y dentro del alcance de este trabajo a el ambiente de control de TI presenta beneficios que deberían ser aprovechados por el sector.

Justificación

Como primer paso para cambiar esta realidad, este trabajo plantea diseñar un modelo de medición de madurez estándar, basado en modelos globalmente reconocidos como son COSO, COBIT y PAM, con el fin de establecer una herramienta que permita realizar análisis de benchmarking para el sector.

El uso de esta herramienta permitiría a las empresas vigiladas comparar sus procesos de control interno de TI contra las buenas prácticas usadas por otras empresas del sector lo cual abra el camino para mejorar en prácticas de control mediante nuevos modelos de alianzas, innovación abierta; lo cual permita la mejora de los controles presentes en las entidades, posiblemente previniendo desfalcos generados por fraudes o errores humanos en el sector financiero.

Capítulo 2
Objetivos

Objetivo general

Establecer un modelo de medición estándar para la implementación del capítulo IV Título I de la circular básica Jurídica 29 de 2014 de la superintendencia financiera de Colombia.

Objetivo Especifico 1:

Desarrollar un modelo conceptual desde la perspectiva GyG-IT que permita establecer las buenas prácticas para la implementación de instrumentos de medición para los organismos de vigilados en por la superintendencia financiera.

Objetivo Especifico 2:

Mapear los objetivos de control del modelo Cobit 5 a la Circular básica jurídica 29 de 2014 y establecer un conjunto de actividades claves que facilite el cumplimiento de la norma citada

Objetivo Especifico 3:

Identificar los requisitos mínimos por cada nivel del PAM para los objetivos de control de Cobit 5 mapeados contra la circular.

Objetivo Especifico 4:

Formular un caso de aplicación del modelo propuesto que permita validar el, implementación del Capítulo IV Título I Parte I de la circular básica Jurídica 29 de 2014

Capítulo 3 Metodología

La metodología mediante la cual se desarrollará este trabajo, consiste en analizar los componentes individuales de: COSO, COBIT, PAM y CE 29 /14 Parte 1, Título I, Capitulo IV, con el fin de identificar lo siguiente:

Análisis CE 29 /14 Parte 1, Título I, Capitulo IV: identificación de los requisitos frente a los componentes de sistemas de control interno mínimos para todas las entidades vigiladas por la SFC así como los componentes específicos indicados para TI.

Análisis COSO: buenas prácticas frente a los componentes de los sistemas de control interno, este estándar dará la base para identificar los macro componentes que deben contener lo indicado por la SFC

Análisis COBIT: Identificación y mapeo, de todos los objetivos de control aplicables a lo requerido por la SFC, en el marco de las buenas prácticas de COSO, de modo que para cada requerimiento, se identifiquen buenas prácticas según los objetivos de control del modelo COBIT

Análisis PAM: una vez identificados los objetivos de control relevantes en COBIT 5, se procederá a mapear los requerimientos para cada uno de los 6 niveles del PAM (0 – 5) con el fin de obtener criterios de medición y comparación para cada uno de los requerimientos de la CE 29 /14 Parte 1, Título I, Capitulo IV

Adicionalmente se realizará la ejecución en 4 fases descritas a continuación:

Fase 1: Elaboración del Marco Conceptual: Esta fase tiene como propósito desarrollar el marco conceptual a partir de una revisión sistemática de la Bibliografía en los temas relacionados con (lista de keywords) utilizando como fuentes de información: ELSEVIER, IEEE-XPLORE, ACM, ISACA, ITIL, COSO, entre otras.

Partiendo de los conceptos presentados en la CE 29 /14 Parte 1, Título I, Capitulo IV y desarrollando los conceptos a medida que estos se hacen relevantes en las siguientes fases del trabajo

Fase 2: Mapeo de Procesos: Realizar un mapeo inicial de los elementos de la CE 29 frente a los principios de COSO los cuales serán utilizados como guía para identificar los procesos principales del COBIT 5 que deben ser cumplidos para cumplir el objetivo deseado y por tanto lograr una calificación 1 del modelo

Fase 3: Identificación de inputs de otros procesos (Mapeo Secundario):
Partiendo de los objetivos de control identificados en la Fase se identifican los inputs necesarios para su ejecución y a su vez se identifican los objetivos de control necesarios para cumplir los objetivos principales

Fase 4: Propuesta de implementación: una vez generado el modelo de medición se identifican las propuestas implementación de los objetivos de control identificados para implementar la CE29, y se realiza la propuesta al regulador para implementar la herramienta de medición como un objeto efectivo de benchmarking para la industria

Capítulo 4
Marco Teórico

Posterior a realizar una búsqueda extensiva en fuentes de investigación, no fue posible encontrar referencias de normativas internacionales que presenten requerimientos puntuales sobre gobierno corporativo y ambiente de control similares a los presentados en la CE29, sin embargo se identificó que por lo general la normativa habla de la importancia de la TI en los ambientes de control modernos y establece la necesidad de incluir controles generales de TI, sin especificar controles o requerimientos dado que dejan en manos de los supervisado la definición de los mismos. Ejemplos (LEY SOX, COSO)

Por tal razón en este apartado se pretender exponer las generalidades de los puntos presentados en la norma así:

- Plan estratégico de tecnología:

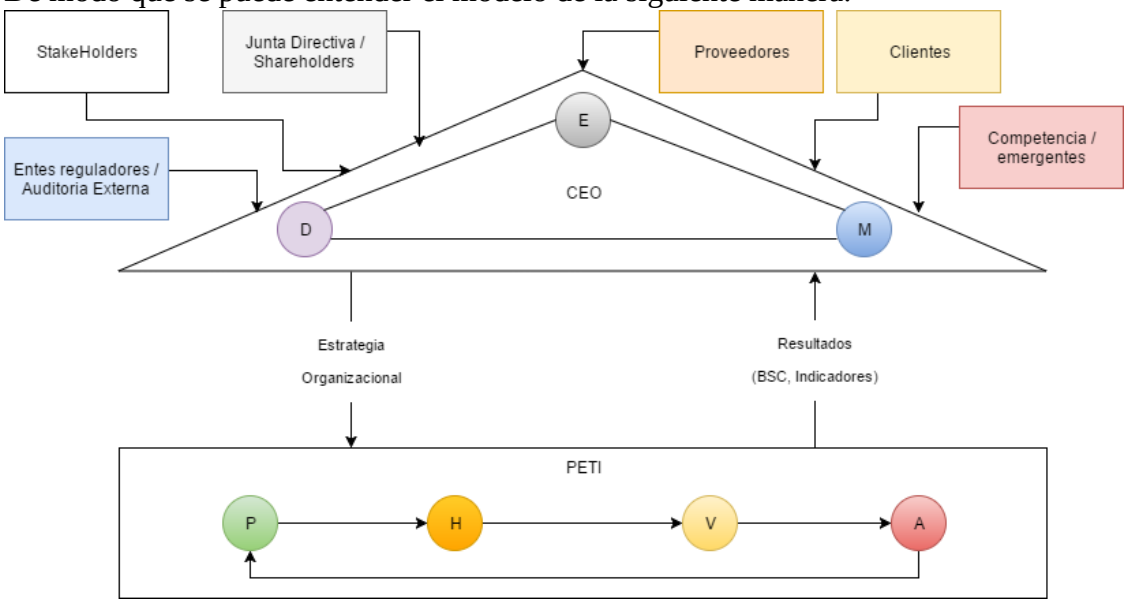
Según la definición presentada en la CE29: "Las entidades deben realizar un proceso de planeación estratégica de tecnología, a intervalos de tiempo regulares, con el propósito de lograr el cumplimiento de los objetivos de la organización a través de las oportunidades que brinda la tecnología a su alcance. El plan estratégico de tecnología debe estar alineado con el plan estratégico institucional y en él se deben contemplar adicionalmente, al menos, los siguientes aspectos:
- Análisis de cómo soporta la tecnología los objetivos del negocio.
- Evaluación de la tecnología actual.
- Estudios de mercado y factibilidad de alternativas tecnológicas que respondan a las necesidades de la entidad.
- Planes operacionales estableciendo metas claras y concretas "

Aun cuando la circula es clara en los puntos mínimos que debe incluir el plan estratégico de TI y su objetivo principal, también se debe expandir esta definición para entender que el PETI es el elemento conector principal del gobierno de TI a la gestión de TI, en otras palabras es el elemento que articula las necesidades de todos los stakeholder de la organización con las estrategias y proyectos necesarios para dar respuestas (directa o indirectamente) a los mismos desde TI.

Tomando de Cobit 5 se puede encontrar que el plan estratégico es el documento que "Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado.
Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos." y cuyo propósito radica en "Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos

y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio."

De modo que se puede entender el modelo de la siguiente manera:



- Infraestructura de tecnología: en la CE29, se hace referencia a la infraestructura de TI como la base que soporta los servicios tecnológicos que apalancan los objetivos del negocio, este contexto se entiende que la infraestructura forma parte de la arquitectura de TI que soporta la organización.

- Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico: de acuerdo con la CE29 y en concordancia con el modelo COSO en el cual se basan tanto la circular como los ambientes de control interno de se deben contar con procesos de monitoreo que le permitan identificar y cumplir con los requerimientos de regulatorios de su entorno.

- Administración de proyectos de sistemas: según el PMI: "es la aplicación del conocimiento, de las habilidades, y de las técnicas para ejecutar los proyectos en forma eficiente y efectiva. Es una competencia estratégica para las organizaciones, y les permite atar los resultados de los proyectos a las metas del negocio, y así competir mejor en su mercado" enmarcado dentro de la definición de proyecto: "una actividad grupal temporal para producir un producto, servicio, o resultado, que es único."

  Es temporal dado que tiene un comienzo y un fin definido, y por lo tanto tiene un alcance y recursos definidos.

Es único ya que no es una operación rutinaria, sino un conjunto específico de operaciones diseñadas para lograr una meta particular. Un equipo de proyecto a menudo incluye a las personas que no siempre trabajan juntas, y a veces son de distintas organizaciones o de varias regiones o países distintos.

Los ejemplos de proyectos incluyen, entre otros, el desarrollo de un software para mejorar un proceso de negocio, la construcción de un puente o de un edificio, un esfuerzo de recuperación luego de un desastre natural, o la entrada en un nuevo mercado para vender.

Es importante la administración de proyectos dado que la gran mayoría de implementaciones tecnológicas se llevan a cabo mediante esta herramienta, por tal motivo es solicitada por la CE29.

- Administración de la calidad: Con el objeto de satisfacer las necesidades de sus clientes (internos y externos), las entidades deben llevar a cabo la planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad de la tecnología que contengan:

    - Programas para establecer una cultura de calidad de la tecnología en toda la entidad.
    - Planes concretos de calidad de la tecnología.
    - Responsables por el aseguramiento de la calidad.
    - Prácticas de control de calidad.
    - Metodología para el ciclo de vida de desarrollo de sistemas.
    - Metodología de prueba y documentación de programas y sistemas.
    - Diseño de informes de aseguramiento de la calidad.
    - Capacitación de usuarios finales y del personal de aseguramiento de la calidad.
    - Desarrollo de una base de conocimiento de aseguramiento de la calidad.

  El sistema de administración de la calidad debe ser objeto de evaluaciones periódicas para ajustarlo a las necesidades de la entidad.

- Adquisición de tecnología, Adquisición y mantenimiento de software de aplicación e Instalación y acreditación de sistemas: 3 ítem presentados en la CE 29 en los cuales se espera que las organizaciones cuenten con procesos y procedimientos los cuales les permitan coordinar y ejecutar la adquisición de tecnología y software, desde pasando por su instalación y acreditación. En consunto con la administración de proyectos del punto anterior, estos se consolidan como las principales herramientas para establecer servicios de TI sólidos.

- Administración de cambios: al igual que todos los sistemas la TI, su administración y gobierno, deben ser adaptables a su entorno, ya sea por que surgen nuevos

requerimientos o nuevos objetivos organizacionales, los cuales requieren del ajuste de los modelos preestablecidos o bien por se deben atender incidentes y/o problemas los cuales puedan impactar la operación y la consecución de los objetivos organizacionales.

Con el fin de minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, se debe diseñar un sistema de administración que permita el análisis, implementación y seguimiento de los cambios requeridos y llevados a cabo a la infraestructura de tecnología que posea la entidad. Como mínimo se tienen que contemplar los siguientes aspectos:

- Identificación clara del cambio a realizar en la infraestructura.
- Categorización, priorización y procedimientos de emergencia a llevar a cabo durante el cambio.
- Evaluación del impacto que ocasiona el cambio en la infraestructura.
- Procedimiento de autorización de los cambios.
- Procedimiento de administración de versiones.
- Políticas de distribución del software.
- Obtención de herramientas automatizadas para realizar los cambios.
- Procedimientos para la administración de la configuración.
- Rediseño de los procesos del negocio que se vean impactados por el cambio en la infraestructura.

- Administración de servicios con terceros: la CE 29 solicita el establecimiento de procesos que aseguren que las terceras partes críticas para el funcionamiento de los procesos de TI son adecuadamente identificados y que se cuenta con SLAs los cuales son monitoreados con el fin de garantizar el cumplimiento de los objetivos para los cuales fueron contratados los terceros.

  En un ambiente en el que es cada vez más común acceder a servicios tercerizados con ambientes en la nube y esquemas de aplicaciones infraestructura y plataforma como servicio es crítico que las compañías cuenten con procesos sólidos para la administración de los mismos.

- Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica: Una vez constituida la infraestructura, los aplicativos y servicios de TI que respaldan las operaciones y objetivos organizacionales, las entidades deben encontrarse en la capacidad de medir y gestión el desempeño, la capacidad y disponibilidad de los mismos, componentes críticos para garantizar que los servicios prestados son confiables y apalancan la estrategia.

- Continuidad del negocio: La CE requiere que la entidades reguladas cumplan con el establecimiento de procesos de continuidad, que se encarguen de medir los riesgos a los que están expuestas las organizaciones y plantear los escenarios de recuperación de TI necesarios con el fin de garantizar la continuidad y supervivencia de la organización en casi de presentarse algún incidente que amenace la consecución de los objetivos organizacionales y la supervivencia de la entidad.

- Seguridad de los sistemas: Con el objeto de salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, corresponde a las entidades supervisadas establecer controles de acceso lógico que aseguren que los sistemas, datos y programas están restringidos exclusivamente a usuarios autorizados, para lo cual se debe contar con procedimientos y recursos sobre los siguientes aspectos:

    - Autorización, autenticación y control de acceso.
    - Identificación de usuarios y perfiles de autorización, los cuales deben ser otorgados de acuerdo con la necesidad de tener y necesidad de conocer.
    - Manejo de incidentes, información y seguimiento.
    - Prevención y detección de código malicioso, virus, entre otros.
    - Entrenamiento de usuarios.
    - Administración centralizada de la seguridad.

- Educación y entrenamiento de usuarios: Como una parte importante de la implementación de los puntos mencionados en la CE 29 y de todos los usuarios deben ser entrenados en los procesos establecidos, de modo que estos puedan ser adecuadamente ejecutados y se vuelvan parte de la cultura organizacional.

- Administración de los datos: Para que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento en los sistemas de información, las entidades tienen que establecer controles generales y de aplicación sobre la operación de la tecnología, atendiendo como mínimo los siguientes aspectos:

    - Establecer controles de entrada, procesamiento y salida para garantizar la autenticidad e integridad de los datos.
    - Verificar la exactitud, suficiencia y validez de los datos de transacciones que sean capturados para su procesamiento (generados por personas, por sistemas o entradas de interface).
    - Preservar la segregación de funciones en el procesamiento de datos y la verificación rutinaria del trabajo realizado. Los procedimientos deben incluir controles de actualización adecuados, como totales de control "corrida a corrida" y controles de actualización de archivos maestros.

- Establecer procedimientos para que la validación, autenticación y edición de los datos sean llevadas a cabo tan cerca del punto de origen como sea posible.
- Definir e implementar procedimientos para prevenir el acceso a la información y software sensitivos de computadores, discos y otros equipos o medios, cuando hayan sido sustituidos o se les haya dado otro uso. Tales procedimientos deben garantizar que los datos marcados como eliminados no puedan ser recuperados por cualquier individuo interno o tercero ajeno a la entidad.
- Establecer los mecanismos necesarios para garantizar la integridad continua de los datos almacenados.
- Definir e implementar procedimientos apropiados y prácticas para transacciones electrónicas que sean sensitivas y críticas para la organización, velando por su integridad y autenticidad.
- Establecer controles para garantizar la integración y consistencia entre plataformas.

- Administración de instalaciones: Con el objeto de proporcionar un ambiente físico conveniente que proteja los equipos y el personal de tecnología contra peligros naturales o fallas humanas, las entidades deben instalar controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su buen funcionamiento teniendo en cuenta, entre otros, los siguientes aspectos:

  - Acceso a las instalaciones.
  - Identificación clara del sitio.
  - Controles de seguridad física.
  - Definición de políticas de inspección y escalamiento de problemas.
  - Planeamiento de continuidad del negocio y administración de crisis.
  - Salud y seguridad del personal.
  - Políticas de mantenimiento preventivo.
  - Protección contra amenazas ambientales.
  - Monitoreo automatizado

- Administración de operaciones de tecnología: de acuerdo con ITIL: “Monitorear y controlar los servicios e infraestructuras de TI. La Gestión de Operaciones de TI lleva a cabo tareas diarias relacionadas con la operación de componentes y aplicaciones de infraestructura. Esto incluye la programación de trabajos en un calendario, actividades de soporte y restauración y el mantenimiento rutinario.

- Documentación: este punto solicitado en la CE 29 obedece a que los procesos de TI se encuentren adecuadamente documentados, aunque en el modelo propuesto se puede considerar que un proceso está documentado o pueda existir alguna información escrita sobre el mismo desde el nivel 2, solo los componentes que logren cubrir el nivel 3 se pueden considerar adecuadamente documentados, ya que

cumplen con una estructura mínima, y su documentación obedece a un proceso y responde a necesidades identificadas por la organización.

Marco de referencia
COSO

Committee of Sponsoring Organizations of the Treadway Commission (COSO): es una iniciativa de varios organismos para la mejora de control interno dentro de las organizaciones. Dentro de COSO el termino de Control interno, está definido como un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y normas (aplicables dentro del entorno de la entidad).

De acuerdo con el marco COSO el control interno consta de cinco componentes relacionados entre sí; éstos derivarán de la manera en que la dirección dirija la unidad y estarán integrados en el **proceso de dirección**.

Los componentes serán los mismos para todas las organizaciones (públicas o privadas) y dependerá del tamaño de la misma la implantación de cada uno de ellos.

Los componentes son:

1. Ambiente de Control.
2. Evaluación de Riesgos.
3. Actividades de Control.
4. Información y Comunicación.
5. Supervisión y Monitoreo.

Ambiente de Control:

El ambiente de control es la base de la pirámide de Control Interno, aportando disciplina a la estructura. En él se apoyan los otros componentes, por lo que es fundamental para concretar los cimientos de un eficaz y eficiente sistema de Control Interno. Marca la pauta del funcionamiento de la unidad e influye en la concientización de sus funcionarios.

Los factores a considerar dentro del entorno de control serán: la integridad y los valores éticos, la capacidad de los funcionarios de la unidad, el estilo de dirección y gestión, la asignación de autoridad y responsabilidad, la estructura organizacional y, las políticas y prácticas de personal utilizadas.

Evaluación de riesgos:

Cada unidad se enfrenta a diversos riesgos internos y externos que deben ser evaluados. Una condición previa a la evaluación de riesgo es la identificación de los objetivos a los distintos niveles, los cuales deberán estar vinculados entre sí.

La evaluación de riesgos consiste en: La identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo deben ser gestionados. A su vez, dados los cambios permanentes del entorno, es necesario que la unidad disponga de mecanismos para identificar y afrontar los riesgos asociados al cambio.

En la evaluación se deberá analizar que los objetivos de área hayan sido apropiadamente definidos, que los mismos sean consistentes con los objetivos institucionales, que sean

oportunamente comunicados, detectados y analizados adecuadamente (los riesgos) y, que se los haya clasificado de acuerdo a la relevancia y probabilidad de ocurrencia.

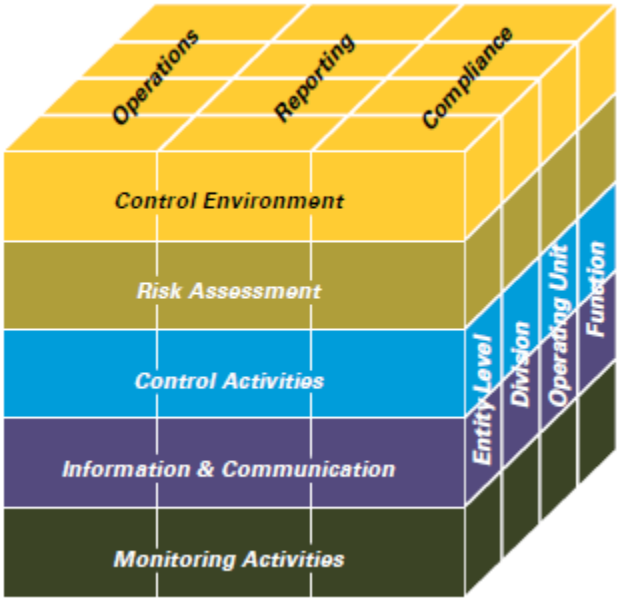
Actividades de Control:
Las actividades de control son: Las políticas, procedimientos, técnicas, prácticas y mecanismos que permiten a la dirección administrar (mitigar) los riesgos identificados durante el proceso de evaluación de riesgos y asegurar que se llevan a cabo los lineamientos establecidos por ella.
Las actividades de control se ejecutan en todos los niveles de la Unidad y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos, de acuerdo a lo señalado en el punto anterior.
En la evaluación del sistema de control interno no solo debe considerarse si fueron establecidas las actividades relevantes para los riesgos identificados, sino también si las mismas son aplicadas en la realidad y si los resultados obtenidos fueron los esperados.

Información y Comunicación:
Se debe identificar, recopilar y propagar la información pertinente en tiempo y forma que permitan cumplir a cada funcionario con sus responsabilidades a cargo. Debe existir una comunicación eficaz -en un sentido amplio- que fluya en todas direcciones a través de todos los ámbitos de la Unidad, de forma descendente como ascendente.

La dirección debe comunicar en forma clara las responsabilidades de cada funcionario dentro del sistema de control interno implementado. Los funcionarios tienen que comprender cuál es su papel en el sistema de control interno y, como las actividades individuales están relacionadas con el trabajo del resto de los actores

Supervisión y Monitoreo:

Los sistemas de control interno requieren -principalmente- de Supervisión, es decir, un proceso que verifique la vigencia del sistema de control a lo largo del tiempo. Esto se logra mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas.



CE 29/14

La circular básica jurídica 29 de 2014 fue expedida para contribuir a la implementación de estándares internacionales en las entidades vigiladas por la Superintendencia financiera de Colombia, especialmente en lo referente a las recomendaciones de política regulatoria de la Organización para la Cooperación y el Desarrollo Económico (OECD - por sus siglas en inglés).

La CE 29/14 está compuesta por 3 partes: Parte 1: "Instrucciones generales aplicables a las entidades vigiladas", Parte 2: "Mercado intermediado" y Parte 3: "Mercado des intermediado", para efectos de este trabajo nos enfocaremos en la parte 1: que contiene las disposiciones aplicables de forma transversal a todas las entidades vigiladas por esta Superintendencia.

A su vez la parte 1 se encuentra dividida en cuatro (4) títulos: Título I: "Aspectos generales", Título II: "Prestación de los Servicios Financieros", Título III: "Competencias y Protección del consumidor Financiero" y el Titulo IV: "Deberes y Responsabilidades", dentro del marco de este trabajo nos enfocaremos sobre el título I, y específicamente sobre su Capítulo IV el cual trata sobre el sistema de control interno.

Finalmente la CE 29 /14 Parte 1, Título I, Capitulo IV habla sobre el sistema de control interno y define temas como: el ámbito de aplicación, objetivos del sistema de control interno (SCI), principios del SCI, elementos del SCI, áreas específicas del dentro del sistema de control interno (gestión contable y TI), Responsables dentro del SCI, Documentos mínimos para sustentar la implementación de un SCI, este trabajo se enfocará específicamente en el área de control interno relacionada con TI, dentro de la cual se establecen lineamientos o requerimientos para:

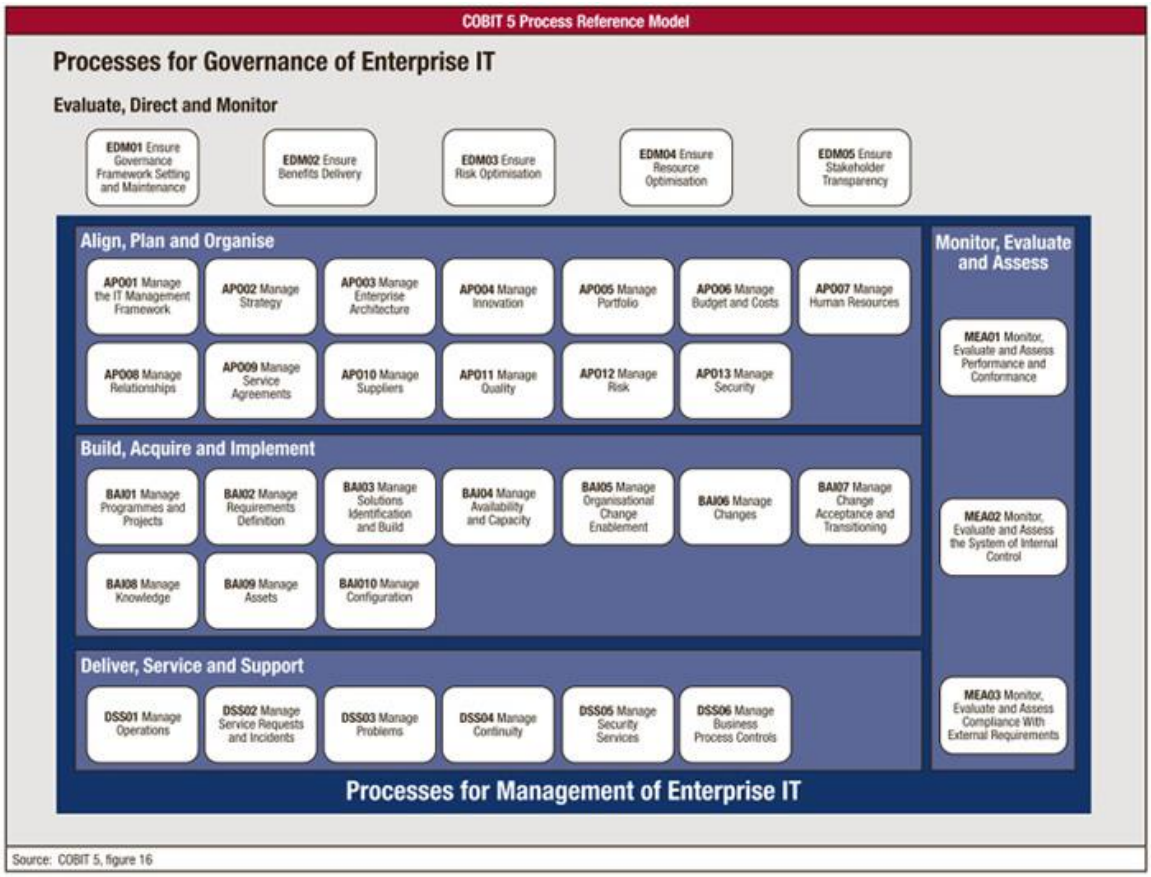
- Plan estratégico de tecnología.
- Infraestructura de tecnología.

- Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
- Administración de proyectos de sistemas.
- Administración de la calidad.
- Adquisición de tecnología.
- Adquisición y mantenimiento de software de aplicación.
- Instalación y acreditación de sistemas.
- Administración de cambios.
- Administración de servicios con terceros.
- Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
- Continuidad del negocio.
- Seguridad de los sistemas.
- Educación y entrenamiento de usuarios.
- Administración de los datos.
- Administración de instalaciones.
- Administración de operaciones de tecnología.
- Documentación.

COBIT

Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenida por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute), contiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

COBIT 5 plantea 5 procesos los cuales están distribuidos en:
EDM: Evaluate Direct and Monitor: el dominio EDM, está conformado por 5 objetivos de control, los cuales se enfocan sobre el Gobierno de TI y su alineamiento con el gobierno corporativo
APO: Allign Plan and Organise: el dominio APO, está conformado ´por 13 objetivos de control, los cuales se enfocan sobre la planeación de TI
BAI: Build Adquire and Implement: El dominio BAI, está conformado por 10 objetivos de control los cuales se enfocan en la adquisición e implementación
DSS: Deliver Service and Support: El dominio DSS el cual cuenta con 6 objetivos de control y se concentran en la entrega de servicio.
MEA: Monitor Evaluate and Assess: El dominio MEA el cual se conforma por 3 objetivos de control y se enfoca en el monitoreo

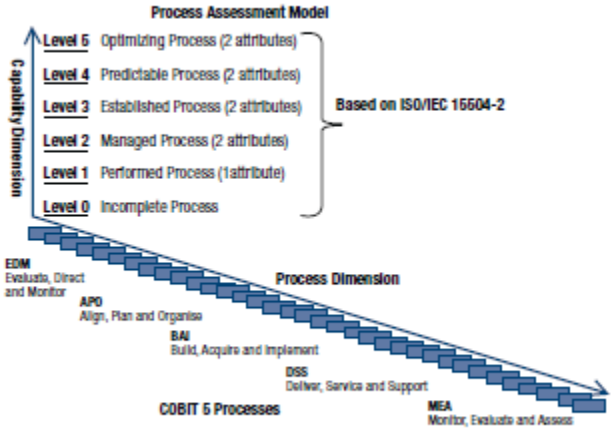


PAM

Process Assesment Model (PAM) por sus siglas en ingles es un modelo de medición de madurez creado por ISACA, inicialmente planteado para la medición de la madures de implementaciones de COBIT 4.1, sin embargo el modelo puede ser aplicado para la medición de madurez de diferentes modelos.

PAM está basado en la ISO 15504 y presenta una escala de medición de 0 a 5, diferenciándose en este aspecto de otros modelos aplicables como el CMMI, actualmente COBIT ha publicado la guía: “Process Assessment Model (PAM): Using COBIT® 5” en el cual se plantea el PAM como un modelo bidimensional de medición de capacidad, en el cual se expresan las dimensiones del proceso (para este caso COBIT 5) y en la otra dimensión el modelo de capacidad.

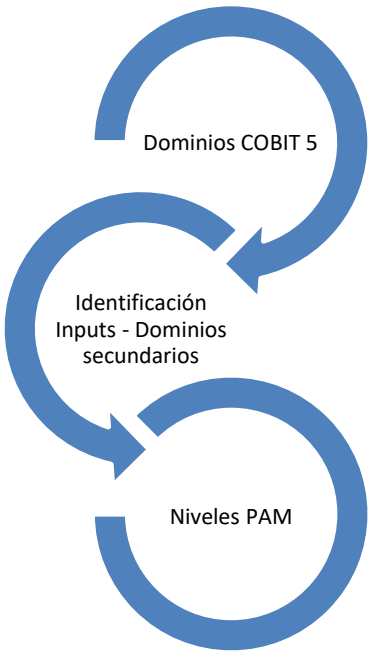
Figure 2—Overview of the Process Assessment Model (PAM)



Source: This figure is adapted from ISO/IEC 15504-2:2003 with the permission of ISO at *www.iso.org*. Copyright remains with ISO.

Capítulo 4
Modelo

El modelo presentado para la medición estandarizada de los apartes de TI de la CE29 se realizó mediante la identificación de los eleméntenos de la norma y un mapeo con COSO y un doble mapeo de los Dominios del COBIT como resultado del análisis se identificó que algunos de los componentes de la norma pueden y deben ser evaluados en conjunto dado que sus objetivos individuales son cubiertos por dominios de COBIT más amplios:



Plan Estratégico

Objetivo:

Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio y logrando ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si se incluyen los siguientes ítems en la evaluación del plan de TI y estos pueden ser demostrados:
    - Análisis de cómo soporta la tecnología los objetivos del negocio.
    - Evaluación de la tecnología actual.
    - Estudios de mercado y factibilidad de alternativas tecnológicas que respondan a las necesidades de la entidad.
    - Planes operacionales estableciendo metas claras y concretas

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
APO02.01 Comprender la dirección de la empresa.	Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo

	a ella. Esta actividad es crítica para la alineación con los objetivos de gobierno
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.	Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos.
APO02.03 Definir el objetivo de las capacidades de TI.	Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.
APO02.04 Realizar un análisis de diferencias.	Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.
APO02.05 Definir el plan estratégico y la hoja de ruta.	Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.
APO02.06 Comunicar la estrategia y la dirección de TI.	Crear conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa.

APO04.03 Supervisar y explorar el entorno tecnológico.	Realizar una supervisión sistemática y un escaneo del entorno externo a la empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, realizando la estrategia corporativa, optimizando costes, evitando la obsolescencia y catalizando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias que permitan analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial.
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de las nuevas tecnologías y la innovación.
APO04.05 Recomendar iniciativas apropiadas adicionales.	Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**

APO02.01 Comprender la dirección de la empresa.	EDM04.01 - Principios guía para la asignación de recursos y capacidades APO04.02 - Oportunidades de innovación vinculadas con los motivadores de la industria Externo - DOFA
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.	APO06.05 - Oportunidades Optimización de Costes APO08.05 - Definición Proyectos de Mejoras Potenciales APO09.01 - Diferencias en los servicios de TI para el negocio APO09.04 - Planes de acción de mejora y recomendaciones APO12.01 - Nuevos problemas y factores de riesgo APO12.02 - Resultado del análisis de riesgo APO12.03 - Perfil de riesgo agregado incluyendo estado sobre las acciones de gestión de riesgo APO12.05 - Propuestas de proyectos para reducción de riesgos BAI04.03 - Planes de rendimiento y capacidades - Mejoras Priorizadas BAI04.05 - Acciones Correctivas BAI09.01 - Revisión de los resultados de ajustes objetivos BAI09.04 - oportunidades para reducir los costes de los activos o incrementar su valor - revisión de los resultados de la optimización de costes
APO02.03 Definir el objetivo de las capacidades de TI.	APO04.05 - análisis de iniciativas rechazadas - Resultados y recomendaciones de la iniciativa de pruebas de conceptos
APO02.04 Realizar un análisis de diferencias.	EDM02.01 - Evaluación de alineación estratégica APO04.06 - Evaluaciones sobre el uso de enfoques innovadores APO05.02 - Expectativas sobre el retorno de inversión

	BAI01.05 - Resultados del programa de supervisión de consecución de objetivos BAI01.06 - Revisión de los resultados de cambios de fase (stagegate) BAI01.13 - Resultados de la revisión post-implementación
APO02.05 Definir el plan estratégico y la hoja de ruta.	EDM04.01 - Plan de recursos aprobado EDM04.03 - realimentación sobre la asignación y eficacia de los recursos y capacidades • Acciones correctivas para gestionar las desviaciones en la gestión de recursos APO03.01 • Alcance definido de la arquitectura • Caso de negocio conceptual de la arquitectura y propuesta de valor APO03.02 - Modelo de arquitectura de la información APO03.03 • Arquitecturas de transición • Implementación a alto nivel y estrategias de migración APO05.01 - Realimentación sobre las estrategias y objetivos APO05.02 - Opciones de financiación APO06.02 - Asignaciones presupuestarias APO06.03 • Plan y presupuesto de TI • Comunicación del presupuesto APO13.02 - Casos de negocio de la seguridad de la información BAI09.05 - Plan de acción para ajustar las cantidades y asignación de licencias DSS04.02 - Aprobación de las opciones estratégicas
APO02.06 Comunicar la estrategia y la dirección de TI.	EDM04.02 - Comunicación de las estrategias de los recursos

APO04.03 Supervisar y explorar el entorno tecnológico.	Externo - Tecnologías Emergentes
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	N/A
APO04.05 Recomendar iniciativas apropiadas adicionales.	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI
- Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados
- Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
- Número de interrupciones del negocio debidas a incidentes en el servicio de TI
- Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados
- Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
- Nivel de concienciación y comprensión de las posibilidades de innovación de TI del negocio ejecutivo
- Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas de la innovación TI
- Número de iniciativas aprobadas resultantes de ideas innovadoras de TI

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el

proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	**Ejecutivos de negocio**	**Director de Informática/Sistemas (CIO)**	**Jefe de Arquitectura del Negocio**	**Jefe de Desarrollo**	**Jefe de Operaciones TI**	**Jefe de Administración TI**	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de**
APO02.01 Comprender la dirección de la empresa.	A	R	C	R	R		R	R	R
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.	R	A	R	R	R	C	C	C	C
APO02.03 Definir el objetivo de las capacidades de TI.	C	R	C	C	C	C	C	C	C
APO02.04 Realizar un análisis de diferencias.	R	A	R	R	R	R	R	R	C
APO02.05 Definir el plan	C	A	C	C	C	C	C	C	C

Restratégico y la hoja de ruta.									
APO02.06 Comunicar la estrategia y la dirección de TI.	R	R	I	I	I	I	I	I	I
APO04.03 Supervisar y explorar el entorno tecnológico.		A	R	R	R		R	R	
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	C	A	R	R	R		R	R	
APO04.05 Recomendar iniciativas apropiadas adicionales.	C	A	R	R	R		R	R	

Infraestructura de TI

Objetivo:

Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI Representando a los diferentes módulos que componen la empresa y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del diseño de la arquitectura de TI su cuenta con infraestructura de TI para soportar el negocio y se puede demostrar su correlación con los objetivos empresariales.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
APO03.01 Desarrollar la visión de la arquitectura de empresa.	La visión de la arquitectura proporciona una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al promotor la herramienta clave para vender los beneficios de la capacidad propuesta a las partes interesadas de la empresa. La visión de la arquitectura de información describe como nuevas capacidades permitirán alcanzar las metas de la empresa y

	los objetivos estratégicos y considera las preocupaciones de las partes interesadas en su implementación. Este componente ahonda en la alineación entre gobierno y gestión y asegura entre otras cosas, que los datos, aplicaciones y demás capas de la arquitectura responden a los objetivos planteados.
APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología. Este componente es su análisis de la capa de tecnología impacta directamente al componente de infraestructura de TI solicitado por la CE 29
APO03.03 Seleccionar las oportunidades y las soluciones.	Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolos a ambos en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que estas iniciativas sean parte del cambio general en la empresa. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar las oportunidades, soluciones y todas las restricciones de la implementación.
APO03.04 Definir la implementación de la arquitectura.	Crear un plan de implementación y de migración viable acorde con la cartera de proyectos y programas. Asegurarse que el plan está coordinado de cerca para asegurar que se proporciona el valor y que se disponen de los recursos necesarios para finalizar los trabajos.
APO03.05 Proveer los servicios de arquitectura empresarial.	La provisión de los servicios de arquitectura empresarial incluye las guías y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación de los valores aportados por la arquitectura y la supervisión del cumplimiento. Se recomienda alinear este proceso con las buenas prácticas de TOGAF

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
APO03.01 Desarrollar la visión de la arquitectura de empresa.	EDM04.01 - Principios directrices de la arquitectura de empresa APO02.05 - Hoja de ruta estratégica Externo - Estrategia empresarial
APO03.02 Definir la arquitectura de referencia.	APO01.01 - Directrices operativas corporativas - Definición de la estructura de la organización y funciones APO01.05 – Emplazamiento operacional de la función TI - Evaluación de las diferentes opciones para la organización de TI APO01.06 - Guía para la clasificación de los datos Externo - Estrategia empresarial
APO03.03 Seleccionar las oportunidades y las soluciones.	APO02.03 - Cambios propuestos en la arquitectura de empresa Externo – Estrategias empresariales - Motivadores de la empresa.

APO03.04 Definir la implementación de la arquitectura.	N/A
APO03.05 Proveer los servicios de arquitectura empresarial.	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI
- Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados
- Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
- Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos
- Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas
- Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada
- Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes
- Tendencia de los resultados de las evaluaciones
- Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:

Matriz Raci Genérica

Actividad	Ejecutivos de negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
APO03.01 Desarrollar la visión de la arquitectura de empresa.	A	R	C	C	C	C		C	
APO03.02 Definir la arquitectura de referencia.	A	R	C	C	C	C		C	
APO03.03 Seleccionar las oportunidades y las soluciones.	A	R	C	C	C	C		C	
APO03.04 Definir la implementación de la arquitectura.	C	A/R	C	C	C	C		C	
APO03.05 Proveer los servicios de arquitectura empresarial.	C	A/R	C	C	C	C		C	

Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.

Objetivo:

Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general, asegurando que la empresa cumple con todos los requisitos externos que le sean aplicables.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del mismo se puede evidenciar que la organización adelanta procesos para garantizar el cumplimiento de derechos de autor, privacidad y comercio electrónico en los casos en los cuales aplique.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
MEA03.01 Identificar requisitos externos de cumplimiento.	Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.
MEA03.02 Optimizar la respuesta a requisitos externos.	Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores

	prácticas pueden adoptarse y adaptarse. Este componente es su análisis de la capa de tecnología impacta directamente al componente de infraestructura de TI solicitado por la CE 29
MEA03.03 Confirmar el cumplimiento de requisitos externos.	Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.
MEA03.04 Obtener garantía del cumplimiento de requisitos externos.	Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
MEA03.01 Identificar requisitos externos de cumplimiento.	Externo - Requisitos de cumplimiento legal y regulatorio

MEA03.02 Optimizar la respuesta a requisitos externos.	N/A
MEA03.03 Confirmar el cumplimiento de requisitos externos.	BAI05.06 - Resultados auditorías de cumplimiento BAI09.05 - Resultados de auditorías de licencias instaladas BAI10.05 - Desviaciones de licencias DSS01.04 - Informes de pólizas de seguros
MEA03.04 Obtener garantía del cumplimiento de requisitos externos.	EDM05.02 - Reglas de validación y aprobación de informes obligatorios. EDM05.03 - Valoración de la efectividad de las evaluaciones.

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación
- Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos
- Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI
- Cobertura de las evaluaciones de conformidad
- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos
- Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
- Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI
- Frecuencia de actualización del perfil de riesgo

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos

Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Ejecutivos de negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
MEA03.01 - Identificar requisitos externos de cumplimiento.	A	R						R	
MEA03.02 - Optimizar la respuesta a requisitos externos.	A	R	R	R	R	R	R	R	R
MEA03.03 - Confirmar el cumplimiento de requisitos externos.	R	R	C	C	C	C	C	R	R
MEA03.04 - Obtener garantía de cumplimiento de requisitos externos.	C	R	C	C	C	C	C	C	C

Administración de proyectos de sistemas

Objetivo:

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, mediante la aplicación de técnicas de gestión a 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.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del mismo se puede evidenciar que la organización adelanta procesos para gestionar los proyectos, programas o portafolios de TI y que estos obedecen a objetivos claros de negocio.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
BAI01.01- Mantener un enfoque estándar para la gestión de programas y proyectos.	Mantener un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno y de gestión y actividades de gestión de la entrega, enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costes, cronograma y calidad) para el negocio de una forma consistente.

BAI01.02 Iniciar un programa.	Iniciar un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar.
BAIO01.03 Gestionar el compromiso de las partes interesadas.	Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna, que llegue a todos las partes interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas.
BAI01.04 Desarrollar y mantener el plan de programa.	Formular un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Mantener y actualizar el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.
BAI01.05 Lanzar y ejecutar el programa.	Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. De acuerdo con los criterios de revisión de lanzamiento o cambio de fase (stage-gate), preparar los cambios de fase, las revisiones de las iteraciones o versiones para informar del progreso del programa y ser capaz de establecer los fundamentos para la financiación de la siguiente etapa después de la revisión del lanzamiento o de cambio de fase (stage-gate).
BAI01.06 Supervisar, controlar e informar de los resultados del programa.	Supervisar y controlar el rendimiento del programa (entrega de soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Informar del

	rendimiento al comité estratégico del programa y a los patrocinadores.
BAI01.07 Lanzar e iniciar proyectos dentro de un programa.	Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común o el alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones de TI. La definición debería estar formalmente aprobada por el patrocinador del programa y del proyecto.
BAI01.08 Planificar proyectos.	Establecer y mantener un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI), para guiar la ejecución del proyecto y controlarlo durante toda su vida. El alcance de los proyectos debería estar claramente definido y vinculado claramente a la construcción o aumento de la capacidad del negocio.
BAI01.09 Gestionar la calidad de los programas y proyectos.	Preparar y ejecutar un plan y procesos y prácticas de gestión de la calidad, alineadas al SGC que describe el enfoque de calidad del programa y el proyecto y cómo será implementado. El plan debería ser formalmente revisado y acordado por todas las partes afectadas y, después, incorporado en los planes integrados del programa y los proyectos.
BAI01.10 Gestionar el riesgo de los programas y proyectos.	Eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser establecidos y registrados en un único punto.
BAI01.11 Supervisar y controlar proyectos.	Medir el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el coste y los riesgos. Evaluar el impacto de las desviaciones en el proyecto y el programa general e informar los resultados a las partes interesadas clave.

BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.	Gestionar los paquetes de trabajo mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinado los recursos de negocio y de TI adecuados.
BAI01.13 Cerrar un proyecto o iteración.	Solicitar a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valor planeados. Identificar y comunicar cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, identificar y documentar las lecciones aprendidas para futuros proyectos, versiones, iteraciones y programas.
BAI01.14 Cerrar un programa.	Eliminar el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor establecidos para el programa.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
BAI01.01- Mantener un enfoque estándar para la	EDM02.02 - Requisitos para revisiones de cambio de estado (stage-gate)

gestión de programas y proyectos.	EDM02.03 - Acciones para mejorar la entrega de valor APO03.04 - • Requisitos de gobierno de la arquitectura • Descripciones en fase de implementación APO05.05 - Portafolios de programas, servicios y activos actualizados APO10.04 - Riesgo de entrega del proveedor identificado
BAI01.02 - Iniciar un programa.	APO03.04 - • Requisitos de gobierno de la arquitectura • Descripciones en fase de implementación APO05.03 - Caso de negocio del programa APO07.03 - Matriz de habilidades y competencias BAI05.02 - Visión y objetivos comunes
BAI01.03 - Gestionar el compromiso de las partes interesadas.	N/A
BAI01.04 Desarrollar y mantener el plan de programa.	APO05.03 - Programas seleccionados con hitos de ROI APO07.03 - Matriz de habilidades y competencias APO07.05 - Inventario de recursos humanos de TI y del negocio BAI05.02 - Equipo y roles para la implementación BAI05.03 - Plan de comunicación de la visión BAI05.04 - Identificación de logros rápidos (quick wins) BAI07.03 - Plan de pruebas de aceptación aprobado BAI07.05 - Aceptación y pase a producción aprobados
BAI01.05 - Lanzar y ejecutar el programa.	BAI05.03 - Comunicaciones de la visión
BAI01.06 - Supervisar, controlar e informar de los resultados del programa.	EDM02.03 - Realimentación sobre el rendimiento del portafolio y del programa APO05.02 - Expectativas del retorno de la inversión APO05.03 – Evaluaciones de los casos de negocio

	APO05.04 - Informes del desempeño del portafolio de inversiones APO05.06 - • Acciones correctivas para mejorar la realización de beneficios.• Resultados de beneficios y comunicaciones relacionadas APO07.05 - • Registro de uso de recursos. • Análisis de escasez de recursos BAI05.04 - Comunicación de beneficios BAI06.03 - Informes de estado de solicitudes de cambios BAI07.05 - Evaluación de los resultados de aceptación
BAI01.07 - Lanzar e iniciar proyectos dentro de un programa.	N/A
BAI01.08 - Planificar proyectos.	BAI07.03 - Plan aprobado de aceptación de pruebas
BAI01.09 - Gestionar la calidad de los programas y proyectos.	APO11.01 - Plan de gestión de la calidad APO11.03 - Requisitos de cliente para la gestión de la calidad
BAI01.10 - Gestionar el riesgo de los programas y proyectos.	APO12.02 - Resultados del análisis de riesgo BAI02.03 - • Acciones de mitigación de riesgos. • Registro de requisitos de riesgos Externo - Marco de referencia de ERM
BAI01.11 - Supervisar y controlar proyectos.	N/A
BAI01.12 - Gestionar los recursos y los paquetes de trabajo del proyecto.	N/A
BAI01.13 - Cerrar un proyecto o iteración.	BAI07.08 - • Plan de acciones de remediación • Informe de revisión post-implementación
BAI01.14 - Cerrar un programa.	BAI07.08 - • Plan de acciones de remediación • Informe de revisión post-implementación

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje de partes interesadas efectivamente comprometidas
- Nivel de satisfacción con la involucración de las partes interesadas
- Porcentaje de grupos de interés que aprueban las necesidades de la empresa, el alcance, los resultados esperados y el nivel de riesgo del proyecto
- Porcentaje de proyectos emprendidos sin casos de negocio aprobados
- Porcentaje de actividades alineadas al alcance y a los resultados esperados
- Porcentaje de programas activos emprendidos sin mapas de valor de programa actualizados y válidos
- Frecuencia de revisiones de estado
- Porcentaje de desviaciones del plan de referencia
- Porcentaje de partes interesadas que firman las revisiones de cambio de estado (stage-gate) de los programas activos
- Número de incidentes con recursos (por ejemplo, habilidades, capacidad)
- Porcentaje de beneficios esperados que se han alcanzado
- Porcentaje de resultados aceptados al primer intento
- Nivel de satisfacción expresada por las partes interesadas en las revisiones de cierre de proyectos

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Ejecutivos de negocio	Director de Informática/Sistemas (CIO)	PMO	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
BAI01.01- Mantener un enfoque estándar para la gestión de programas y proyectos.	R	R	A	C	C	C	C	C	C
BAI01.02 - Iniciar un programa.	A	C	R	C	C	C	C	C	C
BAI01.03 - Gestionar el compromiso de las partes interesadas.	R	R	A	C	C	C	C	C	C
BAI01.04 Desarrollar y mantener el plan de programa.	A	C	R	C	C	C	C	C	C
BAI01.05 - Lanzar y ejecutar el programa.	A	R	R	C	C	C	C	C	C
BAI01.06 - Supervisar, controlar e informar de los resultados del programa.	A	R	R	C	C	C	C	C	C
BAI01.07 - Lanzar e iniciar proyectos dentro de un programa.	R	C	A	C	C	C	C	C	C
BAI01.08 - Planificar proyectos.		R/C	A	C	C	C	C	C	C
BAI01.09 - Gestionar la calidad de los programas y proyectos.	R	C	A	C	C	C	C	C	C

BAI01.10 - Gestionar el riesgo de los programas y proyectos.	R	C	A	C	C	C	C	C	C
BAI01.11 - Supervisar y controlar proyectos.	I	C	A/R	C	C	C	C	C	C
BAI01.12 - Gestionar los recursos y los paquetes de trabajo del proyecto.		C	A/R	C	C	C	C	C	C
BAI01.13 - Cerrar un proyecto o iteración.	C	C	A/R	C	C	C	C	C	C
BAI01.14 - Cerrar un programa.	A	R	R	C	C	C	C	C	C

Administración de la calidad.

Objetivo:

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, mediante la definición y comunicación de 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.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del mismo se puede evidenciar al menos los siguientes elementos:
    - Programas para establecer una cultura de calidad de la tecnología en toda la entidad.
    - Planes concretos de calidad de la tecnología.
    - Responsables por el aseguramiento de la calidad.
    - Prácticas de control de calidad.
    - Metodología para el ciclo de vida de desarrollo de sistemas.
    - Metodología de prueba y documentación de programas y sistemas.
    - Diseño de informes de aseguramiento de la calidad.
    - Capacitación de usuarios finales y del personal de aseguramiento de la calidad.
    - Desarrollo de una base de conocimiento de aseguramiento de la calidad.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**

APO11.01 - Establecer un sistema de gestión de la calidad (SGC).	Establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo.
APO11.02 - Definir y gestionar los estándares, procesos y prácticas de calidad.	Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC. Este debería estar en consonancia con los requisitos del marco de control TI. Considerar la posibilidad de certificar los procesos, las unidades de la organización, los productos o los servicios clave.
APO11.03 - Enfocar la gestión de la calidad en los clientes.	Enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de calidad.
APO11.04 - Supervisar y hacer controles y revisiones de calidad.	Supervisar la calidad de los procesos y servicios de forma permanente como se defina en el SGC. Definir, planificar y aplicar medidas para supervisar la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC. La información recogida debería ser utilizada por los propietarios de los procesos para mejorar la calidad.
APO11.05 - Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	Incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollos de soluciones y los servicios ofrecidos.
APO11.06 - Mantener una mejora continua	Mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Esto debería incluir la necesidad y los beneficios de una mejora continua. Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de mejora continua de la calidad.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
APO11.01 - Establecer un sistema de gestión de la calidad (SGC).	Fuera del Ámbito de COBIT - Sistema empresarial de gestión de la calidad
APO11.02 - Definir y gestionar los estándares, procesos y prácticas de calidad.	BAI02.04 - Revisiones de la calidad aprobadas Fuera del Ámbito de COBIT - • Buenas prácticas de la industria • Certificaciones de calidad disponibles
APO11.03 - Enfocar la gestión de la calidad en los clientes.	Fuera del Ámbito de COBIT - Requisitos de calidad del negocio y los clientes
APO11.04 - Supervisar y hacer controles y revisiones de calidad.	BAI03.6 - • Resultados de las revisiones de calidad, excepciones y correcciones • Plan de aseguramiento de la calidad DSS02.07 - • Estado de solicitudes de cambio e informes de tendencias • Situación de los incidentes e informes de tendencias
APO11.05 - Integrar la gestión de la calidad en la implementación de	N/A

soluciones y la entrega de servicios.	
APO11.06 - Mantener una mejora continua	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje de inversiones de TI en los que la realización del beneficio se monitoriza a través del ciclo de vida económico completo.
- Porcentaje de servicios TI en los que se realizan los beneficios esperados.
- Porcentaje de las inversiones en TI donde los beneficios demandados son alcanzados o excedidos.
- Número de interrupciones del negocio debidas a incidentes en el servicio de TI
- Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados
- Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
- Número de programas/proyectos ejecutados en plazo y en presupuesto
- Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
- Número de programas que necesitan ser revisados significativamente debido a defectos de calidad
- Coste del mantenimiento de aplicaciones respecto al coste total de TI

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Ejecutivos de negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitlectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
APO11.01 - Establecer un sistema de gestión de la calidad (SGC).	A	R	I	I	I	I	I	I	I
APO11.02 - Definir y gestionar los estándares, procesos y prácticas de calidad.		A	I	I	I	I	I	I	I
APO11.03 - Enfocar la gestión de la calidad en los clientes.		R	I	I	I	I	I	I	I
APO11.04 - Supervisar y hacer controles y revisiones de calidad.		A	I	I	I	I	I	I	I
APO11.05 - Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.		A	R	R	R	R	I	I	I

APO11.06 - Mantener una mejora continua		A	R	R	R	R	R	R	R

Adquisición de tecnología, Adquisición y mantenimiento de software de aplicación e

Instalación y acreditación de sistemas.

Objetivo:

Establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales mediante el establecimiento y mantenimiento de soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación (tomando los lineamientos establecidos el proceso de compras corporativo) y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del mismo se puede evidenciar un procedimiento para la adquisición, construcción y/o

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
BAI03.01 - Diseñar soluciones de alto nivel.	Desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas. Asegurar el alineamiento con la estrategia TI y la arquitectura empresarial. Revalorar y actualizar los diseños cuando sucedan cuestiones significativas durante las fases de diseño detallado o de construcción o según la solución evolucione. Asegurar que las partes interesadas

	participen activamente en el diseño y en la aprobación de cada versión.
BAI03.02 - Diseñar los componentes detallados de la solución	Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asegurar que el diseño detallado incluye ANSs y OLAs internos y externos
BAI03.03 - Desarrollar los componentes de la solución	Desarrollar los componentes de la solución progresivamente conforme el diseño detallado siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación. Asegurar que se consideran todos los requerimientos de control en los procesos de negocio, soportando las aplicaciones TI y servicios de infraestructura, productos tecnológicos y servicios y proveedores/suministradores.
BAI03.04 - Obtener los componentes de la solución	Obtener los componentes de la solución sobre la base del plan de adquisiciones y conforme a los requerimientos y diseños detallados, principios de arquitectura y estándares y en los procedimientos generales contractuales y de adquisiciones de la empresa, requerimientos de calidad (QA) y aprobación de estándares. Asegurar que todos los requerimientos legales y contractuales son identificados y cumplidos por el proveedor.
BAI03.05 - Construir soluciones.	Instalar y configurar las soluciones e integrarlas con las actividades de los procesos de negocio. Implementar controles, medidas de seguridad y ‘auditabilidad’ durante la configuración y durante la integración del hardware e infraestructura del software para proteger los recursos y asegurar la disponibilidad e integridad de los datos. Actualizar el catálogo de servicios para reflejar la nueva situación.
BAI03.06 - Realizar controles de calidad.	Desarrollar y ejecutar un plan de calidad (QA) alineado con el SGC para obtener la calidad especificada en la definición

	de los requerimientos y de acuerdo a las políticas y procedimientos de calidad de la empresa.
BAI03.07 - Preparar pruebas de la solución	Establecer un plan de pruebas y entornos necesarios para probar los componentes individualmente y de la solución integrada incluyendo los procesos de negocio y servicios, aplicaciones e infraestructura que los soportan.
BAI03.08 - Ejecutar pruebas de la solución	Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, en concordancia con el plan de pruebas y con las prácticas de desarrollo en el entono apropiado. Hacer partícipes a los dueños de los procesos de negocio y usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores e incidentes identificados durante las pruebas.
BAI03.09 - Gestionar cambios a los requerimientos.	Hacer seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.
BAI03.10 - Mantener soluciones.	Desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura. Incluir revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales.
BAI03.11 - Definir los servicios TI y mantener el catálogo de servicios.	Definir y acordar nuevos servicios TI o cambios y opciones de nivel de servicio. Documentar nuevas definiciones o cambios en los servicios y opciones de nivel de servicio que serán actualizadas en el catálogo de servicios.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.

- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
BAI03.01 - Diseñar soluciones de alto nivel.	APO03.01 - Principios de arquitectura APO03.02 - Descripción de los dominios de referencia y la definición de arquitectura APO04.03 - Análisis de investigación de las posibilidades de innovación APO04.04 - Evaluación de las ideas de innovación BAI02.01 - • Confirmar los criterios de aceptación por las partes interesadas • Repositorio de la definición de requerimientos BAI02.02 - Plan de alto nivel de adquisiciones/desarrollo
BAI03.02 - Diseñar los componentes detallados de la solución	APO03.01 - Principios de arquitectura APO03.02 - Descripción de los dominios de referencia y la definición de arquitectura • Modelo de arquitectura de la información APO03.05 - Guía de desarrollo de la solución APO04.06 - Evaluaciones de utilización de aproximaciones innovadoras BAI02.01 - • Confirmar los criterios de aceptación por parte de las partes interesadas • Repositorio de definición de los requerimientos BAI02.02 - Informe de estudio de viabilidad BAI02.03 - • Acciones de mitigación de riesgos • Registro de riesgos de requerimientos

	BAI02.04 - Aprobación del patrocinador de los requerimientos y soluciones propuestas
BAI03.03 - Desarrollar los componentes de la solución	BAI02.02 - Informe de estudio de viabilidad BAI02.04 - Aprobaciones de los patrocinadores de los requerimientos y soluciones propuestas
BAI03.04 - Obtener los componentes de la solución	BAI02.04 - Aprobaciones de los patrocinadores de los requerimientos y soluciones propuestas
BAI03.05 - Construir soluciones.	N/A
BAI03.06 - Realizar controles de calidad.	APO11.01 - Resultados de las revisiones de efectividad del SGC BAI01.09 - Plan de gestión de calidad
BAI03.07 - Preparar pruebas de la solución	N/A
BAI03.08 - Ejecutar pruebas de la solución	APO04.05 - Análisis de las iniciativas rechazadas
BAI03.09 - Gestionar cambios a los requerimientos.	APO04.05 - Resultados y recomendaciones de las iniciativas de pruebas de concepto BAI02.01 - Registro de peticiones de cambio de los requerimientos
BAI03.10 - Mantener soluciones.	N/A
BAI03.11 - Definir los servicios TI y mantener el catálogo de servicios.	EDM04.01 - Directrices para la asignación de recursos y capacidades APO02.04 - • Valorar beneficios para el entorno objetivo • Cambios requeridos para ajustar la capacidad objetivo APO06.02 - Asignaciones de presupuesto APO06.03 - • Comunicación del presupuesto • Plan y presupuesto TI

	APO08.05 - Definición de mejoras potenciales de proyectos BAI10.02 - Configuración de la línea de referencia BAI10.03 - Aprobación de cambios a la línea de referencia BAI10.04 - Informes del estado de la configuración

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Número de interrupciones del negocio debidas a incidentes en el servicio de TI
- Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados
- Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Propietarios de los procesos de negocios	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de

BAI03.01 - Diseñar soluciones de alto nivel.	R	A/R	C	R	C	C	C	C	C
BAI03.02 - Diseñar los componentes detallados de la solución	R	A/R	C	R	C	C	C	C	C
BAI03.03 - Desarrollar los componentes de la solución	R	A/R	C	R	C	C	C	C	C
BAI03.04 - Obtener los componentes de la solución	R	A/R	C	R	C	C	C	C	C
BAI03.05 - Construir soluciones.	R	A/R	C	R	C	C	C	C	C
BAI03.06 - Realizar controles de calidad.	R	A/R	C	R	C	C	C	C	C
BAI03.07 - Preparar pruebas de la solución	R	A/R	C	R	C	C	C	C	C
BAI03.08 - Ejecutar pruebas de la solución	R	A/R	C	R	C	C	C	C	C
BAI03.09 - Gestionar cambios a los requerimientos.	R	A/R	C	R	C	C	C	C	C

BAI03.10 - Mantener soluciones.	R	A/R	C	R	C	R	R	C	C
BAI03.11 - Definir los servicios TI y mantener el catálogo de servicios.	I	A/R	C	R	C	C	C	C	C

Administración de cambios

Objetivo:

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 mediante la 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.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del mismo se puede evidenciar al menos los siguientes elementos:

    - Identificación clara del cambio a realizar en la infraestructura.
    - Categorización, priorización y procedimientos de emergencia a llevar a cabo durante el cambio.
    - Evaluación del impacto que ocasiona el cambio en la infraestructura.
    - Procedimiento de autorización de los cambios.
    - Procedimiento de administración de versiones.
    - Políticas de distribución del software.
    - Obtención de herramientas automatizadas para realizar los cambios.
    - Procedimientos para la administración de la configuración.
    - Rediseño de los procesos del negocio que se vean impactados por el cambio en la infraestructura.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	Lógica
BAI06.01 - Evaluar, priorizar y autorizar peticiones de cambio.	Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.
BAI06.02 - Gestionar cambios de emergencia.	Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.
BAI06.03 - Hacer seguimiento e informar de cambios de estado.	Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.
BAI06.04 - Cerrar y documentar los cambios.	Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
BAI06.01 - Evaluar, priorizar y autorizar peticiones de cambio.	BAI03.05 - Componentes de la solución integrados y configurados DSS02.03 - Peticiones de Servicio aprobadas DSS03.03 - Soluciones propuestas para errores conocidos DSS03.05 - Soluciones sostenibles identificadas DSS04.08 - Cambios aprobados a los planes DSS06.01 - Análisis de causa raíz y recomendaciones
BAI06.02 - Gestionar cambios de emergencia.	N/A
BAI06.03 - Hacer seguimiento e informar de cambios de estado.	BAI03.09 - Registro de todas las peticiones de cambio aprobadas y aplicadas
BAI06.04 - Cerrar y documentar los cambios.	N/A

4: Proceso Predecible

Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos
- Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
- Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI
- Frecuencia de actualización del perfil de riesgo
- Número de interrupciones del negocio debidas a incidentes en el servicio de TI
- Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados
- Cantidad de trabajo rehecho debido a cambios fallidos
- Reducción en el tiempo y esfuerzo necesarios para aplicar los cambios

• Número y antigüedad de peticiones de cambio en cartera
• Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	**Ejecutivos de negocio**	**Director de Informática/Sistemas (CIO)**	**Jefe de Arquitectura del Negocio**	**Jefe de Desarrollo**	**Jefe de Operaciones TI**	**Jefe de Administración TI**	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de**
BAI06.01 - Evaluar, priorizar y autorizar peticiones de cambio.	A	R	C	R	R	C	R	C	
BAI06.02 - Gestionar cambios de emergencia.	A	R	I	R	R		I	C	
BAI06.03 - Hacer seguimiento e	C	A		R	R		R		

informar de cambios de estado.									
BAI06.04 - Cerrar y documentar los cambios.	A	R	C	R	R	I	I		

Administración de servicios con terceros.

Objetivo:

Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos mediante la administrar de todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento. Dentro de este modelo se considera que el objetivo es cumplido si dentro del mismo se puede evidenciar al menos los siguientes elementos:

    - Inventario de proveedores críticos
    - SLAs

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
APO10.01 - Identificar y evaluar las relaciones y contratos con proveedores.	Identificar proveedores y contratos asociados y categorizarlos por tipo, relevancia y criticidad. Establecer un criterio de evaluación de contratos y proveedores y evaluar la cartera general de proveedores y contratos actuales y alternativos.
APO10.02 - Seleccionar proveedores.	Seleccionar proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos.

	Los requisitos deberían estar optimizados con las aportaciones de nuevos proveedores potenciales.
APO10.03 - Gestionar contratos y relaciones con proveedores.	Formalizar y gestionar las relaciones con cada proveedor. Gestionar, mantener y supervisar los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, las leyes y las regulaciones. Gestionar los conflictos contractuales.
APO10.04 - Gestionar el riesgo en el suministro.	Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente.
APO10.05 - Supervisar el cumplimiento y el rendimiento del proveedor.	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y el valor de lo pagado y tratar las incidencias identificadas.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**

APO10.01 - Identificar y evaluar las relaciones y contratos con proveedores.	Fuera de Cobit - Contratos con los proveedores
APO10.02 - Seleccionar proveedores.	BAI02.02 - Plan de adquisiciones/ desarrollos de alto nivel
APO10.03 - Gestionar contratos y relaciones con proveedores.	BAI03.04 - Planes de adquisición aprobados
APO10.04 - Gestionar el riesgo en el suministro.	APO12.04 - • Resultados de la evaluación de riesgos de terceros. • Análisis de Riesgos e informes de perfil de riesgo para las partes interesadas.
APO10.05 - Supervisar el cumplimiento y el rendimiento del proveedor.	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje de proveedores que cumplen con los requisitos acordados
- Número de infracciones de servicio causadas por los proveedores
- Número de eventos de riesgo que conducen a incidentes del servicio
- Frecuencia de las reuniones con suministradores sobre la gestión de riesgos
- Porcentaje de los incidentes relacionados con los riesgos resueltos adecuadamente (en tiempo y coste)
- Numero de reuniones de revisión con proveedores
- Número de disputas formales con proveedores
- Porcentaje de disputas con proveedores resueltas adecuadamente y en un tiempo razonable

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el

proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Ejecutivos de negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
APO10.01 - Identificar y evaluar las relaciones y contratos con proveedores.	C	A	C	C	C	R	C	C	C
APO10.02 - Seleccionar proveedores.	C	A	C	C	C	R	C	C	C
APO10.03 - Gestionar contratos y relaciones con proveedores.		A	C	R	R	R	C	C	C
APO10.04 - Gestionar el riesgo en el suministro.		A	C	R	R		C	C	C
APO10.05 - Supervisar el cumplimiento y el rendimiento del proveedor.	I	A	C	R	R		C	C	C

Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.

Objetivo:

Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad mediante procesos que permitan equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
BAI04.01 - Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los ANSs. Crear líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.
BAI04.02 - Evaluar el impacto en el negocio.	Identificar los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias del negocio. Asegurar que el

	impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos.
BAI04.03 - Planificar requisitos de servicio nuevos o modificados.	Planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio
BAI04.04 - Supervisar y revisar la disponibilidad y la capacidad	Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a las líneas de referencia establecidas. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.
BAI04.05 - Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**

BAI04.01 - Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	BAI02.01 - Repositorio de definición de requisitos BAI02.03 - Registro de requisito de riesgos
BAI04.02 - Evaluar el impacto en el negocio.	BAI03.02 - AMS internos y externos
BAI04.03 - Planificar requisitos de servicio nuevos o modificados.	BAI02.01 - Criterios de aceptación confirmados por las partes interesadas BAI03.01 - Especificaciones de diseño de alto nivel aprobadas BAI03.02 - Especificaciones de diseño detallado aprobadas BAi03.03 - Componentes de la solución documentados
BAI04.04 - Supervisar y revisar la disponibilidad y la capacidad	N/A
BAI04.05 - Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Número de actualizaciones de capacidad, rendimiento o disponibilidad no planificada
- Número de picos de transacciones donde se excede la meta de rendimiento
- Número de incidentes de disponibilidad
- Número de eventos donde la capacidad ha excedido los límites planificados
- Número y porcentaje de cuestiones de disponibilidad, rendimiento y capacidad no resueltos

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos

Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Propietarios de los procesos del negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
BAI04.01 - Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	I	C		C	A		R	C	C
BAI04.02 - Evaluar el impacto en el negocio.	A	C		C	A		R	C	C
BAI04.03 - Planificar requisitos de servicio nuevos o modificados.	R	C		C	A		R	C	C
BAI04.04 - Supervisar y revisar la	R	C		C	A		R	C	C

disponibilidad y la capacidad									
BAI04.05 - Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	R	I	R	C	A		R	I	I

Continuidad del negocio..

Objetivo:

Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa mediante el establecimiento y mantenimiento de un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
DSS04.01 - Definir la política de continuidad del negocio, objetivos y alcance.	Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.
DSS04.02 - Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.
DSS04.03 - Desarrollar e implementar una respuesta	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para

a la continuidad del negocio.	facilitar que la empresa continúe con sus actividades críticas
DSS04.04 - Ejercitar, probar y revisar el plan de continuidad.	Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.
DSS04.05 - Revisar, mantener y mejorar el plan de continuidad.	Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.
DSS04.06 - Proporcionar formación en el plan de continuidad.	Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.
DSS04.07 - Gestionar acuerdos de respaldo.	Mantener la disponibilidad de la información crítica del negocio.
DSS04.08 - Ejecutar revisiones post reanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
DSS04.01 - Definir la política de continuidad del negocio, objetivos y alcance.	APO09.03 ANS
DSS04.02 - Mantener una estrategia de continuidad.	APO12.06 • Causas raíz relacionadas con riesgos • Comunicaciones del impacto de los riesgos
DSS04.03 - Desarrollar e implementar una respuesta a la continuidad del negocio.	APO09.03 Acuerdos de Nivel Operativo (OLAs)
DSS04.04 - Ejercitar, probar y revisar el plan de continuidad.	N/A
DSS04.05 - Revisar, mantener y mejorar el plan de continuidad.	N/A
DSS04.06 - Proporcionar formación en el plan de continuidad.	RR HH - Lista de personal que requiere formación
DSS04.07 - Gestionar acuerdos de respaldo.	N/A
DSS04.08 - Ejecutar revisiones post reanudación.	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

• Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento
• Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo
• Porcentaje de medios de respaldo transferidos y almacenados de forma Segura
• Número de sistemas críticos para el negocio no cubiertos por el plan
• Número de ejercicios y pruebas que han conseguido los objetivos de recuperación
• Frecuencia de las pruebas
• Porcentaje de mejoras acordadas que han sido reflejadas en el plan
• Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan
• Porcentaje de interesados internos y externos que han recibido formación
• Porcentaje de asuntos identificados que se han tratado subsecuentemente en los materiales de formación

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	**Ejecutivos del negocio**	**Director de Informática/Sistemas (CIO)**	**Jefe de Arquitectura del Negocio**	**Jefe de Desarrollo**	**Jefe de Operaciones TI**	**Jefe de Administración TI**	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de**
DSS04.01 - Definir la política de continuidad del	C	R			R	C	R		R

negocio, objetivos y alcance.									
DSS04.02 - Mantener una estrategia de continuidad.	C	R	R	C	R				R
DSS04.03 - Desarrollar e implementar una respuesta a la continuidad del negocio.	I	R	C	C	R				A
DSS04.04 - Ejercitar, probar y revisar el plan de continuidad.	I	R		C	R				A
DSS04.05 - Revisar, mantener y mejorar el plan de continuidad.	I	R		C	R				R
DSS04.06 - Proporcionar formación en el plan de continuidad.	I	R	R		R	R	R		A
DSS04.07 - Gestionar acuerdos de respaldo.					C	A			R
DSS04.08 - Ejecutar revisiones post reanudación.	C	R	R	C	C	R	R		A

Seguridad de los sistemas.

Objetivo:

Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información mediante la protección de 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.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento y en este modelo debe contar con al menos los siguientes elementos:

    - Autorización, autenticación y control de acceso.
    - Identificación de usuarios y perfiles de autorización, los cuales deben ser otorgados de acuerdo con la necesidad de tener y necesidad de conocer.
    - Manejo de incidentes, información y seguimiento.
    - Prevención y detección de código malicioso, virus, entre otros.
    - Entrenamiento de usuarios.
    - Administración centralizada de la seguridad.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
DSS05.01 - Proteger contra software malicioso (malware).	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).

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

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.

- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
DSS05.01 - Proteger contra software malicioso (malware).	N/A
DSS05.02 - Gestionar la seguridad de la red y las conexiones.	APO01.06 - Gestión de clasificación de la información APO09.03 ANS
DSS05.03 - Gestionar la seguridad de los puestos de usuario final.	APO03.02 - Modelo de arquitectura de información APO09.03 - • Acuerdos de Nivel de Servicio (ANSs) • Acuerdos de Nivel Operativo (OLAs) BAI09.01 - Resultados de pruebas de inventarios físicos DSS06.06 - Informes de violaciones
DSS05.04 - Gestionar la identidad del usuario y el acceso lógico.	APO01.02 - Definición de roles y responsabilidades relacionadas con TI APO03.02 - Modelo de arquitectura de la información
DSS05.05 - Gestionar el acceso físico a los activos de TI.	N/A
DSS05.06 - Gestionar documentos sensibles y dispositivos de salida.	APO03.02 - Modelo de arquitectura de la información
DSS05.07 - Supervisar la infraestructura para	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no

detectar eventos relacionados con la seguridad.	autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Número de vulnerabilidades descubiertas
- Número de rupturas (breaches) de cortafuegos
- Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final
- Número de incidentes que impliquen dispositivos de usuario final
- Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno
- Promedio de tiempo entre los cambios y actualizaciones de cuentas
- Número de cuentas (con respecto al número de usuarios/empleados autorizados)
- Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno
- Clasificación media para las evaluaciones de seguridad física
- Número de incidentes relacionados con seguridad física
- Número de incidentes relacionados con accesos no autorizados a la información

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Propietarios de los procesos del negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
DSS05.01 - Proteger contra software malicioso (malware).	A	C	I	R	R	I	R		
DSS05.02 - Gestionar la seguridad de la red y las conexiones.	A	C	I	R	R	I	R		
DSS05.03 - Gestionar la seguridad de los puestos de usuario final.	A	C	I	R	R	I	R		
DSS05.04 - Gestionar la identidad del usuario y el acceso lógico.	A	C	I	C	R	I	R		C
DSS05.05 - Gestionar el acceso físico a los activos de TI.	A	C	I	C	R	I	R	I	
DSS05.06 - Gestionar documentos sensibles y		A			R				

dispositivos de salida.									
DSS05.07 - Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	A	C	I	C	R	I	R	I	I

Educación y entrenamiento de usuarios.

Objetivo:

Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa

Criterios adaptados del Modelo:

Medición transversal, donde se considera que el objetivo es cumplido, si se cuenta con evidencias que demuestren que los otros puntos del modelo se cuentan con procesos estructurados mediante los cuales se encuentran a los funcionarios de la compañía para que los conozcan y puedan ejecutarlos o se encuentran en un calificación no inferior a 3

Administración de los datos

Objetivo:

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, mediante la definición y mantenimiento de 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.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento y en este modelo debe contar con al menos los siguientes elementos:

    - Establecer controles de entrada, procesamiento y salida para garantizar la autenticidad e integridad de los datos.
    - Verificar la exactitud, suficiencia y validez de los datos de transacciones que sean capturados para su procesamiento (generados por personas, por sistemas o entradas de interface).
    - Preservar la segregación de funciones en el procesamiento de datos y la verificación rutinaria del trabajo realizado. Los procedimientos deben incluir controles de actualización adecuados, como totales de control "corrida a corrida" y controles de actualización de archivos maestros.
    - Establecer procedimientos para que la validación, autenticación y edición de los datos sean llevadas a cabo tan cerca del punto de origen como sea posible.
    - Definir e implementar procedimientos para prevenir el acceso a la información y software sensitivos de computadores, discos y otros equipos o medios, cuando hayan sido sustituidos o se les haya dado otro uso. Tales procedimientos deben garantizar que los datos marcados como eliminados no puedan ser recuperados por cualquier individuo interno o tercero ajeno a la entidad.

- Establecer los mecanismos necesarios para garantizar la integridad continua de los datos almacenados.
- Definir e implementar procedimientos apropiados y prácticas para transacciones electrónicas que sean sensitivas y críticas para la organización, velando por su integridad y autenticidad.
- Establecer controles para garantizar la integración y consistencia entre plataformas.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
DSS06.01 - Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	Evaluar y supervisar continuamente la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.
DSS06.02 - Controlar el procesamiento de la información.	Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).
DSS06.03 - Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quien los está manejando en su nombre.
DSS06.04 - Gestionar errores y excepciones.	Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía

	de precisión e integridad del proceso de información del negocio.
DSS06.05 - Asegurar la trazabilidad de los eventos y responsabilidades de información.	Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.
DSS06.06 -Asegurar los activos de información.	Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**
DSS06.01 - Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	APO01.06 - • Procedimientos de integridad de datos • Directrices de clasificación de datos
DSS06.02 - Controlar el procesamiento de la información.	BAI05.05 - Plan de operación y uso BAI07.02 - Plan de migración
DSS06.03 - Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	EDM04.02 – Responsabilidades asignadas para la gestión de recursos APO11.01 - Roles, responsabilidades y derechos de decisión del SGC APO13.01 - Declaración de alcance del SGSI DSS05.05 - Registros de acceso
DSS06.04 - Gestionar errores y excepciones.	N/A
DSS06.05 - Asegurar la trazabilidad de los eventos y responsabilidades de información.	N/A
DSS06.06 -Asegurar los activos de información.	N/A

4: Proceso Predecible

Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Porcentaje completado de inventario de procesos críticos y controles clave
- Porcentaje de controles clave cubiertos con los planes de pruebas
- Número de incidentes y evidencias del informe de auditoría indicando fallos de los controles clave
- Porcentaje de roles de proceso de negocio con derechos de acceso y niveles de autorización asignados
- Porcentaje de roles de proceso de negocio con una separación clara de tareas

• Número de incidentes y evidencias de auditoría debido a acceso o violación de segregación de funciones.
• Porcentaje de completitud de registros de transacciones rastreables
• Número de incidentes donde el historial de transacciones no pueda ser recuperado

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Ejecutivos del negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
DSS06.01 - Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	R	C			C		C	C	C
DSS06.02 - Controlar el procesamiento de la información.	R	C			C		C	C	

DSS06.03 - Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	R	C			C		C	R	C
DSS06.04 - Gestionar errores y excepciones.	A	I			C		R		
DSS06.05 - Asegurar la trazabilidad de los eventos y responsabilidades de información.	A	C			C		C	C	
DSS06.06 - Asegurar los activos de información.	A	C			C			C	C

Administración de instalaciones y las operaciones de tecnología

Objetivo:

Entregar los resultados del servicio operativo de TI, según lo planificado, mediante la coordinación y ejecución de las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

Criterios adaptados del Modelo:

0: Proceso no establecido

- **Criterio 1: Cumplimiento del objetivo de control:** Se considera que un proceso se encuentra en 0 cuando no cumple con el objetivo principal planteado para el mismo

1: Proceso ejecutado

- **Criterio 1: Rendimiento del proceso:** El proceso cumple con los objetivos y se cuenta con evidencia de su cumplimiento y en este modelo debe contar con al menos los siguientes elementos:

    - Acceso a las instalaciones.
    - Identificación clara del sitio.
    - Controles de seguridad física.
    - Definición de políticas de inspección y escalamiento de problemas.
    - Planeamiento de continuidad del negocio y administración de crisis.
    - Salud y seguridad del personal.
    - Políticas de mantenimiento preventivo.
    - Protección contra amenazas ambientales.
    - Monitoreo automatizado.

2: Proceso Gestionado

- **Criterio 1: Gestión del rendimiento:** El rendimiento del proceso está ahora implementado de una manera administrada (planificada, monitorizada y ajustada) y sus resultados de trabajo están establecidos, controlados y mantenidos adecuadamente. Ejecutando al menos las siguientes actividades:

Actividad	**Lógica**
DSS01.01 - Ejecutar procedimientos operativos	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

DSS01.02 - Gestionar servicios externalizados de TI	Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.
DSS01.03 - Supervisar la infraestructura de TI	Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.
DSS01.04 - Gestionar el entorno	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.
DSS01.05 - Gestionar las instalaciones	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.

3: Proceso Establecido
Criterio 1: Definición del proceso: El proceso gestionado ahora se implementa utilizando un proceso definido que es capaz de lograr sus resultados del proceso.

- Un proceso estándar, incluyendo guías de adaptación adecuadas, están definidos y describe los elementos fundamentales que deben ser incorporados en un proceso definido.
- La secuencia y la interacción del proceso estándar con otros procesos está determinado.
- Las competencias y roles necesarios para llevar a cabo un proceso están identificados como parte del proceso estándar.
- La infraestructura necesaria y el ambiente de trabajo para realizar un proceso está identificada como parte del proceso estándar.
- Los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso están determinados.

Criterio 2: Definición de entradas del proceso: El proceso cuenta con inputs definidos en incluyen al menos los siguientes elementos para su ejecución (no se requiere la implementación de la actividad de control de COBIT a la que se hace referencia)

Actividad	**Inputs**

DSS01.01 - Ejecutar procedimientos operativos	BAI05.05 - Plan de operación y uso
DSS01.02 - Gestionar servicios externalizados de TI	APO09.03 - • OLAs • ANSs BAI05.05 - Plan de operación y uso
DSS01.03 - Supervisar la infraestructura de TI	BAI03.11 - Definiciones de servicio
DSS01.04 - Gestionar el entorno	N/A
DSS01.05 - Gestionar las instalaciones	N/A

4: Proceso Predecible
Criterio 1: Medición de Procesos: Los Procesos Establecidos operan dentro de los límites establecidos para conseguir los resultados esperados de estos para lo cual se miden las siguientes métricas:

- Número de procedimientos operativos no estándar ejecutados
- Número de incidentes causados por problemas operativos
- Tasa de eventos comparada con el número de incidentes
- Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática

Criterio 2: Formalización de procesos input: Los objetivos de control identificados como inputs en el nivel 3 se encuentran a su vez implementados al menos en un nivel 2, es decir, cumplen sus objetivos y se encuentran gestionados.

5: Optimización de procesos
Criterio 1: Innovación de procesos: Los procesos predecibles son continuamente mejorados para satisfacer los objetivos de negocio existentes y futuros mediante la ejecución de mejora continua, es decir, se toman acciones sobre los indicadores medidos en el nivel 4 no solo con el fin de alcanzar el objetivo sino con el fin de optimizar el proceso para alcanzarlo y se pueden evidenciar iniciativas de innovación aplicadas al proceso las cuales han traído beneficios demostrables.

Implementación:
Matriz Raci Genérica

Actividad	Ejecutivos del negocio	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de
DSS01.01 - Ejecutar procedimientos operativos					A		C	C	C
DSS01.02 - Gestionar servicios externalizados de TI		A			R				
DSS01.03 - Supervisar la infraestructura de TI		I	A		A		C	C	
DSS01.04 - Gestionar el entorno		C	I	C	R		I	R	I
DSS01.05 - Gestionar las instalaciones		C	I	C	R		I	R	I

Documentación

Objetivo:

Contar con procedimientos definidos y debidamente documentados alienados con las políticas de calidad de la organización

Criterios adaptados del Modelo:

Medición transversal, donde se considera que el objetivo es cumplido, si se cuenta con evidencias que demuestren que los otros puntos del modelo se encuentran en un calificación no inferior a 3

Capítulo 5
Propuesta de implementación

Cada uno de los elementos propuestos en el modelo y en la CE29 cuentas con una matriz RACI genérica la cual puede ser usada como base para la implementación de los procesos en las entidades, entendiendo que de acuerdo al tamaño y la complejidad del ambiente de TI de cada organización se puede contar con estructuras más amplias o pequeñas, las cuales pueden ser adaptadas para cumplir los roles y actividades identificadas.

De igual manera se proponen indicadores generales en los niveles 4 los cuales pueden ser usados desde niveles más temprano con el fin de soportar una adecuada implementación.

Propuesta de implementación SFC (industria):

Si bien en nuestro ambiente colombiano se persigue activamente la protección de los datos y se reconoce en la mejora de los procesos una ventaja competitiva frente a otras entidades del sector, también se reconoce que como industria se encuentra en el interés colectivo de las personas velar por la mejora continua de los procesos de quienes participan en el mismo.

Por esta razón existen en Colombia y en el mundo diferentes normativas y regulaciones, que pretenden garantizar que las organizaciones implementen estándares mínimos de calidad con el fin de garantizar un buen servicio y operación en el sector, es por esta razón que se propone que sea el ente regulado (en este caso la superintendencia financiera) quien establezca nuevos lineamientos en la industria donde se analice este modelo con el fin de encontrar acuerdos sobre su aplicación en la medición HOMOGENEA de la industria, con el compromiso de que dichos resultados, sean regresados al ente regulador, agrupados y preparados a nivel de industria con el fin de crear un benchmarking objetivo sobre el cual se puedan comparar las compañías de la instruía así como posibles nuevos actores.

Contar con dicha información facilitaría los procesos de innovación y mejora continua de los miembros del sector y a la larga se transforma en beneficios que sean percibidos por todos los stakeholder.

A modo general se recomiendan las siguientes etapas:

1. Conformar equipos de trabajo por industria: especialistas en gobierno de TI para el sector financiero, representantes de la industria y representantes del regulador
2. Análisis del modelo
3. Crear acuerdos sobre el reporte: (estructura, posible anonimidad del resultado)
4. Crear métricas de sector por tamaño y tipo de empresa (banco, fiducia, seguros, etc…)

5. Generar reportes periódicos (se sugieren anuales) con los resultados de la medición.

Capítulo 6
Conclusiones

1. La CE29 aunque es avanzada en materia de definir aspectos puntuales de TI a ser tenidos en cuenta en el gobierno corporativo y los ambientes de control, cuenta con espacio para mejora frente a las definiciones de la normal, así como la actualización de los componentes evaluados bajo estándares más recientes como el COBIT 5. PMI, ITIL V3 y TOGAF, entre otros.
2. Aunque fue posible realizar un mapeo objetivo de los puntos de la norma contra los estándares de COBIT, se identificaron dificultades a la hora de alienar los componentes de control interno con el mismo, principalmente por que la norma no especifica la razón por la cual solicita los componentes que propone, por ejemplo la documentación como último punto, en la mayoría de estándares actuales se puede comprender como un subcomponente de un sistema de administración de calidad, lo cual genera redundancias en la normativa y fueron atendidos en el modelo mediante la simplificación de los puntos solicitados.
3. Si bien el PAM es un modelo establecido y refinado para la medición de madurez de procesos, muchas de las actividades de la norma apuntan a resultado o entregables más no determinan procesos necesarios, por ejemplo el plan estratégico de TI, el cual es un entregable del proceso de administración de la estrategia, motivo por el cual el modelo se amplia de entregables a procesos con el fin de abarcar mayores componentes de gobierno que bajo las buenas practicas actuales cubren las necesidades de control interno y gobiernos de las entidades mejor que la simple construcción de un entregable, razón por la cual fue necesario modificar el modelo de medición disminuyendo y ajustando los criterios estándares del PAM
4. Los procesos normativos de Colombia aun no explotan la oportunidad de pasar de ser una imposición o amenaza de las entidades para pasar a ser una oportunidad a explotar por las mismas, este modelo pretende dar un paso en lograr lo segundo.
5. El reto más importante y que se hace evidente con el doble mapeo del modelo es ser consistentes con el alineamiento estratégico y los objetivos organizacionales, razón por la cual los procesos de administración y gobierno (en el caso de este modelo altamente representados en “plan estratégico”) se hacen un pazo inicial clave en cualquier ambiente de control y deben ser insumo de la totalidad de los otros procesos.

Capítulo 7
Referencia Bibliográfica

COBIT 5 The Framework – ISACA
COBIT 5 Información catalizadora – ISACA
COBIT 5 Procesos catalizadores – ISACA
COBIT 5 Guía de implementación – ISACA
PAM para COBIT 5 – ISACA
ITIL V3 – IT Infraestructure Library – Service Operation
Circular Básica Jurídica 29 del 2014 (C.E 29/14) - Superintendencia Financiera de Colombia
Committe of sponsoring organizations – COSO
MECI – Modelo estándar de Control Interno de Colombia