



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA
COLECTIVIDAD**

**MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS
TECNOLÓGICOS**

VI – VII PROMOCIÓN

**TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE
SISTEMAS TECNOLÓGICOS**

**TEMA: “EVALUACIÓN TECNOLÓGICA DE GOBIERNO Y GESTIÓN DE TI
EN BANCO BANCODESARROLLO MEDIANTE LOS DOMINIOS
EVALUAR/ORIENTAR/SUPERVISAR, ALINEAR/PLANEAR/ORGANIZAR
Y SUPERVISAR/EVALUAR/VALORAR DE COBIT5”.**

**AUTORES: ING. GERARDO CAJAMARCA MENDEZ
 ING. DANIEL GUERRON BENALCAZAR**

DIRECTOR: ING. RON GAVI MARIO GIOVANNY MGS.

SANGOLQUI, MAYO DE 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA
COLECTIVIDAD

CERTIFICADO


ING. MARIO GIOVANNY RON
Director


ING. PABLO XAVIER PARRA
Oponente

CERTIFICAN

Que el trabajo titulado "EVALUACIÓN TECNOLÓGICA DE GOBIERNO Y GESTIÓN DE TI EN BANCO BANCODESARROLLO MEDIANTE LOS DOMINIOS EVALUAR ORIENTAR SUPERVISAR, ALINEAR PLANEAR ORGANIZAR Y SUPERVISAR EVALUAR VALORAR DE COBIT 5", realizado por: Gerardo Cajamarca Méndez y Daniel Guerrón Benalcázar, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas ESPE.

Debido a que se ha cumplido con las normas establecidas por la ESPE para el desarrollo del trabajo de conclusión de carrera, se recomienda su publicación, excepto los anexos que citan información de carácter reservado.

El mencionado trabajo consta de un documento empastado y disco compacto el cual contiene los archivos en formato portátil de Acrobat (PDF).

Autorizan a Gerardo Cajamarca Méndez y Daniel Guerrón Benalcázar, entregar el mismo a la Unidad de Gestión de Postgrados.

Sangolquí, 4 de mayo del 2015.

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE
VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA
COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS
TECNOLÓGICOS

VI Y VII PROMOCIÓN 2012-2014.

DECLARACIÓN DE RESPONSABILIDAD

Cajamarca Méndez Gerardo
Guerrón Benalcázar Daniel

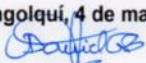
DECLARAMOS QUE:

El proyecto de grado denominado "EVALUACIÓN TECNOLÓGICA DE GOBIERNO Y GESTIÓN DE TI EN BANCO BANCODESARROLLO MEDIANTE LOS DOMINIOS EVALUAR ORIENTAR SUPERVISAR, ALINEAR PLANEAR ORGANIZAR Y SUPERVISAR EVALUAR VALORAR DE COBIT 5", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el trabajo correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.


Ing. Gerardo Cajamarca Méndez

Sangolquí, 4 de mayo del 2015

Ing. Daniel Guerrón Benalcázar

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS
TECNOLÓGICOS

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Gerardo Cajamarca Méndez y Daniel Guerrón
Benalcázar

Autorizamos a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la Institución, del trabajo "EVALUACIÓN TECNOLÓGICA DE GOBIERNO Y GESTIÓN DE TI EN BANCO BANCODESARROLLO MEDIANTE LOS DOMINIOS EVALUAR ORIENTAR SUPERVISAR, ALINEAR PLANEAR ORGANIZAR Y SUPERVISAR EVALUAR VALORAR DE COBIT5", cuyo contenido, ideas y criterios son de nuestra entera exclusiva responsabilidad y autoría.

Sangolquí, 4 de mayo del 2015



Ing. Gerardo Cajamarca Méndez



Ing. Daniel Guerrón Benalcázar

DEDICATORIA

Dedico este trabajo principalmente a mi amada esposa Myriam, quien siempre estuvo a mi lado apoyándome incondicionalmente para seguir adelante y culminar con éxito mi meta.

A mis queridos hijos Bryan, Marlon, Kamila a quienes les robe parte de su tiempo en el cual podríamos a ver estado juntos.

A mi madre Cristina que a pesar de su enfermedad es un ejemplo de lucha.

Gerardo Cajamarca Méndez

DEDICATORIA

Dedico este trabajo a mi amada hija Carmine, quien me mantuvo intensamente motivado para concluir con esta meta, ella desde el primer día en que asumí este reto me invitó a tolerar la nostalgia de no presenciar sus ocurrencias, muestras de amor y alegría.

Lo dedico también a mi esposa Lorena, quien ha sabido aceptar mi ausencia, apoyarme y sobrellevar las actividades durante mis jornadas de estudio y preparación.

Daniel Guerrón Benalcázar.

AGRADECIMIENTOS

Agradezco a Dios por guiarme y acompañarme durante todo el tiempo permitiéndome iniciar y culminar una de mis metas con éxito.

Le doy gracias a mi padre Jorge por estar pendiente de mis estudios.

A mis maestros y amigos por compartir sus conocimientos.

A mi viejo amigo Giovanni Ron por aceptar ser nuestro tutor y guiarnos durante todo el desarrollo de la tesis.

A banco BanCodesarrollo por colaborarnos con su auspicio, para realizar este proyecto brindándonos facilidades en medida de sus posibilidades.

Gerardo Cajamarca Méndez

AGRADECIMIENTOS

Expreso mi infinito agradecimiento a Dios, mis padres, hermanos y la vida por haberme enseñado y estimulado a aceptar retos, resolver obstáculos y nunca rendirme.

A mis familiares, amigos, compañeros y maestros que de múltiples maneras han aportado para que este trabajo concluya exitosamente.

A mi tutor Giovanni Ron Gavi que con profesionalismo y amistad ha guiado la ejecución de este proyecto.

A BanCodesarrollo y su personal, por la apertura y facilidades proporcionadas para que esta evaluación tecnológica se lleve a cabo.

Daniel Guerrón Benalcázar

Tabla de contenido

Índice de Figuras:	xi
Índice de Tablas:.....	xii
Índice de Anexos:	xiii
RESUMEN	xiv
ABSTRACT.....	xv
1 CAPÍTULO I: INTRODUCCIÓN.	1
1.1 Antecedentes.	1
1.2 Situación actual.....	1
1.3 Definición del problema.....	2
1.4 Objetivo general.	3
1.5 Objetivos específicos.	4
2 CAPÍTULO II : MARCO TEÓRICO.	4
2.1 Generalidades.....	4
2.1.1 Auditoría Financiera.....	5
2.1.2 Auditoría Operacional.	5
2.1.3 Auditoría de cumplimiento.	5
2.1.4 Examen Especial.	6
2.1.5 Auditoría Informática.....	6
2.2 Auditoría Informática.....	6
2.2.1 Herramientas y Técnicas para la Auditoría Informática.	8
2.3 Auditoría Tecnológica Basada en Riesgos.....	9
2.3.1 Componentes del riesgo:.....	9
2.3.2 El problema como contingencia del riesgo.	10
2.3.3 Mapa de Riesgo.....	11
2.3.4 Riesgo tecnológico.	11
2.4 COBIT 5®.	12
2.4.1 Principios de COBIT 5 ®:.....	13

2.4.2	Principio 1: Satisfacer las necesidades de las partes interesadas.	14
2.4.3	Catalizadores:.....	15
2.4.4	Principio 2: Cubrir la empresa Extremo a extremo.	15
2.4.5	Principio 3: Aplicar un marco de referencia único integrado.	16
2.4.6	Principio 4: Hacer posible un enfoque holístico.	16
2.4.7	Principio 5: Separar el gobierno de la gestión.	17
2.4.8	Procesos de COBIT 5 ®:	18
3	CAPÍTULO III: EJECUCIÓN DE LA EVALUACIÓN TECNOLÓGICA.	19
3.1	Marco Metodológico.....	19
3.2	Planificación del Proceso de Evaluación Tecnológica.	21
3.3	Levantamiento y Recolección de Información.....	22
3.3.1	Guía de Entrevistas:	22
3.4	Análisis de la Información.	23
3.4.1	Dominio Evaluar/Orientar/Supervisar (EDM).	24
3.4.2	Dominio Alinear/Planear/Organizar (APO).	37
3.4.3	Dominio Supervisar/Evaluar/Valorar (MEA).....	84
3.4.4	Evaluación de Gestión y Gobierno:	95
3.4.5	Nivel de aplicación de COBIT 5:	99
3.5	Hallazgos de la Evaluación Tecnológica.....	100
3.5.1	Dominio Evaluar/Orientar/Supervisar (EDM).	100
3.5.2	Dominio Alinear/Planear/Organizar (APO).	101
3.5.3	Dominio Supervisar/Evaluar/Valorar (MEA).....	104
3.5.4	Procesos COBIT de riesgos.	105
3.5.5	Controles implementados.	106
4	CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES.....	109

4.1	Conclusiones.	109
4.2	Recomendaciones.	110
5	Bibliografía.....	112
	ANEXOS.....	114

Índice de Figuras:

Figura 1: Tipos de Auditoría.....	4
Figura 2: Mapa de Riesgo.....	11
Figura 3: Evolución COBIT.	12
Figura 4: Principios de COBIT 5.	13
Figura 5: Objetivo de Gobierno – Creación de Valor.	14
Figura 6: Gobierno y Gestión en COBIT 5.	16
Figura 7: Áreas clave de Gobierno y Gestión en COBIT 5.	17
Figura 8: Modelo de Referencia de Procesos COBIT 5.	18
Figura 9: Planeamiento del Proceso de Evaluación Tecnológica.	21
Figura 10: Resultado General de la Evaluación Tecnológica.	98
Figura 11: Porcentaje de aplicación implícita de COBIT 5®.	99
Figura 12: Resultado de Evaluación Tecnológica por Procesos.	100
Figura 13: Evaluación Tecnológica Dominio EDM.....	100
Figura 14: Evaluación Tecnológica Dominio APO.	101
Figura 15: Hallazgos Proceso APO04.	101
Figura 16: Hallazgos Proceso APO11.	103
Figura 17: Evaluación Tecnológica Dominio MEA.	104
Figura 18: Riesgos en proceso EDM03.	105
Figura 19: Riesgos en proceso APO12.....	106

Índice de Tablas:

Tabla 1	Parámetros de Evaluación	20
Tabla 2	Plantilla para el proceso EDM01	24
Tabla 3	Plantilla para el proceso EDM02	27
Tabla 4	Plantilla para el proceso EDM03.	30
Tabla 5	Plantilla para el proceso EDM04	32
Tabla 6	Plantilla para el proceso EDM05	34
Tabla 7	Plantilla para el proceso APO01	37
Tabla 8	Plantilla para el proceso APO02	43
Tabla 9	Plantilla para el proceso APO03	47
Tabla 10	Plantilla para el proceso APO04	51
Tabla 11	Plantilla para el proceso APO05	55
Tabla 12	Plantilla para el proceso APO06	58
Tabla 13	Plantilla para el proceso APO07	62
Tabla 14	Plantilla para el proceso APO08	66
Tabla 15	Plantilla para el proceso APO09	69
Tabla 16	Plantilla para el proceso APO10	71
Tabla 17	Plantilla para el proceso APO11	74
Tabla 18	Plantilla para el proceso APO12	78
Tabla 19	Plantilla para el proceso APO13	82
Tabla 20	Plantilla para el proceso MEA01	84
Tabla 21	Plantilla para el proceso MEA02	87
Tabla 22	Plantilla para el proceso MEA03	92
Tabla 23	Resultados de las prácticas en los dominios evaluados	95
Tabla 24	Listado De Controles por Área de Negocio	107

Índice de Anexos:

ANEXO A: RESUMEN DE ENTREVISTAS.

ANEXO B: SOLICITUD DE INFORMACIÓN.

ANEXO C: INVENTARIO DE EVIDENCIA.

ANEXO D: MATRICES RACI.

ANEXO E: VALORACIÓN DE CRITERIOS.

ANEXO F: DOCUMENTACIÓN BANCODESARROLLO.

RESUMEN

El presente documento contiene la información completa de la Evaluación Tecnológica de Gobierno y Gestión de TI en banco BanCodesarrollo mediante los dominios Evaluar Orientar Supervisar, Alinear Planear Organizar y Supervisar Evaluar Valorar de Cobit 5®, se sustenta en su marco de trabajo, metodología sugerida y herramientas de trabajo creadas para dicho propósito, describe el proceso de evaluación, aspectos analizados, tablas y gráficas que explican los resultados, así como el detalle de los hallazgos, finalizando con conclusiones y recomendaciones acorde con el trabajo de campo realizado y las situaciones identificadas.

PALABRAS CLAVE:

EVALUACIÓN TECNOLÓGICA.

GOBIERNO.

GESTIÓN.

TI.

COBIT 5.

ABSTRACT

This document contains the complete information about government technology and TI Management evaluation in BanCodesarrollo bank by means of domains Evaluate Direct Monitor, Align Plan Organise and Monitor Evaluate Assess COBIT 5®, it sustains in its framework, methodology and working tools created for that purpose, the evaluation process describes, aspects analyzed, tables and graphs that explain results such us details of findings, ending with conclusions and recommendations according with fieldwork performed and identified situations.

KEYWORDS:

TECHNOLOGICAL EVALUATION.

GOVERNMENT.

MANAGEMENT.

IT.

COBIT 5.

1 CAPÍTULO I: INTRODUCCIÓN.

1.1 Antecedentes.

El banco BanCodesarrollo es Institución Financiera Ecuatoriana que tras contar con una importante trayectoria en el Sistema Cooperativo Nacional se constituyó como banco en febrero del 2014, incorporándose a un destacado segmento institucional donde se vuelve más visible para la Superintendencia de Bancos y Seguros del Ecuador, por lo que se torna indispensable que la institución considere y adopte todos los lineamientos de carácter normativo, orientados a cumplir con las regulaciones y administrar de manera integral sus riesgos.

Este proyecto evaluará técnicamente al banco BanCodesarrollo empleando principalmente el Marco de Referencia de Gobierno y Gestión de TI Cobit5® y sus dominios Evaluar/Orientar/Supervisar, Alinear/Planear/Organizar y Supervisar/Evaluar/Valorar.

Esta evaluación permitirá conocer el gobierno de TI y observar el impacto de los riesgos tecnológicos en la gestión de TI, valorar los controles que se ha implementado así como medir su efectividad, en procura de minimizar la afectación ante la ocurrencia de eventos sobre los activos de tecnología.

1.2 Situación actual.

Tanto a nivel nacional como internacional existen iniciativas de manera independiente o como parte de un Plan de Auditoría Interna o Externa que plantean la necesidad de realizar este tipo de evaluaciones en las áreas de

Tecnología de Información y que desde luego las ejecutan con diferentes propósitos como:

- Evaluar el grado de madurez en la adopción de marcos de referencia para gestión de TI.
- Evaluar el nivel de cumplimiento de la normativa aplicable vigente.
- Determinar el grado de riesgo y el nivel de gestión que existe en las organizaciones.
- Fortalecer la cultura de control interno a nivel corporativo para asegurar el cumplimiento de objetivos estratégicos del negocio como herramienta para cumplir con las metas económicas inclusive.
- Determinar la Eficiencia Administrativa de sus áreas de TI.

Partiendo de lo dicho los trabajos enfocan sus esfuerzos a la gestión de riesgos de TI, empleando para ellos buenas prácticas, estándares y marcos de referencia, en su mayoría emplean COBIT sea versión 4.1 o 5 para realizar la evaluación.

No obstante de una evaluación el aspecto clave y el beneficio se puede lograr únicamente con la aplicación de las recomendaciones emitidas y la constante evaluación en procura de siempre actuar apegado a la dinámica del negocio.

1.3 Definición del problema.

En la actualidad las instituciones financieras se ven envueltas en una corriente presionada a fortalecer su gestión integral de riesgos, incrementar su madurez en la gestión de tecnología de información alineada totalmente a los objetivos del negocio y apoyada en la adopción de estándares, buenas prácticas y marcos de referencia de reconocimiento internacional.

La realidad y limitaciones de cada institución financiera es muy particular lo que hace suponer que exista una falta de cultura y madurez institucional para gestionar de manera integral los riesgos corporativos.

Este proyecto busca respuesta a las siguientes interrogantes:

- ¿Banco BanCodesarrollo gestiona su tecnología alineándose a marcos de referencia y buenas prácticas?
- ¿Cuál es el nivel de alineamiento de su gobierno y gestión de TI con respecto a lo que sugieren a los dominios Evaluar/Orientar/Supervisar, Alinear/Planear/Organizar y Supervisar/Evaluar/Valorar de Cobit5®?
- ¿Cuán relevante y favorable institucionalmente hablando podría ser el que banco BanCodesarrollo reoriente su enfoque implementando Cobit5®?

1.4 Objetivo general.

Evaluar tecnológicamente a banco BanCodesarrollo, empleando principalmente el Marco de referencia para los Objetivos de Control y Tecnología Relacionada Cobit5® en el ámbito de los dominios Evaluar/Orientar/Supervisar, Alinear/Planear/Organizar y Supervisar/Evaluar/Valorar para tener un entendimiento detallado del gobierno y gestión de TI.

1.5 Objetivos específicos.

- Determinar el nivel de implementación de gobierno y gestión de TI de banco BanCodesarrollo.
- Valorar los controles que se han implementado y determinar en base al análisis de riesgos su afectación al banco.
- Emitir recomendaciones orientadas a fortalecer el gobierno y gestión de TI.
- Ayudar al banco BanCodesarrollo a robustecer el gobierno y gestión de TI, mediante la optimización de los niveles de riesgo y el uso de recursos tecnológicos.

2 CAPÍTULO II: MARCO TEÓRICO.

2.1 Generalidades.

La Auditoría puede definirse como una práctica metódica y profesional en la que se recopilan y evalúan datos sobre una entidad con el propósito de determinar e informar la relación existente entre la información y los criterios establecidos. (Bermeo, 2012).

Existen diversos tipos de Auditorías, estas por su ámbito de ejecución, propósito o especificidad pueden ser clasificadas, dando como resultado la tipificación que se aprecia en la Figura 1.



Figura 1: Tipos de Auditoría.

Las auditorías se ejecutan en función a normas nacionales e internacionales, con apego a normas y directrices, siguiendo metodologías y procedimientos, empleando varias técnicas y haciendo uso de herramientas que faciliten y posibiliten su labor (Bermeo, 2012).

2.1.1 Auditoría Financiera.

Es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la situación financiera de la empresa, este proceso solo es posible llevarlo a cabo a través de un elemento llamado evidencia de auditoría, ya que el auditor hace su trabajo posterior a las operaciones de la empresa. (gerencie, 2013)

2.1.2 Auditoría Operacional.

Es el examen posterior, profesional, objetivo y sistemático de la totalidad o parte de las operaciones o actividades de una entidad, proyecto, programa, inversión o contrato en particular, sus unidades integrantes u operacionales específicas.

Su propósito es determinar los grados de efectividad, economía y eficiencia alcanzados por la organización y formular recomendaciones para mejorar las operaciones evaluadas. Relacionada básicamente con los objetivos de eficacia, eficiencia y economía. (gerencie, 2013)

2.1.3 Auditoría de cumplimiento.

Es la comprobación o examen de operaciones financieras, administrativas, económicas y de otra índole de una entidad para establecer que se han realizado conforme a las normas legales, reglamentarias, estatutarias y de procedimientos que le son aplicables.

Esta auditoria se practica mediante la revisión de documentos que soportan legal, técnica, financiera y contablemente las operaciones para determinar si los procedimientos utilizados y las medidas de control interno están de acuerdo con las normas que le son aplicables y si dichos procedimientos están operando de manera efectiva y son adecuados para el logro de los objetivos de la entidad (gerencie, 2013).

2.1.4 Examen Especial.

Revisión de auditoria que tiene características particulares que generalmente obedecen a requerimientos de Alta Gerencia y que por su impacto merece especial e inmediata atención y que no fueron planificados (puce, 2015).

2.1.5 Auditoria Informática.

Es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio. (Computacionales, 2011)

2.2 Auditoría Informática.

La Auditoria de Tecnología de Información como se le conoce actualmente, (Auditoria informática o Auditoria de sistemas en nuestro medio), se ha consolidado en el mundo entero como cuerpo de conocimientos cierto y consistente, respondiendo a la acelerada evolución de la tecnología informática de los últimos 10 años.

La INFORMACIÓN es considerada un activo tan o más importante que cualquier otro en una organización.

Existe pues, un cuerpo de conocimientos, normas, técnicas y buenas practicas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la INFORMACION tratada y almacenada a través del computador y equipos afines, así como de la eficiencia, eficacia y economía con que la administración de un ente están manejando dicha INFORMACION y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo lo anterior con el objetivo de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoria de general aceptación y conocimiento técnico específico. (Computacionales, 2011)

Los principales criterios respecto de la Información que se analiza en la Auditoría Informática son la Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Confiabilidad y Cumplimiento. (Bermeo, 2012)

Entre las principales motivaciones para llevar a cabo un trabajo de Auditoría Informática están:

- Determinar una mejor relación costo-beneficio de los sistemas tecnológicos.
- Incrementar el nivel de satisfacción de los usuarios de TI.
- Validar y asegurar la integridad, confidencialidad, disponibilidad y confiabilidad de la información.
- Develar la situación actual del área informática en pro de apoyarla para la consecución de los objetivos propuestos.
- Fortalecer la seguridad en el entorno del talento humano, datos, hardware, software e instalaciones.
- Gestionar los riesgos en el uso de TI.

Varias administraciones suelen cuestionar la existencia de argumentos válidos para recurrir a servicios de Evaluaciones o Auditorías Informáticas, sin embargo se podrían justificar reflexionando sobre lo siguiente:

- Razonabilidad de la elevada demanda de presupuesto de TI.

- Incertidumbre a nivel directivo sobre el verdadero soporte tecnológico del área de TI.
- Nivel de protección en seguridades lógicas y físicas que garanticen la integridad del personal, la infraestructura tecnológica y la información crítica de la empresa.
- Creciente apareamiento de fraudes informáticos.
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano.
- Insatisfacción debido a la falta de oportunidad en la prestación de servicios de TI.

2.2.1 Herramientas y Técnicas para la Auditoría Informática.

El trabajo de campo de la auditoría informática se facilita con el empleo de herramientas y técnicas, las más relevantes se describen a continuación:

2.2.1.1 Cuestionarios.

Los cuestionarios están formados de un conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito y cuyo fin es poner en evidencia determinados aspectos.

2.2.1.2 Entrevistas.

La entrevista es una de las actividades personales más importante del auditor con la que se recoge más información brindando una visión más profunda de la realidad y de otros aspectos que se declaran y deberán ser evidenciados.

2.2.1.3 Checklist.

Las listas de verificación constituyen una guía para que los puntos a analizar o actividades no sean omitidas. (Computacionales, 2011)

2.2.1.4 Trazas y/o Huellas.

Para la verificación de programas o sistemas el auditor informático se apoya en productos de software potentes y modulares que entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Las trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas, las mencionadas trazas no deben modificar en absoluto el sistema. (Computacionales, 2011)

2.3 Auditoria Tecnológica Basada en Riesgos.

Partiendo de una definición sencilla de **riesgo**, como la posibilidad de que un acontecimiento no esperado genere un resultado no deseado y la de **control interno** como una práctica común de los miembros de una organización, y con el objeto de proporcionar un grado de seguridad razonable en la consecución de objetivos surge la lógica necesidad de implementar algo que los permita prever y hacerles frente, lo que motiva al nacimiento de la administración y posterior concepto de gestión de riesgos. (Córdova, 2012)

2.3.1 Componentes del riesgo:

a) Probabilidad: Posibilidad de ocurrencia de un riesgo, medible a través de criterios de frecuencia o considerando la existencia de factores internos y externos, que propician el riesgo aún si éste no ha sucedido.

b) Severidad: Magnitud de los efectos o consecuencias que ocasionaría a la institución la ocurrencia de un riesgo.

c) Nivel de riesgo: Resultado de confrontar la severidad y la probabilidad con los controles existentes.

d) Riesgos de Tecnología: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la institución y soporten el cumplimiento de la misión.

e) Administración de Riesgos: Proceso estructurado, consistente y continuo, implementado a través de toda la entidad para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el logro de los objetivos institucionales, a fin de proponer soluciones o alternativas para minimizar el impacto de los riesgos en el rendimiento institucional. (olacefs, 2011)

2.3.2 El problema como contingencia del riesgo.

La gama de riesgos que se enfrentan en una entidad depende, entre otros, de los siguientes factores:

- El volumen de los recursos.
- La complejidad de las actividades.
- Estructura organizativa.
- Magnitud de recursos y productos.
- Giro de la empresa.
- Nivel de tecnificación alcanzado.
- Lapso y momento evolutivo de la entidad.
- Marco competitivo nacional e internacional.
- La velocidad con que se desenvuelve la entidad.

Tipos de Riesgos

Riesgo Inherente: nivel de riesgo propio de la actividad sin tener en cuenta el efecto de los controles.

$$\begin{array}{r}
 \text{Fallas} \\
 + \\
 \text{Efecto en los recursos} \\
 \hline
 \text{Riesgo Inherente}
 \end{array}$$

Riesgo Residual: nivel resultante del riesgo después de aplicar los controles.

$$\begin{array}{c} \text{Riesgo Inherente} \\ - \text{ Controles} \\ \hline \text{Riesgo Residual} \end{array}$$

2.3.3 Mapa de Riesgo

El mapa de riesgo es una gráfica que facilita la identificación del impacto y probabilidad que este tiene, esto se aprecia en la Figura 2.

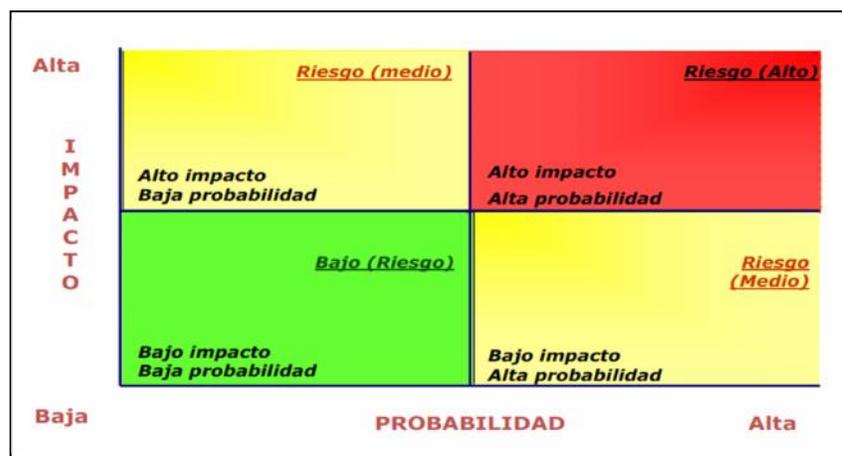


Figura 2: Mapa de Riesgo.

Fuente: (Carrión, 2013)

2.3.4 Riesgo tecnológico.

Depende de las características de cada una de las compañías, el tipo de tecnología que esté utilizando, procesos a los que ésta esté relacionada dentro de la operación.

Esto depende de la operación de cada empresa y de la constante innovación tecnológica que existe (Carrión, 2013).

2.4 COBIT 5®.

Cobit 5® es un marco de trabajo integral creado por ISACA¹ con el objeto de ayudar a las empresas a alcanzar sus objetivos para el gobierno y gestión de tecnologías corporativas, este marco busca mantener el equilibrio entre la generación de beneficios, optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012)

Cobit 5® es el resultado de la meritoria evolución de los conceptos de gestión de tecnología de información que han ido madurando a través del tiempo y respondiendo a las necesidades cambiantes del entorno empresarial, inicialmente partiendo de: COBIT 1 en 1996, con un enfoque netamente de Auditoría; Cobit 2 en 1998, que incorporó el criterio de Control; Cobit 3 en el 2000, que incursionó en el concepto de gestión, para avanzar a Cobit 4.0 en 2005 y Cobit 4.1 en 2007 con un enfoque de Gobierno; y para llegar a Cobit 5 en el 2012 con un enfoque integral de gobierno y gestión de TI. (ISACA, 2014)

La evolución que COBIT ha tenido, los enfoques y aportes de sus variantes así como el año en que se han presentado pueden observarse en la Figura 3.

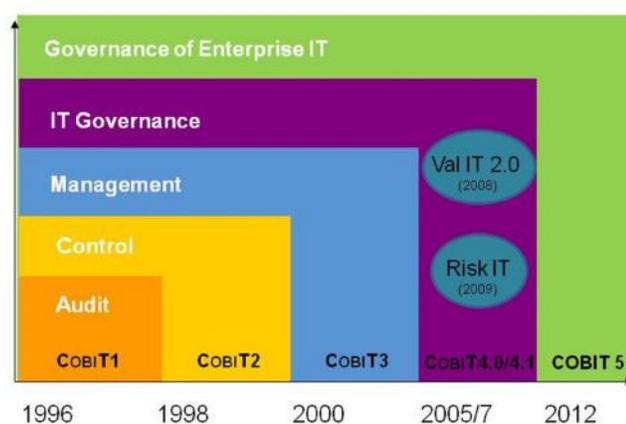


Figura 3: Evolución COBIT.

Fuente: (Castelo, 2013)

¹Information Systems Audit and Control Association en español Asociación para el Control y Auditoría de Sistemas de Información.

ISACA lideró el estudio, definición y difusión de este marco de referencia, no obstante de ello no es el único producto resultado de la preocupación de varias organizaciones como ISACA o ISO², COBIT también se nutre con otros modelos como Risk IT³ y Val IT⁴, Para su implementación puede soportarse con estándares y buenas prácticas como ITIL⁵, las series 27000 de ISO y PRINCE2⁶. (Navarro, 2012)

2.4.1 Principios de COBIT 5 ®:

COBIT 5® se basa en cinco principios claves que se detallan en la Figura 4.



Figura 4: Principios de COBIT 5.

Fuente: (ISACA, 2012)

Estos principios son los que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado además en una serie

²International Standardization Organization.

³ Risk It.- Marco de trabajo de ISACA para ayudar a las organizaciones a equilibrar los riesgos con los beneficios.

⁴ Val IT.- Marco de trabajo de gobernabilidad para crear valor de negocio de las inversiones de TI.

⁵Information Technology Infrastructure Library.

⁶PRojects IN Controlled Environments 2.

holística de siete habilitadores, que optimizan la inversión en tecnología e información así como su uso en beneficio de las partes interesadas. (ISACA, 2014)

2.4.2 Principio 1: Satisfacer las necesidades de las partes interesadas.

Las empresas se constituyen para crear valor para sus accionistas, es decir están motivadas en la obtención de beneficios, y desde luego a un costo óptimo de los recursos mientras que se optimiza el riesgo. No obstante de que los beneficios puedan tomar otra forma en relación a la naturaleza como por ejemplo los resultados financieros para empresas comerciales o el servicio público para entidades gubernamentales. De tal manera que la creación de valor se constituye un objetivo de gobierno para cualquier empresa. (ISACA, 2012)

La creación de valor se enfoca en la realización de beneficios, optimización del riesgo y optimización de recursos tal cual lo muestra la Figura 5.



Figura 5: Objetivo de Gobierno – Creación de Valor.

Fuente: (ISACA, 2012)

En este contexto COBIT 5 plantea un mecanismo para la traducción de necesidades de las partes interesadas en metas corporativas a través de la Cascada de Metas de Cobit 5, la cual emplea cuatro pasos para establecer

metas en todos los niveles y áreas de la empresa en apoyo a los objetivos generales y requisitos de las partes interesadas. Alineando así las necesidades de la empresa, las soluciones y los servicios de TI. (ISACA, 2012)

Los pasos cubren las siguientes actividades:

1. Identificación de motivos de partes interesadas y necesidades que generan.
2. Definición de metas empresariales a consecuencia de las necesidades de las partes interesadas.
3. Identificación de metas relacionadas con TI vinculadas a alcanzar las metas corporativas.
4. Identificación de catalizadores u objetivos que permitirán alcanzar los objetivos estratégicos.

2.4.3 Catalizadores:

Los catalizadores obedecen a diez y siete (17) metas corporativas que tienen relación con los objetivos de gobierno y diez y siete (17) metas relacionadas con TI, todas distribuidas en cuatro dimensiones: Financiera, Cliente, Interna y Aprendizaje/Crecimiento.

2.4.4 Principio 2: Cubrir la empresa Extremo a extremo.

Cobit 5 integra el gobierno de TI en el gobierno corporativo, es decir que cubre todas las funciones y procesos para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que la información pueda ser procesada, contemplando servicios internos/externos de TI relevantes así como procesos de negocio internos/externos. (ISACA, 2012)

Adicional a los objetivos de gobierno surgen otros elementos del enfoque de gobierno como: catalizadores, alcance y roles, actividades y relaciones que constituyen el sistema de gobierno, tal cual se puede identificar en la Figura 6.

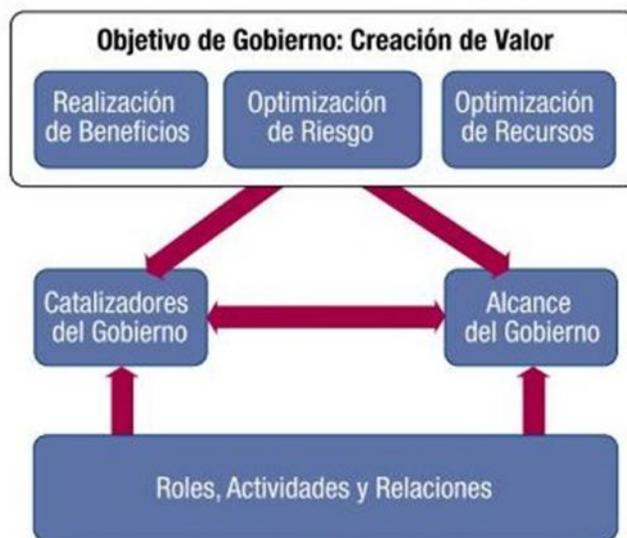


Figura 6: Gobierno y Gestión en COBIT 5.

Fuente: (ISACA, 2012)

2.4.5 Principio 3: Aplicar un marco de referencia único integrado.

Cobit 5 es un marco de referencia único e integrado porque se alinea con otros estándares y marcos de referencia, es una guía en lenguaje común y no técnico, que además integra conocimiento disperso de investigaciones de ISACA. (ISACA, 2012)

2.4.6 Principio 4: Hacer posible un enfoque holístico.

Cobit 5 logra el enfoque holístico a través de los siguientes siete catalizadores corporativos concebidos como factores que individual o colectivamente influyen sobre si algo funcionará: (ISACA, 2012)

- Procesos.
- Información
- Estructuras Organizativas.
- Principios, Políticas y Marcos.
- Cultura, Ética y Comportamientos.
- Personas, Habilidades y Competencia

- Servicios, Infraestructura y Aplicaciones.

2.4.7 Principio 5: Separar el gobierno de la gestión.

Para tratar este principio es conveniente partir de las siguientes definiciones:

“El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas”, y por otro lado “La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales”, es así que el gobierno y la gestión deben interactuar para obtener un sistema de gobierno eficiente y eficaz, empleando siete (7) catalizadores, considerando además que COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas. (ISACA, 2012)

Es así que esta especificación de gobierno y gestión en COBIT 5 dan lugar a las áreas clave ilustradas en la Figura 7.

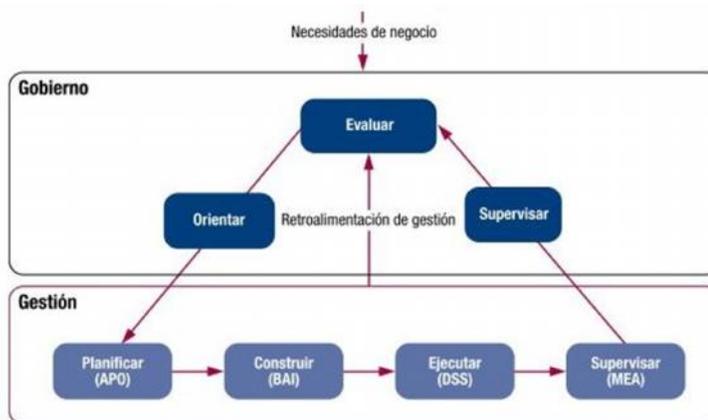


Figura 7: Áreas clave de Gobierno y Gestión en COBIT 5.

Fuente: (ISACA, 2012)

2.4.8 Procesos de COBIT 5 ®:

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

Gobierno: Contiene un dominio y cinco (5) procesos de gobierno; dentro de los cuales se definen prácticas de evaluación, orientación y supervisión.

Gestión: Contiene cuatro dominios y treinta y dos (32) procesos de gestión; con prácticas para planificar, construir, ejecutar y supervisar. (ISACA, 2012)

Los dominios de COBIT 5 Evaluar, Orientar y Supervisar (EDM); Alinear, Planificar y Organizar (APO); Construir, Adquirir e Implementar (BAI); Entregar, dar Servicio y Soporte (DSS) y Supervisar, Evaluar y Valorar (MEA) así como los procesos que los conforman se pueden identificar con mayor detalle en la Figura 8.

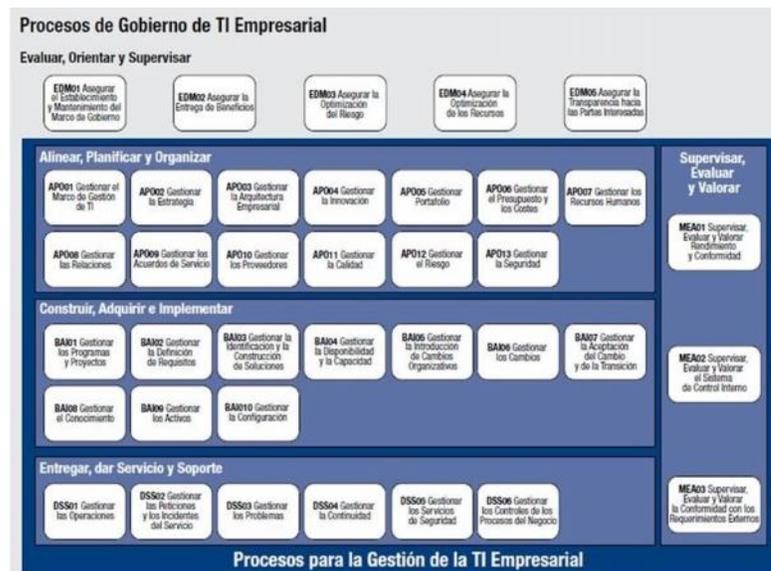


Figura 8: Modelo de Referencia de Procesos COBIT 5.

Fuente: (ISACA, 2012)

3 CAPÍTULO III: EJECUCIÓN DE LA EVALUACIÓN TECNOLÓGICA.

3.1 Marco Metodológico.

Para el presente trabajo se ha empleado el marco de referencia COBIT 5, la metodología de evaluación considera el documento Procesos Catalizadores de Cobit 5, en la cual se sugiere estudiar los procesos catalizadores, efectuando un barrido por cada uno de los procesos, en este barrido se deben observar las descripciones y propósito, tener en cuenta las metas del negocio y las metas de tecnología de información, de manera complementaria prestar especial atención en las prácticas y actividades de los procesos dentro del dominio de estudio.

Partiendo de que la existencia de un documento no reflejaría necesariamente la situación en BanCodesarrollo se ha determinado indispensable que examinar la consistencia y profundidad con la que las estrategias, políticas, procedimientos y demás instrumentos de gobierno y gestión de TI se encuentran definidos.

Por otro lado en nuestro rol de Auditores es inadmisibles llegar a una determinación subjetiva de que si se practica o cumple con el marco de referencia, razón por la que se han definido dos criterios que facilitan la valoración, estos son:

- **Evaluación.-** hace referencia a la situación de aplicabilidad de COBIT 5 dentro de BanCodesarrollo, es decir si se usan o no las actividades recomendadas por este marco de trabajo. Por lo que se le ha asignado el peso de dos (2) puntos cuando se aplica y cero (0) cuando no se lo hace.
- **Cobertura.-** se refiere al nivel de profundidad en la ejecución de las actividades sugeridas por COBIT 5, dicho de otro modo si lo conocido en las entrevistas se ve reflejado en la evidencia analizada, para lo que se han establecido tres niveles de cobertura: Completa a la que le

corresponde un peso de dos y medio (2.5) puntos, Parcial a la que se califica con uno punto setenta y cinco (1,75) y Nula a la que se le concede cero (0) puntos.

El resumen de los criterios, parámetros y puntos se puede observar en la Tabla 1.

Tabla 1
Parámetros de Evaluación

Evaluación	Valor	Cobertura	Valor
Aplica	2	Completa	2,5
No Aplica	0	Parcial	1,75
		Nula	0

Cabe destacar que producto de estos dos criterios (Evaluación*Cobertura) se tendría la posibilidad de alcanzar el puntaje mínimo de cero (0) y el máximo de cinco (5).

Con el objeto de que se refleje y facilite la labor de evaluación se ha creado una herramienta de trabajo de campo denominada "Plantilla COBIT", esta contiene la información de análisis para cada uno de los procesos en su respectivo dominio, y mediante la selección de parámetros se calcula automáticamente la puntuación para cada actividad.

Esta puntuación posteriormente se promedia con las demás actividades para obtener el resultado para la práctica y finalmente los resultados de las prácticas se promedian para alcanzar el puntaje del proceso.

Más adelante se muestran las tablas de evaluación que han sido obtenidas para cada uno de los procesos de los dominios de COBIT 5 de gobierno y gestión.

Pensando en que sería poco probable alcanzar una puntuación general máxima se ha acordado como límite mínimo aceptable de esta evaluación tres (3) puntos, consecuentemente cualquier resultado inferior a este será analizado con profundidad, a consecuencia de su baja aplicación y cobertura.

Esta evaluación tecnológica se complementa con el análisis de riesgo basado en dos aspectos:

- **Procesos COBIT de Riesgo:** En COBIT 5 existen dos procesos claramente identificables y orientados al riesgo: APO13 Gestionar el Riesgo y el proceso EDM03 Asegurar la Optimización del Riesgo.
- **Controles Implementados:** La naturaleza del negocio de BanCodesarrollo conlleva a mantener reserva respecto de la información que pueda ser divulgada, sin embargo es indispensable conocer los controles implementados para gestionar los riesgos.

3.2 Planificación del Proceso de Evaluación Tecnológica.

Para la ejecución del presente proyecto se ha ideado la planificación que guiará el proceso de evaluación tecnológica, de forma general se han previsto tres fases: Levantamiento, análisis de información e identificación de hallazgos, con actividades específicas para cada fase, las cuales se exponen a detalle en la Figura 9.

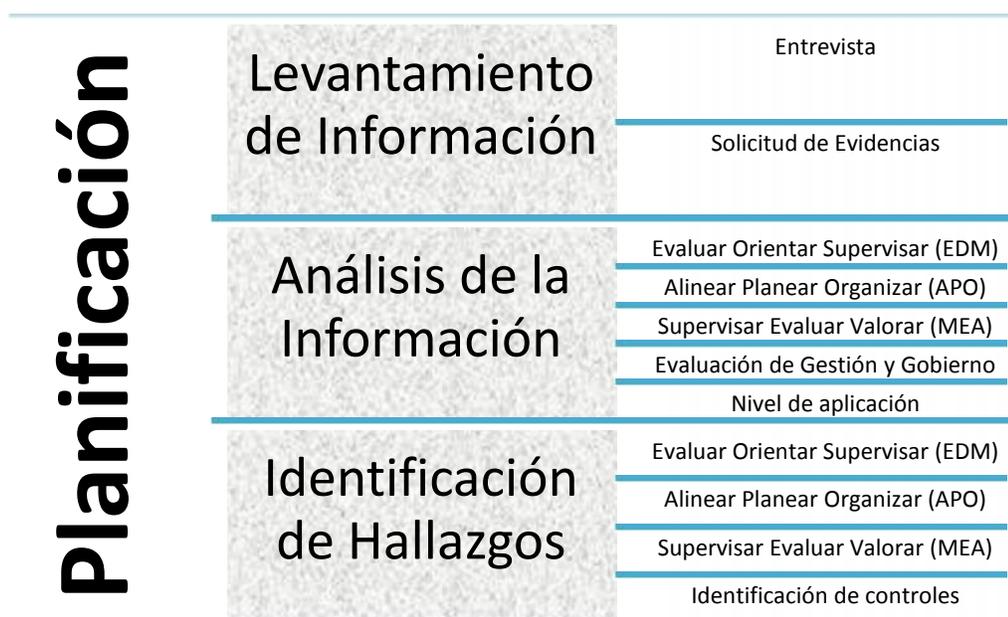


Figura 9: Planeamiento del Proceso de Evaluación Tecnológica.

3.3 Levantamiento y Recolección de Información.

El levantamiento y recolección de la información acorde con la etapa anterior “Planificación de Evaluación Tecnología” se efectuó a través de la autorización de Gerencia General de BanCodesarrollo y la coordinación con el Subgerente de Operaciones.

Lo que dio lugar al establecimiento de fechas para reuniones de trabajo y entrevistas con el personal a cargo de las áreas de:

- Producción.
- Desarrollo.
- Operaciones.
- Riesgos.
- Talento Humano.
- Seguridad Informática.

Las entrevistas realizadas al personal clave e interdisciplinario de BanCodesarrollo tenían como propósito la identificación de cada una de las actividades relativas a las labores que ejecutan, así como la identificación de documentación que debería ser solicitada para el respaldo, sustentación y evidencia de las prácticas de gobierno y gestión de tecnología en esta institución financiera.

3.3.1 Guía de Entrevistas:

La guía de entrevistas utilizada consolida los principios sobre los cuales se fundamenta COBIT 5, los dominios y procesos correspondientes a gobierno y gestión.

Como resultado de la aplicación de la guía se tiene el resumen de entrevistas, al que se lo puede revisar en el **ANEXO A: RESUMEN DE ENTREVISTAS.**

Para conocer por menores de los lineamientos, políticas, procedimientos y actividades se ha solicitado al personal de BanCodesarrollo varios materiales que aportan valiosa información al análisis, precisamente el **ANEXO B: SOLICITUD DE INFORMACIÓN** contiene el detalle de los documentos requeridos a BanCodesarrollo para complementar el análisis y evaluación.

Atendiendo a la naturaleza del trabajo y la necesidad de salvaguardar la confidencialidad de la información entregada por BanCodesarrollo, motivado además en dar a conocer los materiales que sustentan la evaluación tecnológica realizada se ha creado un documento que detalla cada uno de los documentos a los que se ha tenido acceso, estos constan en el **ANEXO C: INVENTARIO DE EVIDENCIA.**

Cabe indicar que para el efecto el equipo de trabajo primero ha identificado la necesidad y posteriormente se ha conversado con las autoridades respecto de la posibilidad de disponer de dichos materiales, algunos de los cuales han sido provistos en formato PDF y otros en formato físico para analizarlos con la debida reserva.

3.4 Análisis de la Información.

Previa a la aplicación de la “Plantilla COBIT” se llevaron a cabo lecturas, discusiones y análisis minuciosos de la información y documentación recibida,

Adicionalmente se hizo un mapeo para conocer de qué manera los diferentes miembros y estamentos de la organización participan en el gobierno y gestión acorde con los siguientes roles:

- R: Responsable de la ejecución.
- A: Quien rinde cuentas de la ejecución de tareas.
- C: A quien se le informa y consulta.
- I: A quien se informa o reporta.

Dichas matrices se ponen a disposición en el **ANEXO D: MATRICES RACI.**

Con el serio propósito de poseer un argumento confiable y no subjetivo para valorar los criterios Evaluación y Cobertura, se ha generado un documento donde figuran los procesos, prácticas y documentación analizada al que se ha denominado **ANEXO E: VALORACIÓN DE CRITERIOS**.

Atendiendo el pedido de BanCodesarrollo respecto de la confidencialidad de la información y a manera de sustentar la existencia física de los insumos utilizados para este trabajo se ha construido el **ANEXO F: DOCUMENTACIÓN DE BANCODESARROLLO**.

A continuación se muestra el detalle de la evaluación realizada a cada dominio y proceso dentro del alcance de este proyecto.

3.4.1 Dominio Evaluar/Orientar/Supervisar (EDM).

El primer dominio evaluado corresponde a Gobierno de TI y se denomina Evaluar, Orientar y Supervisar, identificado por sus siglas en inglés como EDM, a continuación se presenta la aplicación de la “Plantilla Cobit” en cada uno de los procesos.

3.4.1.1 EDM01:

La aplicación de la plantilla para el proceso EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno, se detalla en la Tabla 2.

Tabla 2
Plantilla para el proceso EDM01.

Código:	EDM01	Área:	Gobierno
Proceso:	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	Dominio:	Evaluar, Orientar y Supervisar
Descripción del Proceso:			
Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.			
Declaración del Propósito del Proceso:			

CONTINÚA →

<p>Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.</p>			
<p>El proceso apoya la consecución de un conjunto de principales metas TI:</p>			
Meta TI		Métricas relacionadas	
01 Alineamiento de TI y estrategia de negocio.		<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 	
03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.		<ul style="list-style-type: none"> • Porcentaje de roles de la dirección ejecutiva con responsabilidad claramente definida en decisiones TI. • Número de veces que TI está en la agenda del Consejo de Administración de manera proactiva. • Frecuencia de reuniones del comité ejecutivo de estrategia de TI. • Tasa de ejecución de decisiones TI ejecutivas. 	
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio		<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 	
<p>Prácticas y Actividades</p>			
EDM01.0 1	Evaluar el sistema de gobierno.	Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	4.06
Actividad	Evaluación	Cobertura	Calificación
1. Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno.	Aplica	Completa	5
2. Determinar la relevancia de TI y su papel con respecto al negocio.	Aplica	Completa	5
3. Considerar las regulaciones externas, obligaciones legales y contractuales y determinar cómo deben ser aplicadas en el gobierno de TI de la empresa.	Aplica	Parcial	3.5
4. Alinear el uso y el procesamiento ético de la información y su impacto en la sociedad, en el entorno natural y en los intereses de las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa.	Aplica	Parcial	3.5
5. Determinar las implicaciones del entorno de control conjunto de la empresa con respecto a TI.	Aplica	Parcial	3.5
6. Articular los principios que guiarán el diseño de la toma de decisiones sobre el gobierno de TI.	Aplica	Parcial	3.5
7. Comprender la cultura empresarial de la toma de decisiones y determinar un modelo óptimo en la toma de decisiones para TI.	Aplica	Parcial	3.5
8. Determinar los niveles apropiados para la delegación de autoridad, incluyendo reglas de umbrales, para las decisiones de TI.	Aplica	Completa	5

CONTINÚA →

Prácticas y Actividades			
EDM01.02	Orientar el sistema de gobierno.	Informar a los líderes y obtener su apoyo, su aceptación su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.	3.42
Actividad	Evaluación	Cobertura	Calificación
1. Comunicar los principios del gobierno de TI y acordar con el gestor ejecutivo la manera de establecer un liderazgo informado y comprometido.	Aplica	Parcial	3.5
2. Establecer o delegar el establecimiento de las estructuras, procesos y prácticas del gobierno en línea con los principios de diseño acordados.	Aplica	Parcial	3.5
3. Asignar responsabilidad, autoridad y la responsabilidad de que se apliquen los principios de diseños de gobierno, los modelos de toma de decisión y de delegación acordados.	Aplica	Completa	5
4. Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos con la responsabilidad de la supervisión y toma de decisiones.	Aplica	Parcial	3.5
5. Orientar al personal para que siga las directrices relevantes para un comportamiento ético y profesional y garantizar que las consecuencias del no cumplimiento se conocen y se respetan.	Aplica	Completa	5
6. Orientar el establecimiento de un sistema de recompensa para promover el cambio cultural deseable.	No Aplica	Nula	0
Prácticas y Actividades			
EDM01.03	Supervisar el sistema de gobierno.	Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada.	4.00
Actividad	Evaluación	Cobertura	Calificación
1. Evaluar la efectividad y rendimiento de las partes interesadas en las que se ha delegado responsabilidad y autoridad para el gobierno de TI de la empresa.	Aplica	Completa	5
2. Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.	Aplica	Completa	5
3. Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.	Aplica	Parcial	3.5
4. Mantener la supervisión sobre el punto hasta el que TI satisface las obligaciones (regulatorias, legislación, leyes comunes, contractuales), políticas internas, estándares y directrices profesionales.	Aplica	Parcial	3.5
5. Proporcionar supervisión de la efectividad de, y el cumplimiento, con el sistema de control de la empresa.	Aplica	Parcial	3.5

CONTINÚA →

6. Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.	Aplica	Parcial	3.5
--	--------	---------	-----

3.4.1.2EDM02:

La aplicación de la plantilla para el proceso EDM02: Asegurar la Entrega de Beneficios, se detalla en la Tabla 3.

Tabla 3
Plantilla para el proceso EDM02

Código:	EDM02	Área:	Gobierno
Proceso:	Asegurar la Entrega de Beneficios	Dominio:	Evaluar, Orientar y Supervisar
Descripción del Proceso:			
Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.			
Declaración del Propósito del Proceso:			
Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 		
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	<ul style="list-style-type: none"> • Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico. • Porcentaje de servicios TI donde se obtienen los beneficios esperados. • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados. 		
06 Transparencia de los costes, beneficios y riesgos de las TI.	<ul style="list-style-type: none"> • Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI 		

CONTINÚA →

07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> Número de interrupciones de negocio debidas a incidentes de servicios TI Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 		
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	<ul style="list-style-type: none"> Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. Número de iniciativas aprobadas resultantes de ideas TI innovadoras. 		
Prácticas y Actividades			
EDM02.01	<p>Evaluar la optimización de valor.</p> <p>Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.</p>	3.69	
Actividad	Evaluación	Cobertura	Calificación
1. Comprender los requerimientos de las partes interesadas; temas estratégicos de TI, tales como la dependencia de las TI; y comprender la tecnología y sus capacidades considerando la importancia actual y potencial de TI para la estrategia de la empresa.	Aplica	Parcial	3.5
2. Comprender los elementos clave de gobierno necesarios para la entrega fiable, segura y coste efectiva de un valor óptimo por el uso de los servicios, activos y recursos de TI existentes y potenciales.	Aplica	Completa	5
3. Comprender y discutir regularmente las oportunidades que podrían surgir de los cambios habilitados en la empresa por las tecnologías actuales, nuevas o emergentes y optimizar el valor creado por estas oportunidades.	Aplica	Parcial	3.5
4. Comprender lo que se entiende por valor en la empresa y considerar cómo de bien se ha comunicado, comprendido y aplicado a través de los procesos de la empresa.	Aplica	Parcial	3.5
5. Evaluar la efectividad de la integración y alineamiento de las estrategias de TI en la empresa y con los objetivos de la empresa para aportar valor.	Aplica	Parcial	3.5
6. Comprender y considerar cómo de efectivos son los roles, responsabilidades, asignaciones y organismos de toma de decisiones actuales asegurando la creación de valor de las inversiones, servicios y activos de TI.	Aplica	Parcial	3.5
7. Considerar cómo de bien alineada está la gestión de las inversiones, servicios y activos de TI con la gestión de valor y las prácticas de gestión financiera.	Aplica	Parcial	3.5
8. Evaluar la alineación del portafolio de inversiones, servicios y activos con los objetivos estratégicos de la empresa; con el valor de la empresa financiero y no financiero; con el riesgo, tanto de servicio como al del beneficio; con los procesos de negocio; la efectividad en términos de usabilidad, disponibilidad y responsabilidad; y eficiencia en términos de coste, redundancia y salud técnica.	Aplica	Parcial	3.5
Prácticas y Actividades			

CONTINÚA →

EDM02.02	Orientar la optimización del valor.	Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico.	3.00
Actividad	Evaluación	Cobertura	Calificación
1. Definir y comunicar la cartera y los tipos de inversión, categorías, criterios y ponderaciones relativas a los criterios que permitan puntuaciones de valores relativos.	Aplica	Parcial	3.5
2. Definir los requerimientos para los cambios de fase (stage-gate) y otras revisiones por la importancia de la inversión para la empresa y el riesgo asociado, cronograma del programa, planes de financiación y la entrega de capacidades clave y beneficios y la contribución continuada al valor.	Aplica	Parcial	3.5
3. Orientar a la dirección para considerar usos potenciales de TI innovadoras que posibiliten que la empresa responda a nuevas oportunidades y desafíos, lleve a cabo nuevos negocios, incremente la competitividad o mejore sus procesos.	Aplica	Parcial	3.5
4. Orientar los cambios necesarios en la asignación de imputaciones y responsabilidades en la ejecución del portafolio de inversiones y la entrega de valor a partir de los servicios y procesos de negocio.	Aplica	Parcial	3.5
5. Definir y comunicar a nivel de empresa los objetivos de entrega de valor y las medidas de resultados para permitir un control eficaz.	Aplica	Parcial	3.5
6. Orientar los cambios necesarios en la cartera de inversiones y servicios para realinearlos con los objetivos de la empresa actuales y esperados y/o sus limitaciones	Aplica	Parcial	3.5
7. Recomendar la consideración de innovaciones potenciales, cambios organizativos o mejoras operativas que desde las iniciativas TI pudieran impulsar un incremento de valor para la empresa.	No Aplica	Nula	0
Prácticas y Actividades			
EDM02.03	Supervisar la optimización de valor.	Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Identificar los problemas significativos y considerar las acciones correctivas.	4.40
Actividad	Evaluación	Cobertura	Calificación
1. Definir un conjunto equilibrado de objetivos de desempeño, métricas, metas y puntos de referencia. Las métricas deberían cubrir la actividad y la medida de resultados, incluyendo los indicadores de retardo y de avance de los resultados, así como un equilibrio adecuado de las medidas financieras y no financieras. Revisarlos y acordarlos con las funciones de TI y de negocio, y otras partes interesadas relevantes.	Aplica	Parcial	3.5
2. Recoger los datos pertinentes, oportunos, completos, fiables y precisos para informar sobre los avances en la entrega de valor respecto a los objetivos. Obtener una sucinta, de alto nivel, completa vista de la cartera, programa y desempeño TI (capacidades técnicas y operativas) que soporten la toma de decisiones y aseguren que los resultados esperados se están logrando.	Aplica	Parcial	3.5

CONTINÚA →

3. Conseguir informes habituales y relevantes de la cartera, programa y desempeño de TI (tecnológico y funcional). Revisar el progreso de la empresa hacia los objetivos identificados y el grado en el que los objetivos previstos son alcanzados, los entregables obtenidos, los objetivos de rendimiento alcanzados y el riesgo mitigado.	Aplica	Completa	5
4. Tras la revisión de los informes, tomar las medidas de gestión apropiadas según sea necesario para asegurar que el valor sea optimizado.	Aplica	Completa	5
5. Tras la revisión de los informes, asegúrese de que las medidas correctivas apropiadas son iniciadas y controladas.	Aplica	Completa	5

3.4.1.3EDM03:

La aplicación de la plantilla para el proceso EDM03: Asegurar la Optimización del Riesgo, se detalla en la Tabla 4.

Tabla 4

Plantilla para el proceso EDM03.

Código:	EDM03	Área:	Gobierno
Proceso:	Asegurar la Optimización del Riesgo	Dominio:	Evaluar, Orientar y Supervisar
Descripción del Proceso:			
Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.			
Declaración del Propósito del Proceso:			
Asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI. • Frecuencia de actualización del perfil de riesgo. 		
06 Transparencia de los costes, beneficios y riesgos de las TI.	<ul style="list-style-type: none"> • Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI 		

CONTINÚA →

10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones.	<ul style="list-style-type: none"> Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública. Número de servicios TI sin requerimientos de seguridad destacables. Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados. Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías 		
15	Cumplimiento de las políticas internas por parte de las TI.	<ul style="list-style-type: none"> Número de incidentes relacionados con el incumplimiento de políticas. Porcentaje de interesados que entienden las políticas. Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas. Frecuencia de revisión y actualización de políticas 		
Prácticas y Actividades				
EDM03.01	Evaluar la gestión de riesgos.	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	3.75	
Actividad		Evaluación	Cobertura	Calificación
1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).		Aplica	Completa	5
2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.		Aplica	Parcial	3.5
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.		Aplica	Parcial	3.5
4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.		Aplica	Parcial	3.5
5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.		Aplica	Parcial	3.5
6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las pérdidas relacionadas con TI y la tolerancia de los líderes a los mismos.		Aplica	Parcial	3.5
Prácticas y Actividades				
EDM03.02	Orientar la gestión de riesgos.	Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.	3.42	
Actividad		Evaluación	Cobertura	Calificación
1. Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.		Aplica	Completa	5
2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.		Aplica	Parcial	3.5
3. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.		Aplica	Parcial	3.5

CONTINÚA →

4. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).	Aplica	Completa	5
5. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.	Aplica	Parcial	3.5
6. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.	No Aplica	Nula	0
Prácticas y Actividades			
EDM03.03	Supervisar la gestión de riesgos.	Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	3.38
Actividad	Evaluación	Cobertura	Calificación
1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.	Aplica	Parcial	3.5
2. Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.	No Aplica	Nula	0
3. Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.	Aplica	Completa	5
4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.	Aplica	Completa	5

3.4.1.4EDM04:

La aplicación de la plantilla para el proceso EDM04: Asegurar la Optimización de los Recursos, se detalla en la Tabla 5.

Tabla 5

Plantilla para el proceso EDM04

Código:	EDM04	Área:	Gobierno
Proceso:	Asegurar la Optimización de los Recursos	Dominio:	Evaluar, Orientar y Supervisar
Descripción del Proceso:			
Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.			
Declaración del Propósito del Proceso:			
Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.			
El proceso apoya la consecución de un conjunto de principales metas TI:			

CONTINÚA →

Meta TI		Métricas relacionadas		
09 Agilidad de las TI.		<ul style="list-style-type: none"> Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos. Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas. Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada. 		
11 Optimización de activos, recursos y capacidades de las TI.		<ul style="list-style-type: none"> 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 la alta dirección del negocio y de TI con los costes y capacidades TI. 		
16 Personal del negocio y de las TI competente y motivado.		<ul style="list-style-type: none"> Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles. Porcentaje de personal satisfecho con sus roles en TI. Número de horas de aprendizaje/ formación por miembro del personal. 		
Prácticas y Actividades				
EDM04.01	Evaluar la gestión de recursos.	Evaluar la gestión de recursos. Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa.	3.80	
Actividad		Evaluación	Cobertura	Calificación
1. Examinar y evaluar la estrategia actual y futura, las opciones de aprovisionamiento de recursos TI y desarrollar capacidades para cubrir las necesidades actuales y futuras (incluyendo alternativas de aprovisionamiento).		Aplica	Parcial	3.5
2. Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI puedan satisfacer las necesidades de la empresa, con la habilidad y capacidad requerida de acuerdo a las prioridades acordadas y las limitaciones presupuestarias.		Aplica	Parcial	3.5
3. Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la empresa para la entrega de valor y la mitigación de riesgos con los recursos asignados.		Aplica	Parcial	3.5
4. Comprender los requisitos para alinear la gestión de recursos con la planificación de recursos empresariales financieros y humanos.		Aplica	Completa	5
5. Definir los principios para la gestión y el control de la arquitectura de la empresa.		Aplica	Parcial	3.5
Prácticas y Actividades				
EDM04.02	Orientar la gestión de recursos.	Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica.	4.10	
Actividad		Evaluación	Cobertura	Calificación
1. Comunicar e impulsar la adopción de estrategias de gestión de recursos, principios y el plan de recursos y las estrategias de arquitectura de empresa acordados.		Aplica	Parcial	3.5
2. Asignar responsabilidades para la ejecución de la gestión de recursos.		Aplica	Completa	5

CONTINÚA →

3. Definir los objetivos, medidas y métricas clave para la gestión de los recursos		Aplica	Parcial	3.5
4. Establecer los principios relacionados con la protección de recursos.		Aplica	Parcial	3.5
5. Alinear la gestión de recursos con la planificación de RRHH y financiera de la empresa.		Aplica	Completa	5
Prácticas y Actividades				
EDM04.03	Supervisar la gestión de recursos.	Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.		3.50
Actividad		Evaluación	Cobertura	Calificación
1. Supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la empresa mediante objetivos y métricas acordados.		Aplica	Parcial	3.5
2. Supervisar las estrategias de aprovisionamiento TI y de arquitectura de la empresa y los recursos y capacidades TI para garantizar que las necesidades actuales y futuras de la empresa puedan ser satisfechas.		Aplica	Parcial	3.5
3. Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes.		Aplica	Parcial	3.5

3.4.1.5 EDM05:

La aplicación de la plantilla para el proceso EDM05: Asegurar la Transparencia hacia las Partes Interesadas, se detalla en la Tabla 6.

Tabla 6

Plantilla para el proceso EDM05

Código:	EDM05	Área:	Gobierno
Proceso:	Asegurar la Transparencia hacia las Partes Interesadas	Dominio:	Evaluar, Orientar y Supervisar
Descripción del Proceso:			
Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.			
Declaración del Propósito del Proceso:			
Asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		

CONTINÚA →

03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.		<ul style="list-style-type: none"> • Porcentaje de roles de la dirección ejecutiva con responsabilidad claramente definida en decisiones TI. • Número de veces que TI está en la agenda del Consejo de Administración de manera proactiva. • Frecuencia de reuniones del comité ejecutivo de estrategia de TI. • Tasa de ejecución de decisiones TI ejecutivas. 	
06 Transparencia de los costes, beneficios y riesgos de las TI.		<ul style="list-style-type: none"> • Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI 	
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio		<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 	
Prácticas y Actividades			
EDM05.01	Evaluar los requisitos de elaboración de informes de las partes interesadas.	Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación.	3.50
Actividad	Evaluación	Cobertura	Calificación
1. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes respecto al uso de TI dentro de la empresa (regulación, legislación, leyes generales, requisitos contractuales), incluyendo alcance y frecuencia.	Aplica	Parcial	3.5
2. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes para otros interesados respecto al uso de TI dentro de la empresa, incluyendo alcance y condiciones.	Aplica	Parcial	3.5
3. Mantener los principios de comunicación con interesados externos e internos, incluyendo formatos y canales de comunicación y los principios de aceptación y aprobación de los informes por parte de las partes interesadas.	Aplica	Parcial	3.5
Prácticas y Actividades			
EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.	3.50
Actividad	Evaluación	Cobertura	Calificación
1. Orientar el establecimiento de la estrategia de comunicación para interesados externos e internos.	Aplica	Parcial	3.5
2. Orientar la implementación de mecanismos para garantizar que la información cumple todos los criterios de los requisitos corporativos obligatorios en cuanto a elaboración de informes de TI.	Aplica	Parcial	3.5

CONTINÚA →

3. Establecer mecanismos de validación y aprobación de la elaboración obligatoria de informes.		Aplica	Parcial	3.5
4. Establecer mecanismos de escalado en la elaboración de informes.		Aplica	Parcial	3.5
Prácticas y Actividades				
EDM05.03	Supervisar la comunicación con las partes interesadas.	Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.		3.50
Actividad		Evaluación	Cobertura	Calificación
1. Evaluar periódicamente la eficacia de los mecanismos para asegurar la precisión y la fiabilidad de la elaboración obligatoria de informes.		Aplica	Parcial	3.5
2. Evaluar periódicamente la eficacia de los mecanismos y las salidas de la comunicación con interesados externos e internos.		Aplica	Parcial	3.5
3. Determinar si se están cumpliendo los requisitos de los diferentes interesados.		Aplica	Parcial	3.5

3.4.2 Dominio Alinear/Planear/Organizar (APO).

El segundo dominio pertenece a Gestión de TI y se denomina Alinear, Planear y Organizar, identificado por sus siglas en inglés como APO, a continuación se desarrolla la evaluación para los procesos que lo conforman.

El segundo dominio pertenece a Gestión de TI y se denomina Alinear, Planear y Organizar, identificado por sus siglas en inglés como APO, a continuación se desarrolla la evaluación para los procesos que lo conforman.

3.4.2.1 APO01:

La aplicación de la plantilla para el proceso APO01: Gestionar el Marco de Gestión TI, se detalla en la Tabla 7.

Tabla 7

Plantilla para el proceso APO01

Código:	APO01	Área:	Gestión
Proceso:	Gestionar el Marco de Gestión de TI	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.			
Declaración del Propósito del Proceso:			
Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 		

CONTINÚA →

02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	<ul style="list-style-type: none"> • Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación. • Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos. • Número de incumplimientos relacionados con proveedores de servicios TI. • Cobertura de evaluaciones de cumplimiento. 		
09 Agilidad de las TI.	<ul style="list-style-type: none"> • Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos. • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas. • Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada. 		
11 Optimización de activos, recursos y capacidades de las TI.	<ul style="list-style-type: none"> • 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 la alta dirección del negocio y de TI con los costes y capacidades TI. 		
15 Cumplimiento de las políticas internas por parte de las TI.	<ul style="list-style-type: none"> • Número de incidentes relacionados con el incumplimiento de políticas. • Porcentaje de interesados que entienden las políticas. • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas. • Frecuencia de revisión y actualización de políticas 		
16 Personal del negocio y de las TI competente y motivado.	<ul style="list-style-type: none"> • Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles. • Porcentaje de personal satisfecho con sus roles en TI. • Número de horas de aprendizaje/ formación por miembro del personal. 		
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	<ul style="list-style-type: none"> • Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas TI innovadoras. 		
Prácticas y Actividades			
APO01.0 1	Definir la estructura organizativa	Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.	4.88
Actividad	Evaluación	Cobertura	Calificación
1. Definir el alcance, las funciones internas y externas, los roles internos y externos, y las capacidades y los derechos de decisión requeridos, incluidas actividades de TI realizadas por terceras partes.	Aplica	Completa	5
2. Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la gestión y ejecución de servicios de TI.	Aplica	Parcial	3.5
3. Establecer la implicación de las partes interesadas críticas para la toma de decisiones (quiénes rendirán cuentas, quiénes son responsables, quiénes deben ser consultados y quiénes informados).	Aplica	Completa	5
4. Alinear la organización relativa a TI con los modelos organizativos de arquitectura corporativa.	Aplica	Completa	5
5. Definir el enfoque, los roles y las responsabilidades de cada función dentro de la estructura organizativa relativa a TI.	Aplica	Completa	5

CONTINÚA →

6. Definir las estructuras y relaciones de gestión para contribuir a las funciones y roles de gestión y ejecución, en consonancia con la dirección de gobierno establecida.		Aplica	Completa	5
7. Establecer un Comité Estratégico de TI (o equivalente) a nivel del Consejo de Administración. Este comité debería asegurarse de que el gobierno de TI, como parte del gobierno corporativo, está contemplado de forma adecuada, debe aconsejar sobre la dirección estratégica y revisar las inversiones principales, en representación del consejo de administración al completo.		Aplica	Completa	5
8. Establecer un comité directivo de TI (o equivalente) compuesto por la dirección ejecutiva, de negocio y de TI para determinar las prioridades de los programas de inversión de TI de acuerdo con la estrategia y prioridades de negocio de la empresa; realizar un seguimiento del estado de los proyectos y resolver los conflictos de recursos; y supervisar los niveles de servicio y las mejoras en el servicio.		Aplica	Completa	5
9. Proporcionar directrices para cada estructura de gestión (incluyendo órdenes, objetivos, asistentes a reuniones, marco temporal, seguimiento, supervisión y vigilancia), así como las entradas requeridas y las salidas esperadas en cuanto a las reuniones.		Aplica	Completa	5
10. Definir reglas básicas de comunicación mediante la identificación de las necesidades comunicativas y la implementación de planes basados en dichas necesidades, teniendo en cuenta la comunicación de arriba hacia abajo, de abajo hacia arriba y horizontal.		Aplica	Completa	5
11. Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre el negocio y las funciones de TI dentro de la empresa y con entidades no pertenecientes a la empresa.		Aplica	Completa	5
12. Verificar regularmente la adecuación y la eficacia de la estructura organizativa.		Aplica	Completa	5
APO01.0 2	Establecer roles y responsabilidades	Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.		5.00
Actividad		Evaluación	Cobertura	Calificación
1. Establecer, acordar y comunicar roles y responsabilidades relativos a TI para todo el personal de la empresa, de acuerdo con las necesidades y los objetivos del negocio. Delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones.		Aplica	Completa	5
2. Tener en cuenta los requisitos desde la empresa y la continuidad del servicio de TI a la hora de definir los roles, incluyendo el respaldo por parte de la plantilla y los requisitos de formación interdisciplinar.		Aplica	Completa	5
3. Contribuir al proceso de continuidad del servicio de TI manteniendo actualizada la información de contacto y las descripciones de roles de la empresa.		Aplica	Completa	5
4. Incluir en las descripciones de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales.		Aplica	Completa	5

CONTINÚA →

5. Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. El nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas.		Aplica	Completa	5
6. Asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades.		Aplica	Completa	5
7. Estructurar los roles y las responsabilidades para reducir las posibilidades de que un solo rol pueda comprometer un proceso crítico.		Aplica	Completa	5
APO01.0 3	Mantener los elementos catalizadores del sistema de gestión	Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos.		4.50
Actividad	Evaluación	Cobertura	Calificación	
1. Adquirir comprensión de la visión, la dirección y la estrategia corporativas.	Aplica	Parcial	3.5	
2. Tener en cuenta el entorno interno de la empresa, incluyendo la cultura y la filosofía de gestión, la tolerancia al riesgo, la seguridad, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de integridad en la gestión.	Aplica	Completa	5	
3. Inferir e integrar los principios de TI con los principios de negocio.	Aplica	Parcial	3.5	
4. Alinear el entorno de control de TI con el entorno de políticas de TI, con los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control. Evaluar las buenas prácticas o los requisitos específicos del sector (p. ej., normativa específica del sector) e integrarlos donde corresponda.	Aplica	Parcial	3.5	
5. Alinearse con todos los estándares y códigos de práctica de gobierno y gestión aplicables a nivel nacional e internacional y evaluar buenas prácticas disponibles, como el Marco de Trabajo Integrado para Control Interno de COSO y el Marco de Trabajo Integrado para Gestión Empresarial del Riesgo de COSO.	Aplica	Completa	5	
6. Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.	Aplica	Completa	5	
7. Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativo o de negocio.	Aplica	Completa	5	
8. Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.	Aplica	Completa	5	
9. Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.	Aplica	Completa	5	
APO01.0 4	Comunicar los objetivos y la dirección de gestión	Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa.		5.00

CONTINÚA →

Actividad		Evaluación	Cobertura	Calificación
1. Comunicar continuamente los objetivos y la dirección de TI. Asegurar que las comunicaciones reciban apoyo de la dirección ejecutiva, tanto de palabra como mediante acciones, empleando todos los canales disponibles.		Aplica	Completa	5
2. Garantizar que la información comunicada engloba una clara articulación de la misión, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código ético/de conducta, las políticas y procedimientos, los roles y las responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado para cada respectiva audiencia dentro de la empresa.		Aplica	Completa	5
3. Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo.		Aplica	Completa	5
APO01.0 5	Optimizar la ubicación de la función de TI	Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte del CIO debe ser proporcional a la importancia de las TI en la empresa.		5.00
Actividad		Evaluación	Evidencia	Calificación
1. Entender el contexto de la función de TI, incluyendo una evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, híbrido), importancia de TI, la situación y opciones para la provisión.		Aplica	Completa	5
2. Identificar, evaluar y priorizar las opciones para la ubicación en la organización, los modelos operativos y de aprovisionamiento.		Aplica	Completa	5
3. Definir la ubicación de la función de TI y obtener aprobación.		Aplica	Completa	5
APO01.0 6	Definir la propiedad de la información (datos) y del sistema	Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.		4.25
Actividad		Evaluación	Cobertura	Calificación
1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa.		Aplica	Parcial	3.5
2. Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario.		Aplica	Parcial	3.5
3. Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.		Aplica	Completa	5
4. Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (data warehouses) y archivos de datos.		Aplica	Completa	5

CONTINÚA →

APO01.07	Gestionar la mejora continua de los procesos	Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso.	0.00	
Actividad		Evaluación	Cobertura	Calificación
1. Identificar los procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora. Analizar las diferencias en la capacidad y control del proceso. Identificar las opciones de mejora y rediseño de procesos. Priorizar iniciativas para la mejora de procesos basadas en el potencial coste-beneficio.		No Aplica	Parcial	0
2. Implementar las mejoras acordadas, funcionando como una práctica normal del negocio y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.		No Aplica	Parcial	0
3. Considerar las maneras de mejorar la eficiencia y eficacia (p. ej., mediante formación, documentación, estandarización y automatización de procesos).		Aplica	Nula	0
4. Aplicar prácticas de gestión de calidad para la actualización de procesos.		No Aplica	Nula	0
5. Retirar procesos, componentes o catalizadores desactualizados.		No Aplica	Nula	0
APO01.08	Mantener el cumplimiento con las políticas y procedimientos	Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control.	4.10	
Actividad		Evaluación	Cobertura	Calificación
1. Hacer un seguimiento del cumplimiento con políticas y procedimientos.		Aplica	Parcial	3.5
2. Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir el cambio de requerimientos).		Aplica	Parcial	3.5
3. Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.		Aplica	Completa	5
4. Evaluar periódicamente el desempeño de los catalizadores del marco de referencia y adoptar las acciones necesarias.		Aplica	Parcial	3.5
5. Analizar las tendencias en el funcionamiento y cumplimiento y adoptar las acciones apropiadas.		Aplica	Completa	5

3.4.2.2APO02:

La aplicación de la plantilla para el proceso APO02: Gestionar la estrategia, se detalla en la Tabla 8.

Tabla 8

Plantilla para el proceso APO02

Código:	APO02		Área:	Gestión
Proceso:	Gestionar la Estrategia		Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:				
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.				
Declaración del Propósito del Proceso:				
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.				
El proceso apoya la consecución de un conjunto de principales metas TI:				
Meta TI	Métricas relacionadas			
01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 			
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 			
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	<ul style="list-style-type: none"> • Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas TI innovadoras. 			
Prácticas y Actividades				
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 (motivadores de la industria, reglamentos relevantes, bases para la competencia).	4.50	
Actividad	Evaluación	Cobertura	Calificación	
1. Desarrollar y mantener un entendimiento de las estrategias y objetivos del negocio, así como del entorno y los retos operativos actuales.	Aplica	Completa	5	
2. Desarrollar y mantener un entendimiento del entorno externo a la empresa.	Aplica	Parcial	3.5	
3. Identificar las partes interesadas más importantes y obtener comprensión de sus requerimientos.	Aplica	Completa	5	
4. Identificar y analizar las fuentes de los cambios en la empresa y en el entorno externo.	Aplica	Completa	5	
5. Determinar prioridades para el cambio estratégico.	Aplica	Completa	5	

CONTINÚA →

6. Entender la actual arquitectura de empresa y trabajar con el proceso de arquitectura de empresa para determinar cualquier brecha potencial en la arquitectura.		Aplica	Parcial	3.5
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.		4.63
Actividad		Evaluación	Cobertura	Calificación
1. Desarrollar un punto de referencia del negocio, entorno de TI, capacidades y servicios actuales respecto al que las necesidades futuras puedan ser comparadas. Incluir el correspondiente detalle, a alto nivel, de la arquitectura empresarial actual (negocios, información, datos, aplicaciones y dominios de tecnología), procesos de negocio, procesos de TI y sus procedimientos, estructura organizativa de TI, provisión de servicios externos, gobierno de TI, habilidades y competencias de TI en toda la empresa.		Aplica	Completa	5
2. Identificar los actuales y potenciales riesgos y tecnologías en declive.		Aplica	Completa	5
3. Identificar diferencias entre el negocio actual y las capacidades de TI, entre servicios y estándares y mejores prácticas de referencia, entre empresas competidoras y sus capacidades de TI y entre un análisis comparativo de las mejoras prácticas y la provisión de servicios emergentes de TI.		Aplica	Parcial	3.5
4. Identificar los problemas, fortalezas, oportunidades y amenazas en el entorno actual, las capacidades y servicios para entender el desempeño actual. Identificar las áreas a mejorar en términos de la contribución de TI a los objetivos del negocio.		Aplica	Completa	5
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.		4.00
Actividad		Evaluación	Cobertura	Calificación
1. Considerar la aprobación de tecnologías emergentes e ideas innovadoras.		Aplica	Parcial	3.5
2. Identificar las amenazas por el rechazo a las actuales y nuevas tecnologías adquiridas.		Aplica	Completa	5
3. Definir los objetivos/metas de TI a alto nivel y cómo contribuirán a los objetivos de negocio empresariales.		Aplica	Completa	5
4. Definir el proceso de negocio requerido y deseado, las capacidades y los servicios de TI; describir los cambios a alto nivel en la arquitectura empresarial (negocio, información, datos, aplicaciones y dominios tecnológicos), el negocio, los procesos y procedimientos de TI, la estructura organizativa de TI, proveedores de servicios tecnológicos, gobierno de TI y las habilidades y competencias.		Aplica	Parcial	3.5
5. Alinear y acordar los cambios en la arquitectura de empresa con el arquitecto corporativo.		Aplica	Parcial	3.5

CONTINÚA →

6. Demostrar trazabilidad de la estrategia del negocio y sus necesidades.		Aplica	Parcial	3.5
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.		3.50
Actividad		Evaluación	Cobertura	Calificación
1. Identificar todas las diferencias y cambios necesarios para realizar en el entorno deseado.		Aplica	Parcial	3.5
2. Considerar las implicaciones a alto nivel de todas las diferencias. Considerar el valor de los posibles cambios en el negocio y capacidades de TI, servicios de TI y arquitectura empresarial y las consecuencias de no realizarlos.		Aplica	Parcial	3.5
3. Evaluar el impacto de posibles cambios en el negocio y en los modelos operativos de TI, la capacidad de investigación y desarrollo de tecnología y los programas de inversión de TI.		Aplica	Parcial	3.5
4. Mejorar la definición del entorno deseado y preparar una declaración de valor con los beneficios a percibir de ese entorno.		Aplica	Parcial	3.5
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.		3.93
Actividad		Evaluación	Cobertura	Calificación
1. Definir las iniciativas necesarias para cerrar las diferencias y migrar del entorno actual al deseado, incluyendo el presupuesto de inversión/operativo, fuentes de financiación y estrategia de provisión.		Aplica	Parcial	3.5
2. Identificar y abordar adecuadamente los riesgos, costes e implicaciones de los cambios organizativos, evolución tecnológica, requisitos normativos, reingeniería de los procesos de negocio, dotación de personal, oportunidades de internalización (insourcing) y externalización (outsourcing), etc., en el proceso de planificación.		Aplica	Parcial	3.5
3. Determinar dependencias, solapamientos, sinergias e impactos entre las iniciativas y priorizar las iniciativas.		Aplica	Parcial	3.5
4. Identificar los requerimientos de recursos, planificación y presupuestos de inversión/operacional de cada iniciativa.		Aplica	Parcial	3.5
5. Crear una hoja de ruta indicando la planificación y las interdependencias de las iniciativas.		Aplica	Parcial	3.5
6. Traducir los objetivos en medidas de resultado representadas por métricas (qué) y objetivos (cuánto) que puedan ser relacionados con los beneficios empresariales.		Aplica	Completa	5
7. Obtener formalmente soporte de las partes interesadas y obtener aprobación del plan.		Aplica	Completa	5

CONTINÚA →

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.	3.50	
Actividad		Evaluación	Cobertura	Calificación
1. Desarrollar y mantener una red de aprobación, apoyo e impulso de la estrategia de TI.		Aplica	Parcial	3.5
2. Desarrollar un plan de comunicación que cubra los mensajes necesarios, audiencias objetivo, mecanismos/canales de comunicación y horarios.		Aplica	Parcial	3.5
3. Preparar un paquete de comunicaciones que entregue el plan de manera eficaz utilizando los medios de comunicación y tecnologías disponibles.		Aplica	Parcial	3.5
4. Obtener realimentación y actualizar el plan de comunicaciones y de entrega según sea necesario.		Aplica	Parcial	3.5

3.4.2.3APO03:

La aplicación de la plantilla para el proceso APO03: Administrar la Arquitectura Empresarial, se detalla en la Tabla 9.

Tabla 9

Plantilla para el proceso APO03

Código:	APO03	Área:	Gestión
Proceso:	Administrar la Arquitectura Empresarial	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
<p>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 mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.</p>			
Declaración del Propósito del Proceso:			
<p>Representar 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.</p>			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 		
09 Agilidad de las TI.	<ul style="list-style-type: none"> • Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos. • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas. • Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada. 		
11 Optimización de activos, recursos y capacidades de las TI.	<ul style="list-style-type: none"> • 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 la alta dirección del negocio y de TI con los costes y capacidades TI. 		
Prácticas y Actividades			

CONTINÚA →

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 la preocupaciones de las partes interesadas en su implementación.	3.63
Actividad	Evaluación	Cobertura	
1. Identificar a las partes interesadas clave de la empresa y sus objetivos/preocupaciones y definir los requisitos clave de la empresa a ser considerados, así como la visión de la arquitectura a ser desarrollada para satisfacer los distintos requisitos de las partes interesadas.	Aplica	Parcial	3.5
2. Identificar los objetivos y los impulsores estratégicos de la empresa y definir las limitaciones con las que habrá que tratar, incluyendo las limitaciones en toda la empresa y las específicas del proyecto (duración, planificación, recursos, etc.).	Aplica	Parcial	3.5
3. Alinear los objetivos de la arquitectura con las prioridades estratégicas del plan empresarial.	Aplica	Completa	5
4. Entender los deseos y las capacidades del negocio y, a continuación, identificar las opciones para realizar dichas capacidades.	Aplica	Parcial	3.5
5. Evaluar la disposición de la empresa para el cambio.	Aplica	Parcial	3.5
6. Definir qué está dentro y qué está fuera del alcance de la arquitectura de partida y los esfuerzos de arquitectura objetivo, entendiendo que el punto de partida y el objetivo no necesitan ser descritos con el mismo nivel de detalle.	Aplica	Parcial	3.5
7. Confirmar y elaborar los principios de la arquitectura, incluyéndose los principios de la empresa. Asegurarse de que todas las definiciones existentes están vigentes y aclarar cualquier área de ambigüedad.	Aplica	Parcial	3.5
8. Entender los objetivos estratégicos actuales de la empresa y trabajar conjuntamente con el procesos de planificación estratégica para asegurarse que las oportunidades de arquitectura de TI empresarial se apoyan en el desarrollo del plan estratégico.	Aplica	Parcial	3.5
9. Crear la visión de la arquitectura atendiendo a las preocupaciones de las partes interesadas, en los requisitos de capacidad del negocio, en el alcance, en las limitaciones y principios: visión de alto nivel de las arquitecturas de partida y objetivo.	Aplica	Parcial	3.5
10. Definir las proposiciones de valor, los objetivos y métricas de la arquitectura objetivo.	Aplica	Parcial	3.5
11. Identificar los riesgos empresariales asociados con el cambio de la nueva visión de la arquitectura, evaluar el nivel de riesgo inicial (por ejemplo, crítico, marginal o despreciable) y desarrollar una estrategia de mitigación para cada riesgo importante.	Aplica	Parcial	3.5

CONTINÚA →

12. Desarrollar el caso de negocio del concepto de arquitectura empresarial, bosquejar los planes y el trabajo de arquitectura y asegurar que están aprobados para iniciar el proyecto que esté alineado e integrado con la estrategia empresarial.		Aplica	Parcial	3.5
APO03.02	Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios de negocio, información, datos, aplicaciones y tecnología.		3.28
Actividad		Evaluación	Cobertura	Calificación
1. Mantener un repositorio de la arquitectura que contenga los estándares, los componentes reutilizables, el modelado, las relaciones, las dependencias y las vistas para permitir una uniformidad en la organización y el mantenimiento.		Aplica	Parcial	3.5
2. Seleccionar los puntos de vista de referencia del repositorio de arquitectura que permitirán al arquitecto demostrar cómo están siendo consideradas las preocupaciones de las partes interesadas en la arquitectura.		Aplica	Parcial	3.5
3. Por cada punto de vista, seleccionar los modelos necesarios para soportar cada uno de ellos, utilizando las herramientas o métodos seleccionados y los niveles apropiados de descomposición.		Aplica	Parcial	3.5
4. Desarrollar descripciones de dominio de arquitectura de partida, utilizando el alcance y nivel de detalle necesarios para apoyar la arquitectura objetivo y, hasta el punto que sea posible, identificando los bloques relevantes del repositorio de la arquitectura.		Aplica	Parcial	3.5
5. Mantener un modelo de arquitectura de procesos como parte de las descripciones de dominio de referencia y objetivo. Estandarizar las descripciones y la documentación de los procesos. Definir las funciones y responsabilidades de los que deciden el proceso, el propietario del proceso, los usuarios del proceso, el equipo del proceso y cualquier otra parte interesada que debieran estar involucrados.		No Aplica	Nula	0
6. Mantener un modelo de arquitectura de información como parte de las descripciones de dominio de referencia y objetivo, que sea consistente con la estrategia de la empresa y que permita un uso óptimo de la información para la toma de decisiones. Mantener un diccionario de datos de la empresa que promueva una interpretación común y un esquema de clasificación que incluya detalles sobre el propietario de los datos, definición de los niveles de seguridad apropiados y los requisitos de retención y destrucción de los datos.		Aplica	Completa	5
7. Verificar la consistencia interna y precisión de los modelos de la arquitectura y realizar un análisis de diferencias entre el punto de partida y el objetivo. Priorizar las desviaciones y definir los nuevos componentes o modificaciones que se deben desarrollar en la arquitectura objetivo. Resolver los impactos potenciales, tales como las incompatibilidades, inconsistencias o conflictos dentro de la arquitectura prevista.		Aplica	Parcial	3.5
8. Realizar una revisión formal con las partes interesadas para comprobar que la arquitectura propuesta frente a la motivación original del proyecto de arquitectura y la declaración de arquitectura funcionan.		Aplica	Parcial	3.5
9. Finalizar la arquitectura de los dominios de negocio, información, datos, aplicaciones y tecnología y crear un documento de definición de la arquitectura.		Aplica	Parcial	3.5

CONTINÚA →

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.	3.50
Actividad	Evaluación	Cobertura	Calificación
1. Determinar y confirmar los atributos clave del cambio, incluyendo la cultura empresarial y cómo ésta impactará en la implementación de la arquitectura de empresa, así como en las capacidades de transición empresarial.	Aplica	Parcial	3.5
2. Identificar los motivadores de la empresa que podrían limitar la secuencia de implementación, incluyendo una revisión de los planes estratégicos y de negocio de la empresa y de las líneas de negocio y considerando la madurez de la arquitectura de empresa actual.	Aplica	Parcial	3.5
3. Revisar y consolidar los resultado del análisis de diferencias entre las arquitecturas de partida y objetivo y evaluar sus implicaciones respecto a las potenciales oportunidades y soluciones, interdependencias y alineación con los vigentes programas habilitados para TI.	Aplica	Parcial	3.5
4. Evaluar las necesidades, las carencias, las soluciones y los factores para identificar un conjunto mínimo de requisitos funcionales cuya integración en el plan de trabajo daría lugar a una implementación más eficiente y eficaz de la arquitectura objetivo.	Aplica	Parcial	3.5
5. Conciliar los requisitos ya consolidados con las posibles soluciones.	Aplica	Parcial	3.5
6. Afinar las dependencias iniciales, asegurándose que todas las restricciones sobre los planes de implementación y migración están identificadas y se han consolidado en el informe de análisis de dependencias.	Aplica	Parcial	3.5
7. Confirmar el grado de preparación de la empresa y el riesgo asociado a la transformación empresarial,	Aplica	Parcial	3.5
8. Formular una implementación de alto nivel y una estrategia de migración que servirán de guía para la implementación de la arquitectura objetivo y para la estructura de la arquitectura de transición en línea con los objetivos estratégicos y los plazos de la empresa.	Aplica	Parcial	3.5
9. Identificar y agrupar los principales paquetes de trabajo en un conjunto de programas y proyectos coherentes, respetando el enfoque y la dirección de la estrategia empresarial en su implementación.	Aplica	Parcial	3.5
10. Desarrollar una serie de arquitecturas de transición cuando sea necesario un enfoque incremental por el alcance del cambio necesario para alcanzar la arquitectura de información objetivo.	Aplica	Parcial	3.5
APO03.04	Definir la implantación 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.	5

CONTINÚA →

Actividad		Evaluación	Cobertura	Calificación
1. Establecer lo que el plan de implementación y migración deberían incluir como parte del programa y plan de proyectos para asegurarse que están alineados con los requisitos de los decisores aplicables.		Aplica	Completa	5
2. Confirmar las fases y los progresos de la arquitectura de transición y actualizarlos en el documento de definición de la arquitectura.		Aplica	Completa	5
3. Definir los requisitos de gobierno de implementación de la arquitectura.		Aplica	Completa	5
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.		3.50
Actividad		Evaluación	Cobertura	Calificación
1. Confirmar el alcance y las prioridades y proporcionar orientación para el desarrollo y despliegue de soluciones.		Aplica	Parcial	3.5
2. Gestionar la cartera de servicios de arquitectura de la empresa para asegurar el alineamiento con los objetivos estratégicos y el desarrollo de soluciones.		Aplica	Parcial	3.5
3. Gestionar los requisitos de la arquitectura empresarial y dar soporte con los principios de dicha arquitectura, modelos y componentes básicos.		Aplica	Parcial	3.5
4. Identificar y alinear las prioridades de la arquitectura empresarial a los motivadores del valor. Definir y recoger los valores de las medidas y las métricas utilizadas y comunicar el valor de la arquitectura empresarial.		Aplica	Parcial	3.5
5. Establecer un foro tecnológico para facilitar guías de uso de la arquitectura, soporte en los proyectos y guía en la selección de la tecnología. Medir el cumplimiento con estos estándares y guías de referencia, incluyendo el cumplimiento con requisitos externos y su importancia para el negocio.		Aplica	Parcial	3.5

3.4.2.4APO04:

La aplicación de la plantilla para el proceso APO04: Gestionar la Innovación, se detalla en la Tabla 10.

Tabla 10

Plantilla para el proceso APO04

Código:	APO04	Área:	Gestión
Proceso:	Gestionar la Innovación	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			

CONTINÚA →

Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.			
Declaración del Propósito del Proceso:			
Lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	<ul style="list-style-type: none"> • Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico. • Porcentaje de servicios TI donde se obtienen los beneficios esperados. • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados 		
08 Uso adecuado de aplicaciones, información y soluciones tecnológicas.	<ul style="list-style-type: none"> • Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios TI • Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos • Nivel de satisfacción de los usuarios de negocio con la formación y los manuales de usuario • Valor presente neto (NPV) mostrando el nivel de satisfacción del negocio con la calidad y utilidad de las soluciones tecnológicas. 		
09 Agilidad de las TI.	<ul style="list-style-type: none"> • Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos. • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas. • Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada. 		
11 Optimización de activos, recursos y capacidades de las TI.	<ul style="list-style-type: none"> • 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 la alta dirección del negocio y de TI con los costes y capacidades TI. 		
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	<ul style="list-style-type: none"> • Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas TI innovadoras. 		
Prácticas y Actividades			
APO04.01	Crear un entorno favorable para la innovación.	Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados.	0.70
Actividad	Evaluación	Cobertura	Calificación
1. Crear un plan de innovación que incluya el apetito por el riesgo, el presupuesto previsto para invertir en la innovación y los objetivos de la innovación.	No Aplica	Nula	0

CONTINÚA →

2. Proveer de una infraestructura que pueda permitir innovar, tales como herramientas de colaboración para mejorar el trabajo entre diferentes ubicaciones geográficas y divisiones de la empresa.			Aplica	Parcial	3.5
3. Crear un entorno que fomente la innovación manteniendo iniciativas de recursos humanos relevantes, tales como el reconocimiento de la innovación y programas de reconocimiento, una rotación apropiada en los puestos de trabajo y tiempo prudencial para la experimentación.			No Aplica	Nula	0
4. Mantener un programa que permita a los empleados presentar ideas innovadoras y crear una estructura adecuada de toma de decisiones para evaluar y aplicar estas ideas.			No Aplica	Nula	0
5. Animar a innovar a los clientes, proveedores y socios comerciales.			No Aplica	Nula	0
APO04.02	Mantener un entendimiento del entorno de la empresa.	Trabajar junto a las partes interesadas para entender sus retos. Mantener un entendimiento adecuado de la estrategia corporativa y del entorno competitivo, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.	1.17		
Actividad			Evaluación	Cobertura	Calificación
1. Mantener una comprensión de los motores del negocio y de la industria, de la estrategia corporativa, operaciones corporativas y otras incidencias de modo que los potenciales valores añadidos tecnológicos o innovaciones TI puedan ser identificadas.			No Aplica	Nula	0
2. Realizar reuniones periódicas con las unidades de negocio, divisiones y/o otras entidades interesadas para entender los problemas actuales del negocio, cuellos de botella de los procesos u otras limitaciones donde las tecnologías emergentes o la innovación TI puede crear oportunidades.			Aplica	Parcial	3.5
3. Entender los parámetros de inversiones corporativas para la innovación y las nuevas tecnologías, de modo que se desarrollen las estrategias adecuadas.			No Aplica	Nula	0
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.	3.50		
Actividad			Evaluación	Cobertura	Calificación
1. Comprender el interés de la empresa y su potencial para adoptar nuevas innovaciones tecnológicas canalizando los esfuerzos de concienciación en las innovaciones tecnológicas más oportunas.			Aplica	Parcial	3.5
2. Realizar estudios y analizar el entorno exterior, incluyendo sitios web apropiados, diarios y conferencias para identificar tecnologías emergentes			Aplica	Parcial	3.5
3. Consultar con terceras personas expertas cuando se necesite confirmar los resultados de la investigación o como fuente de información en tecnologías emergentes.			Aplica	Parcial	3.5
4. Recopilar las ideas innovadoras del personal de TI y analizarlas para su posible implementación.			Aplica	Parcial	3.5
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.	3.50		
Actividad			Evaluación	Cobertura	Calificación

CONTINÚA →

1. Evaluar las tecnologías identificadas, considerando aspectos tales como tiempo para alcanzar la madurez, riesgo inherente de la nueva tecnología (incluyendo posibles implicaciones legales), ajuste con la arquitectura empresarial y potencial para proporcionar valor añadido.		Aplica	Parcial	3.5
2. Identificar cualquier problema que pueda necesitar ser resuelto o probado a través de una iniciativa de prueba de concepto.		Aplica	Parcial	3.5
3. Alcance de la iniciativa de prueba de concepto, incluyendo resultados deseados, presupuesto necesario, plazos de tiempo y responsabilidades.		Aplica	Parcial	3.5
4. Obtener autorización para realizar la prueba de concepto.		Aplica	Parcial	3.5
5. Realizar pruebas de concepto para evaluar las tecnologías emergentes u otras ideas innovadoras, identificar cualquier problema y determinar si más implementaciones deberían ser tenidas en cuenta, basándose en la viabilidad y el potencial retorno de la inversión (ROI).		Aplica	Parcial	3.5
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.		1.75
Actividad		Evaluación	Cobertura	Calificación
1. Documentar los resultados de las pruebas de concepto, incluyendo guía y recomendaciones para programas de innovación y tendencias.		Aplica	Parcial	3.5
2. Comunicar las oportunidades de innovación viables en la estrategia TI y en los procesos de arquitectura empresarial.		Aplica	Parcial	3.5
3. Realizar un seguimiento de las pruebas de concepto para medir el grado en que las mismas han influenciado en las inversiones reales.		No Aplica	Nula	0
4. Analizar y comunicar las razones por las que se ha rechazado una prueba de concepto.		No Aplica	Nula	0
APO04.06	Supervisar la implementación y el uso de la innovación.	Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas.		0.00
Actividad		Evaluación	Cobertura	Calificación
1. Valorar la implementación de nuevas tecnologías o innovaciones TI adoptadas como parte de la estrategia TI y desarrollos de la arquitectura empresarial y su realización durante programas de gestión de iniciativas.		No Aplica	Nula	0
2. Capturar lecciones aprendidas y oportunidades de mejora.		No Aplica	Nula	0
3. Ajustar el plan de innovación, si fuese necesario.		No Aplica	Nula	0
4. Identificar y evaluar el posible valor obtenido como fruto del uso de la innovación.		No Aplica	Nula	0

3.4.2.5APO05:

La aplicación de la plantilla para el proceso APO05: Gestionar la Cartera, se detalla en la Tabla 11.

Tabla 11

Plantilla para el proceso APO05

Código:	APO05	Área:	Gestión
Proceso:	Gestionar la Cartera	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.			
Declaración del Propósito del Proceso:			
Optimizar el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portafolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 		
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	<ul style="list-style-type: none"> • Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico. • Porcentaje de servicios TI donde se obtienen los beneficios esperados. • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados 		
13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	<ul style="list-style-type: none"> • Número de programas/proyectos en tiempo y en presupuesto. • Porcentaje de interesados satisfechos con la calidad del programa/proyecto. • Número de programas que necesitan revisiones significativas debido a defectos de calidad. • Coste de mantenimiento de las aplicaciones respecto al coste TI global. 		
Prácticas y Actividades			
APO05.01	Establecer la mezcla del objetivo de inversión.	Revisar y garantizar la claridad de las estrategias y servicios actuales corporativos y de TI. Definir una adecuada mezcla de inversión, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste, retorno de inversión esperado a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio. Ajustar las estrategias corporativas y de TI cuando sea necesario.	4,10
Actividad	Evaluación	Cobertura	Calificación

CONTINÚA →

1. Validar que las inversiones TI y los servicios TI actuales están alineados con la visión y los principios corporativos, metas y objetivos estratégicos, visión de la arquitectura empresarial y prioridades.				Aplica	Completa	5
2. Conseguir un entendimiento común entre TI y otras funciones de negocio sobre las potenciales oportunidades de TI para conducir y sustentar la estrategia corporativa.				Aplica	Completa	5
3. Crear una mezcla de inversión que logre el balance adecuado entre distintas dimensiones, incluyendo el equilibrio justo de retornos a corto y largo plazo, beneficios financieros y no financieros e inversiones de alto y bajo riesgo.				Aplica	Parcial	3,5
4. Identificar las categorías generales de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura, activos de TI, recursos, habilidades, prácticas, controles y relaciones necesarias para sustentar la estrategia corporativa.				Aplica	Parcial	3,5
5. Acordar una estrategia TI y unas metas, considerando las interrelaciones existentes entre la estrategia corporativa y los servicios TI, activos y otros recursos. Identificar y facilitar sinergias que puedan ser alcanzadas.				Aplica	Parcial	3,5
APO05.02	Determinar la disponibilidad y las fuentes de fondos.	la	Determinar las fuentes potenciales de fondos, diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas del retorno de inversión.			5,00
Actividad				Evaluación	Cobertura	Calificación
1. Entender la disponibilidad y el compromiso de los fondos actuales, el gasto actual aprobado y la cantidad real gastada hasta la fecha.				Aplica	Completa	5
2. Identificar las opciones para obtener financiación adicional para las inversiones TI internamente o de fuentes externas.				Aplica	Completa	5
3. Determinar las implicaciones de la fuente de financiación en las expectativas de retorno de la inversión.				Aplica	Completa	5
APO05.03	Evaluar y seleccionar los programas a financiar.	a	Basado en los requisitos de la mezcla general del portafolio de inversión, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión. Dedicar fondos e iniciar los programas.			4,00
Actividad				Evaluación	Cobertura	Calificación
1. Reconocer las oportunidades de inversión y clasificarlas en línea con las categorías del portafolio de inversiones. Especificar los resultados empresariales esperados, todas las iniciativas necesarias para alcanzar los resultados esperados, costes, dependencias y riesgos y como todo debe ser medido.				Aplica	Parcial	3,5
2. Realizar evaluaciones detalladas de todos los caso de negocio de los programas, evaluando el alineamiento estratégico, beneficios corporativos, riesgo y disponibilidad de recursos.				Aplica	Parcial	3,5
3. Evaluar el impacto en el portafolio general de inversiones por añadir los programas candidatos, incluyendo cualquier cambio que pueda ser requerido por otros programas.				Aplica	Parcial	3,5
4. Decidir qué programas candidatos deberían ser trasladados al portafolio de inversiones activas. Determinar si los programas rechazados deberían ser conservados para ser considerados en el futuro, o provistos con algún tipo de inversión para determinar si el caso de negocio puede ser mejorado o descartado.				Aplica	Completa	5

CONTINÚA →

5. Determinar los hitos necesarios para el ciclo de vida económico de cada programa seleccionado. Asignar y reservar totalmente los fondos para cada hito. Mover el programa al portafolio de inversiones activas.		Aplica	Parcial	3,5
6. Establecer procedimientos para comunicar el coste, beneficios y aspectos relativos al riesgo de esos portafolios a los procesos de priorización de presupuesto, gestión del coste y gestión del beneficio.		Aplica	Completa	5
APO05.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	Regularmente, supervisar y optimizar el rendimiento del portafolio de inversiones y de los programas individuales a lo largo de todo el ciclo de vida de inversión.		3,50
Actividad		Evaluación	Cobertura	Calificación
1. Revisar regularmente el portafolio para identificar y explotar sinergias, eliminar programas duplicados e identificar y mitigar el riesgo.		Aplica	Parcial	3,5
2. Cuando sucedan cambios, volver a evaluar y a priorizar el portafolio para asegurar que está alineado con la estrategia del negocio y que la mezcla de inversión objetivo se mantiene, de modo que el portafolio esté optimizando el valor global. Esto puede requerir que los programas cambien, se aplacen, se retiren o bien que nuevos programas se inicien.		Aplica	Parcial	3,5
3. Ajustar los objetivos, previsiones, presupuestos y, si fuese necesario, el grado de monitorización empresariales para reflejar los gastos en que se incurriría y los beneficios de la empresa que se obtendrían gracias a los programas del portafolio de inversiones activas. Incorporar los gastos del programa en el mecanismo de prorrateo de costes.		Aplica	Parcial	3,5
4. Proporcionar una vista precisa a las partes interesadas sobre el rendimiento del portafolio de inversiones.		Aplica	Parcial	3,5
5. Aportar informes ejecutivos para la revisión por parte de la alta dirección de los progresos de la empresa hacia las metas identificadas, estableciendo qué debe seguir siendo gastado y conseguido sobre qué franjas temporales.		Aplica	Parcial	3,5
6. Incluir en la supervisión periódica del rendimiento información sobre en qué medida los objetivos planificados han sido alcanzados, el riesgo mitigado, las capacidades creadas, los entregables obtenidos y las metas de rendimiento, conseguidas.		Aplica	Parcial	3,5
7. Identificar desviaciones para: • Control presupuestario entre el real y el presupuesto • Gestión del beneficio de: – Real versus objetivos de inversión en soluciones, probablemente expresados en términos de ROI, NPV o tasa interna de retorno (IRR) – Tendencia actual del coste del portafolio de servicios para la mejora de la productividad de la entrega del servicio,		Aplica	Parcial	3,5
8. Desarrollar métricas para medir la contribución de TI a la empresa, y establecer objetivos de rendimiento adecuados que reflejen las metas de capacidad corporativas y de TI. Utilizar asistencia de expertos externos y de datos de análisis comparativos para desarrollar métricas.		Aplica	Parcial	3,5
APO05.05	Mantener los portafolios.	Mantener los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.		2,33
Actividad		Evaluación	Cobertura	Calificación

CONTINÚA →

1. Crear y mantener portafolios de programas de inversiones TI, servicios TI y activos TI, que constituyan la base del presupuesto actual de TI y soporten los planes estratégicos y tácticos de TI.		Aplica	Parcial	3,5
2. Trabajar con los responsables de entrega del servicio para mantener los portafolios de servicio y con los responsables de operaciones y arquitectos para mantener el portafolio de activos. Apoyar los planes tácticos y estratégicos de TI.		Aplica	Parcial	3,5
3. Eliminar los programas del portafolio de inversiones activas cuando los beneficios corporativos deseados han sido alcanzados o cuando está claro que los beneficios no serán alcanzados dentro del criterio de valor establecido para el programa.		No Aplica	Nula	0
APO05.06	Gestionar la consecución de beneficios.	Supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas, basadas en el caso de negocio acordado actual.		2,33
Actividad		Evaluación	Cobertura	Calificación
1. Utilizar las métricas acordadas y realizar seguimiento sobre cómo los beneficios son obtenidos, cómo evolucionan a lo largo del ciclo de vida de programas y proyectos, cómo son entregados desde los servicios TI y cómo resultan al someterlos a un análisis comparativo interno y de la industria. Comunicar los resultados a las partes interesadas.		Aplica	Parcial	3,5
2. Implementar acciones correctivas cuando los beneficios alcanzados se desvían significativamente de los esperados. Actualizar los casos de negocio para las nuevas iniciativas e implementar procesos de negocio y mejoras del servicio según se requiera.		Aplica	Parcial	3,5
3. Considerar obtener orientación de expertos externos, líderes de la industria y datos de análisis comparativos para probar y mejorar las métricas y los objetivos.		No Aplica	Nula	0

3.4.2.6APO06:

La aplicación de la plantilla para el proceso APO06: Gestionar el Presupuesto y los Costes, se detalla en la Tabla 12.

Tabla 12

Plantilla para el proceso APO06

Código:	APO06	Área:	Gestión
Proceso:	Gestionar el Presupuesto y los Costes	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.			

CONTINÚA →

Declaración del Propósito del Proceso:			
Fomentar la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos relacionados con las TI y brindar transparencia y responsabilidad sobre el coste y valor de negocio de soluciones y servicios. Permitir a la empresa tomar decisiones informadas con respecto a la utilización de soluciones y servicios de TI.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	<ul style="list-style-type: none"> • Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico. • Porcentaje de servicios TI donde se obtienen los beneficios esperados. • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados. 		
06 Transparencia de los costes, beneficios y riesgos de las TI.	<ul style="list-style-type: none"> • Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI. 		
Prácticas y Actividades			
APO06.01	Gestionar las finanzas y la contabilidad.	Establecer y mantener un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI, como parte integral de los sistemas financieros empresariales y el plan de cuentas para administrar las inversiones y los costes de TI. Capturar y asignar los costes reales, analizar las desviaciones entre las previsiones y los costes reales, e informar usando los sistemas empresariales de medición financiera.	5.00
Actividad	Evaluación	Cobertura	Calificación
1. Definir procesos, entradas y salidas y responsabilidades de manera alineada con las políticas y el enfoque empresariales de presupuesto y contabilización de costes para manejar sistemáticamente el presupuesto y asignación de costes de TI; catalizar estimaciones de costes y beneficios de TI justos, transparentes, repetibles y comparables y usarlos como dato de entrada a la cartera de programas de negocio habilitados por las TI; y asegurarse de que se mantienen los presupuestos y costes de las carteras de servicios y activos de TI.	Aplica	Completa	5
2. Definir un esquema de clasificación para identificar todos los elementos de coste relacionados con las TI, la forma en que se distribuyen entre los presupuestos y servicios, y la forma en que son capturados.	Aplica	Completa	5
3. Utilizar la información financiera y de cartera para proporcionar datos de entrada a casos de negocio para nuevas inversiones en activos y servicios de TI.	Aplica	Completa	5
4. Definir la forma de analizar, informar (a quién y cómo), y utilizar el control presupuestario y los procesos de gestión de beneficios.	Aplica	Completa	5
5. Establecer y mantener prácticas para la planificación financiera, gestión de inversiones y toma de decisiones y la optimización de los gastos recurrentes de operación para entregar el máximo valor a la empresa con el menor gasto posible.	Aplica	Completa	5
APO06.02	Priorizar la asignación de recursos.	Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales por parte de unidades de negocio individuales. Incluir el uso potencial de proveedores de servicio externos y considerar las opciones de compra, desarrollo y alquiler.	5.00
Actividad	Evaluación	Cobertura	Calificación

CONTINÚA →

1. Establecer un órgano de toma de decisiones para priorizar recursos de TI y del negocio, incluyendo el uso de proveedores de servicio externos dentro de las asignaciones presupuestarias de alto nivel para programas habilitados por TI, servicios TI y activos de TI conforme a lo establecido por los planes estratégicos y tácticos. Considerar las opciones para la compra o desarrollo de activos y servicios capitalizados frente a la utilización de activos externos y de servicios sobre una base de pago por uso.			Aplica	Completa	5
2. Posicionar todas las iniciativas de TI sobre la base de los casos de negocio y planes estratégicos y tácticos, y establecer procedimientos para determinar las asignaciones presupuestarias y cortes. Establecer un procedimiento para comunicar las decisiones presupuestarias y revisar con los responsables del presupuesto de las unidades de negocio.			Aplica	Completa	5
3. Identificar, comunicar y resolver los impactos más significativos de las decisiones presupuestarias en los casos de negocios, carteras y planes estratégicos (por ejemplo, cuando los presupuestos puedan requerir una revisión debido a las circunstancias cambiantes de la empresa, cuando no son suficientes para apoyar los objetivos estratégicos o los objetivos del caso de negocio)			Aplica	Completa	5
4. Obtener la ratificación del Comité Ejecutivo para los cambios generales en el presupuesto de TI que afecten negativamente a los planes estratégicos y tácticos de la entidad y ofrecer acciones sugeridas para resolver estos impactos.			Aplica	Completa	5
APO06.03	Crear y mantener presupuestos.	Preparar un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos basado en la cartera de programas habilitados por TI y servicios de TI.			4.36
Actividad			Evaluación	Cobertura	Calificación
1. Implementar un presupuesto formal de TI, incluyendo todos los costes de TI esperados de los programas habilitados por las TI, servicios de TI y activos de TI según las indicaciones de la estrategia, programas y carteras.			Aplica	Parcial	3.5
2. Al crear el presupuesto, considere los siguientes componentes: • Alineamiento con el negocio • Alineamiento con la estrategia de aprovisionamiento • Fuentes de financiación autorizadas • Costes internos de recursos, incluyendo personal, activos de información y alojamiento. • Costes de terceras partes, incluyendo contratos de externalización, consultores y proveedores de servicio. • Gastos de capital y operativos. • Elementos de coste que dependen de la carga de trabajo.			Aplica	Completa	5
3. Documentar las razones para justificar las contingencias y revisarlas regularmente.			Aplica	Completa	5
4. Indicar la necesidad de planificar presupuestos a los dueños de procesos, servicios o programas, así como a los jefes de proyecto y gerentes de activos.			Aplica	Completa	5
5. Revisar los planes de presupuesto y tomar decisiones sobre las asignaciones presupuestarias. Compilar y ajustar el presupuesto en base a necesidades empresariales cambiantes y consideraciones financieras.			Aplica	Parcial	3.5
6. Registrar, mantener y comunicar el presupuesto actual de TI, incluidos los gastos comprometidos y los gastos corrientes, teniendo en cuenta los proyectos de TI registrados en las carteras de inversiones habilitadas por TI y la operación y el mantenimiento de las carteras de activos y servicios.			Aplica	Completa	5

CONTINÚA →

7. Seguimiento de la eficacia de los diferentes aspectos de la elaboración de presupuestos y utilización de los resultados para implementar mejoras para garantizar que futuros presupuestos sean más precisos, fiables y rentables.		Aplica	Parcial	3.5
APO06.04	Modelar y asignar costes.	Establecer y utilizar un modelo de costes de TI basado en la definición del servicio, asegurando que la asignación de costes de los servicios es identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicio. Revisar regularmente y comparar la idoneidad del modelo de costes/prorrateo de costes para mantener su pertinencia y adecuación al negocio en evolución y las actividades de TI que le dan soporte.		3.75
Actividad		Evaluación	Cobertura	Calificación
1. Clasificar todos los costes de TI adecuadamente, incluidos los relativos a los proveedores de servicio, de acuerdo con el marco de contabilidad de la gestión de la empresa.		Aplica	Completa	5
2. Revisar los catálogos de definición de servicios para identificar servicios sujetos a prorrateo de costes hacia el usuario y aquellos servicios que son compartidos.		Aplica	Parcial	3.5
3. Definir y acordar un modelo que: • Soporte el cálculo de las tasas de prorrateo de costes por servicio • Defina cómo se calcularán y cargarán los costes de TI • Es diferenciado, donde y cuando sea apropiado • Está alineado con el presupuesto de TI.		Aplica	Parcial	3.5
4. Diseñar el modelo de costes para ser lo suficientemente transparente como para permitir a los usuarios identificar su uso real y sus cargos, y para mejor catalizar la previsibilidad de los costes de TI y la utilización eficiente y eficaz de los recursos de TI.		Aplica	Parcial	3.5
5. Después de la revisión con los departamentos usuarios, obtener la aprobación y comunicar los datos de entrada y salida del modelo de costes de TI a la gerencia de los departamentos usuarios.		Aplica	Parcial	3.5
6. Comunicar a los dueños de los procesos empresariales los cambios en el modelo de costes y prorrateo de costes.		Aplica	Parcial	3.5
APO06.05	Gestionar costes.	Implementar un proceso de gestión de costes comparando los costes reales con los presupuestos. Los costes deben ser supervisados y comunicados y, en el caso de desviaciones, identificados oportunamente, así como evaluado su impacto en los procesos y servicios empresariales.		4.33
Actividad		Evaluación	Cobertura	Calificación
1. Asegurar la debida autorización y la independencia entre los responsables de los presupuestos de TI y los individuos que capturan, analizan y reportan información financiera.		Aplica	Completa	5
2. Establecer escalas de tiempo para la operación del proceso de gestión de costes en línea con los requisitos presupuestarios y de contabilidad.		Aplica	Completa	5
3. Definir un método para la recopilación de datos relevantes para identificar desviaciones en: • Control presupuestario entre presupuesto y real • Gestión del beneficio de: – Inversiones para soluciones actual vs objetivo; posiblemente, expresados en términos de ROI, NPV o IRR. – La tendencia actual del coste del servicio para la optimización del coste de los servicios (por ejemplo, definido como coste por usuario). – Real contra presupuesto de la capacidad de respuesta y la mejora de la previsibilidad de la entrega de soluciones. • Distribución de costes entre directos e indirectos (absorbidos y no absorbidos)		Aplica	Parcial	3.5

CONTINÚA →

4. Definir cómo se consolidan los costes para los niveles adecuados en la empresa y la forma en que se presentará a las partes interesadas. Los informes proporcionan información que permite la identificación oportuna de las medidas correctivas necesarias.	Aplica	Completa	5
5. Indicar a los responsables de gestión de costes que capturen, recojan y consoliden los datos, y presenten y comuniquen los datos a los pertinentes propietarios del presupuesto. Los analistas presupuestarios y los propietarios analizan conjuntamente las desviaciones y comparan el desempeño con parámetros internos y de la industria. El resultado del análisis proporciona una explicación de las desviaciones significativas y las acciones correctivas sugeridas.	Aplica	Parcial	3.5
6. Asegurarse de que los niveles adecuados de gestión revisan los resultados del análisis y aprueban las propuestas de acciones correctivas.	Aplica	Completa	5
7. Alinear los presupuestos y servicios de TI a la infraestructura de TI, procesos empresariales, y a los propietarios que los utilizan.	Aplica	Parcial	3.5
8. Asegurarse de que los cambios en las estructuras de costes y necesidades de la empresa se identifican y los presupuestos y las provisiones se revisan según sea necesario.	Aplica	Parcial	3.5
9. A intervalos regulares, y especialmente cuando se recortan los presupuestos debido a limitaciones financieras, identificar formas de optimizar los costes e introducir eficiencia sin poner en peligro los servicios.	Aplica	Completa	5

3.4.2.7APO07:

La aplicación de la plantilla para el proceso APO07: Gestionar los Recursos Humanos, se detalla en la Tabla 13.

Tabla 13

Plantilla para el proceso APO07

Código:	APO07	Área:	Gestión
Proceso:	Gestionar los Recursos Humanos	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.			
Declaración del Propósito del Proceso:			
Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		

CONTINÚA →

01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio.
11 Optimización de activos, recursos y capacidades de las TI.	<ul style="list-style-type: none"> • 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 la alta dirección del negocio y de TI con los costes y capacidades TI.
13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	<ul style="list-style-type: none"> • Número de programas/proyectos en tiempo y en presupuesto. • Porcentaje de interesados satisfechos con la calidad del programa/proyecto. • Número de programas que necesitan revisiones significativas debido a defectos de calidad. • Coste de mantenimiento de las aplicaciones respecto al coste TI global.
16 Personal del negocio y de las TI competente y motivado.	<ul style="list-style-type: none"> • Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles. • Porcentaje de personal satisfecho con sus roles en TI. • Número de horas de aprendizaje/ formación por miembro del personal.
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	<ul style="list-style-type: none"> • Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas TI innovadoras.

Prácticas y Actividades

APO07.01	Mantener la dotación de personal suficiente y adecuada.	Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.	4.70
Actividad	Evaluación	Cobertura	Calificación
1. Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar que: <ul style="list-style-type: none"> • La función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos empresariales. • La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI. 	Aplica	Completa	5
2. Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa	Aplica	Completa	5
3. Incluir controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores. El alcance y la frecuencia de estos controles dependen de la sensibilidad y/o criticidad de la función.	Aplica	Completa	5
4. Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias, contratistas externos y acuerdos de servicio con terceras partes.	Aplica	Completa	5
5. Asegurarse de que el entrenamiento cruzado se lleva a cabo y que hay respaldo para el personal clave para reducir la dependencia de una sola persona.	Aplica	Parcial	3.5

CONTINÚA →

APO07.02	Identificar personal clave de TI.	Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal.	3.88	
Actividad		Evaluación	Cobertura	Calificación
1. Minimizar la dependencia en una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión, el respaldo (backup) del personal, el entrenamiento cruzado e iniciativas de rotación de puestos.		Aplica	Parcial	3.5
2. Como medida de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que deben tomar los individuos clave.		Aplica	Completa	5
3. Tomar acciones expeditivas con respecto a cambios laborales, especialmente despidos.		Aplica	Parcial	3.5
4. Probar regularmente los planes de respaldo (backup) del personal.		Aplica	Parcial	3.5
APO07.03	Mantener las habilidades y competencias del personal.	Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.	3.93	
Actividad		Evaluación	Cobertura	Calificación
1. Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos.		Aplica	Parcial	3.5
2. Proporcionar una planificación formal de la carrera y desarrollo profesional para fomentar el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave.		Aplica	Parcial	3.5
3. Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias.		Aplica	Completa	5
4. Identificar las diferencias entre las habilidades necesarias y las disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva, tales como formación (técnica y en habilidades de comportamiento), contratación, redistribución y cambios en las estrategias de contratación.		Aplica	Parcial	3.5
5. Desarrollar y ejecutar programas de formación basados en los requisitos organizativos y de procesos, incluidos los requisitos sobre conocimiento empresarial, control interno, conducta ética y seguridad.		Aplica	Completa	5
6. Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Revisar la planificación de la sucesión.		Aplica	Parcial	3.5
7. Revisar los materiales y programas de formación de manera regular para asegurarse su adecuación a los requisitos empresariales cambiantes y su impacto en los conocimientos, aptitudes y habilidades necesarias.		Aplica	Parcial	3.5

CONTINÚA →

APO07.04	Evaluar el desempeño laboral de los empleados.	Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado.	4.44
Actividad	Evaluación	Cobertura	Calificación
1. Considerar los objetivos funcionales/de empresa como el contexto para establecer las metas individuales.	Aplica	Completa	5
2. Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales. Basar las metas en objetivos SMART (específicos, medibles, realizables, pertinentes y de duración determinada) que reflejen las competencias básicas, los valores empresariales y las habilidades necesarias para la(s) función(es).	Aplica	Completa	5
3. Recopilar los resultados de la evaluación de desempeño de 360 grados.	Aplica	Completa	5
4. Implementar y comunicar un proceso disciplinario.	Aplica	Completa	5
5. Proporcionar instrucciones específicas para el uso y almacenamiento de información personal en el proceso de evaluación, de conformidad con la legislación laboral y sobre datos personales aplicables	Aplica	Parcial	3.5
6. Proporcionar retroalimentación oportuna sobre el desempeño frente a las metas del individuo.	Aplica	Completa	5
7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, el desarrollo de competencias y el logro exitoso de los objetivos de desempeño. Asegurar que el proceso se aplica de forma coherente y en consonancia con las políticas de la organización.	Aplica	Parcial	3.5
8. Desarrollar planes de mejora del desempeño basados en los resultados del proceso de evaluación y los requisitos de capacitación y desarrollo de competencias identificados.	Aplica	Parcial	3.5
APO07.05	Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.	3.88
Actividad	Evaluación	Cobertura	Calificación
1. Crear y mantener un inventario de recursos humanos de negocio y TI.	Aplica	Completa	5
2. Entender la demanda actual y futura de recursos humanos para apoyar el logro de los objetivos de TI y ofrecer servicios y soluciones basados en la cartera de las iniciativas actuales relacionadas con las TI, la cartera de inversiones futuras y las necesidades operativas del día a día.	Aplica	Parcial	3.5
3. Identificar las carencias y proporcionar datos de entrada a planes de aprovisionamiento, así como a los procesos de contratación de la empresa y de TI. Crear y revisar el plan de personal, haciendo seguimiento del uso real.	Aplica	Parcial	3.5
4. Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos.	Aplica	Parcial	3.5
APO07.06	Gestionar el personal contratado.	Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados.	3.06

CONTINÚA →

Actividad	Evaluación	Cobertura	Calificación
1. Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización y el marco de control de TI.	Aplica	Parcial	3.5
2. Obtener un acuerdo formal por parte de los contratistas en el inicio del contrato en cuanto a que están obligados a cumplir con el marco de control de TI de la empresa, tal como políticas de control de seguridad, control de acceso físico y lógico, uso de las instalaciones, requisitos de confidencialidad de la información y los acuerdos de confidencialidad.	Aplica	Parcial	3.5
3. Advertir a los contratistas de que la gerencia se reserva el derecho de supervisar e inspeccionar todo uso de los recursos de TI, incluyendo correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.	No Aplica	Nula	0
4. Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades como parte de sus contratos, incluidos requisitos explícitos para documentar su trabajo en base a normas y formatos previamente acordados.	Aplica	Parcial	3.5
5. Revisar el trabajo de los contratistas y basar la aprobación de los pagos en los resultados.	Aplica	Parcial	3.5
6. Definir todo el trabajo a realizar por terceras partes en contratos formales y sin ambigüedades.	Aplica	Parcial	3.5
7. Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios.	Aplica	Parcial	3.5
8. Llevar a cabo revisiones periódicas para asegurarse de que las funciones de los contratistas y sus derechos de acceso son adecuados y en línea con los acuerdos.	Aplica	Parcial	3.5

3.4.2.8APO08:

La aplicación de la plantilla para el proceso APO08: Gestionar las Relaciones, se detalla en la Tabla 14.

Tabla 14

Plantilla para el proceso APO08

Código:	APO08	Área:	Gestión
Proceso:	Gestionar las Relaciones	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.			
Declaración del Propósito del Proceso:			
Crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.			

CONTINÚA →

El proceso apoya la consecución de un conjunto de principales metas TI:				
Meta TI	Métricas relacionadas			
01 Alineamiento de TI y estrategia de negocio.	<ul style="list-style-type: none"> • Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio. 			
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 			
12 Capacitación y soporte de procesos de negocio y tecnología en procesos de negocio integrando aplicaciones.	<ul style="list-style-type: none"> • Número de incidentes del procesamiento de negocio causados por errores de integración de la tecnología. • Número de cambios en los procesos de negocio que tienen que ser retrasados o revisados debido a problemas de integración de la tecnología. • Número de programas de negocio facilitados por TI retrasados o incurriendo en costes adicionales debido a problemas de integración de la tecnología. • Número de aplicaciones o infraestructuras críticas operando aisladamente y no integradas. 			
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	<ul style="list-style-type: none"> • Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas TI innovadoras. 			
Prácticas y Actividades				
APO08.01	Entender las expectativas del negocio.	las del	Entender el enfoque y expectativas actuales del negocio para TI. Asegurar que los requisitos son entendidos, gestionados y comunicados y su estado acordado y aprobado.	3.93
Actividad	Evaluación	Cobertura	Calificación	
1. Identificar a las partes interesadas del negocio, sus intereses y sus áreas de responsabilidad.	Aplica	Completa	5	
2. Revisar la orientación de la empresa, asuntos, objetivos estratégicos actuales y alineamiento con la arquitectura empresarial.	Aplica	Completa	5	
3. Mantener una atención sobre los procesos de negocio y actividades asociadas y entender los patrones de demanda relacionados con el volumen y uso de servicios.	Aplica	Parcial	3.5	
4. Esclarecer las expectativas del negocio para los servicios y soluciones basados en TI y asegurar que los requisitos son definidos con criterios y métricas aceptados por el negocio.	Aplica	Parcial	3.5	
5. Confirmar el acuerdo sobre las expectativas del negocio, los criterios de aceptación y las métricas para las partes relevantes de la infraestructura TI por todas las partes interesadas.	Aplica	Parcial	3.5	
6. Gestionar las expectativas asegurando que las unidades de negocio entienden las prioridades, dependencias, restricciones financieras y la necesidad de planificar peticiones.	Aplica	Parcial	3.5	
7. Entender el entorno de negocio actual, limitaciones o flujos de procesos, expansión o contracción geográfica y motivaciones de la industria/regulación.	Aplica	Parcial	3.5	

CONTINÚA →

APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	Limitaciones de TI para mejorar el negocio. Identificar oportunidades potenciales para que la TI sea catalizadora de la mejora del rendimiento empresarial.	3.50	
Actividad		Evaluación	Cobertura	Calificación
1. Entender las tendencias tecnológicas y las nuevas tecnologías y cómo pueden aplicarse de modo innovador para mejorar el rendimiento de los procesos de negocio.		Aplica	Parcial	3.5
2. Tomar un papel proactivo en identificar y comunicar a las partes interesadas clave las oportunidades, riesgos y limitaciones. Esto incluye tecnologías, servicios y modelos de negocios tanto actuales como emergentes.		Aplica	Parcial	3.5
3. Colaborar en acordar los siguientes pasos para las principales nuevas iniciativas en colaboración con la gestión de la cartera de servicios, incluyendo el desarrollo de casos de negocio.		Aplica	Parcial	3.5
4. Asegurar que el negocio y la TI entienden y aprecian los objetivos estratégicos y la visión de la arquitectura empresarial.		Aplica	Parcial	3.5
5. Coordinar durante la planificación de nuevas iniciativas TI para asegurar la integración y el alineamiento con la arquitectura empresarial.		Aplica	Parcial	3.5
APO08.03	Gestionar relaciones con las el negocio.	Gestionar la relación con los clientes (representantes del negocio). Asegurar que los roles y responsabilidades de la relación están definidas, asignados y se facilita la comunicación.	3.50	
Actividad		Evaluación	Cobertura	Calificación
1. Asignar un responsable de la relación como punto único de contacto por cada unidad de negocio significativa. Asegurar que se ha identificado una contra-parte única en la organización de la empresa y que tenga entendimiento del negocio, suficiente concienciación tecnológica y un nivel apropiado de autoridad.		Aplica	Parcial	3.5
2. Gestionar la relación de un modo formal y transparente que asegure un enfoque en conseguir, como objetivo común y compartido, resultados exitosos apoyando los objetivos estratégicos dentro de las limitaciones del presupuesto y de la tolerancia de riesgos.		Aplica	Parcial	3.5
3. Definir y comunicar un proceso de reclamaciones y escalado de las mismas para resolver cualquier incidencia en la relación.		Aplica	Parcial	3.5
4. Planificar interacciones específicas y calendarios basados en objetivos acordados mutuamente y en un lenguaje común (reuniones de revisión del servicio y del rendimiento, revisión de nuevas estrategias o planes, etc.).		Aplica	Parcial	3.5
5. Asegurar que las decisiones claves son acordadas y aprobadas por las partes interesadas responsables y relevantes.		Aplica	Parcial	3.5
APO08.04	Coordinar y comunicar.	Trabajar con las partes interesadas y coordinar de extremo a extremo la entrega de los servicios TI y las soluciones proporcionadas al negocio.	3.88	
Actividad		Evaluación	Cobertura	Calificación
1. Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.		Aplica	Completa	5
2. Coordinar y comunicar actividades operativas, roles y responsabilidades, incluyendo la definición de los tipos de petición, escalado jerárquico, periodos de interrupción significativos (planeados o no) y contenido y frecuencia de los informes del servicio.		Aplica	Parcial	3.5

CONTINÚA →

3. Tomar consideración de la reacción del negocio ante eventos que puedan influenciar en la relación con el mismo. Proporcionar soporte directo si fuera necesario.		Aplica	Parcial	3.5
4. Mantener un plan de comunicación extremo a extremo que defina el contenido, frecuencia y destinatarios de la información de la entrega del servicio, incluyendo el estado del valor entregado y los riesgos identificados.		Aplica	Parcial	3.5
APO08.05	Proveer datos de entrada para la mejora continua de los servicios.	Mejorar y evolucionar continuamente los servicios basados en TI y la entrega del servicio a la empresa para alinearlos con unos cambiantes requisitos de empresa y tecnológicos.		2.33
Actividad		Evaluación	Cobertura	Calificación
1. Llevar a cabo análisis de satisfacción de clientes y proveedores. Asegurar que se actúa sobre las cuestiones detectadas y que se reportan los resultados y estados.		Aplica	Parcial	3.5
2. Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.		Aplica	Parcial	3.5
3. Trabajar con la gestión del servicio y los propietarios de los procesos para asegurar que los servicios basados en TI y la gestión de los procesos del servicio son mejorados continuamente y las causas raíz de cualquier incidente son identificadas y resueltas.		No Aplica	Nula	0

3.4.2.9APO09:

La aplicación de la plantilla para el proceso APO09: Gestionar los Acuerdos de Servicio, se detalla en la Tabla 15.

Tabla 15

Plantilla para el proceso APO09

Código:	APO09	Área:	Gestión
Proceso:	Gestionar los Acuerdos de Servicio	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.			
Declaración del Propósito del Proceso:			
Asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> Número de interrupciones de negocio debidas a incidentes de servicios TI Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 		

CONTINÚA →

14	Disponibilidad de información útil y relevante para la toma de decisiones.	<ul style="list-style-type: none"> Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión. Número de incidentes de procesos de negocio causados por la indisponibilidad de la información. Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave. 		
Prácticas y Actividades				
APO09.01	Identificar servicios TI.	Analizar los requisitos del negocio y el modo en que los servicios TI y los niveles de servicio soportan los procesos de negocio. Discutir y acordar servicios potenciales y niveles de servicio con el negocio y compararlos con la cartera actual para identificar servicios nuevos o modificados, u opciones de nivel de servicio.	3.17	
Actividad		Evaluación	Cobertura	Calificación
1. Valorar los servicios TI actuales y los niveles de servicio para identificar lagunas entre los servicios existentes y los procesos de negocio de los que son base. Identificar áreas de mejora de los servicios existentes y de las opciones de nivel del servicio.		Aplica	Parcial	3.5
2. Analizar, estudiar y estimar la futura demanda y confirmar la capacidad de los servicios TI existentes.		Aplica	Parcial	3.5
3. Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios TI nuevos o rediseñados.		No Aplica	Nula	0
4. Comparar los requisitos identificados con los componentes del servicio existentes en el catálogo. Si es posible, agrupar los componentes del servicio existentes (servicios TI, opciones de nivel de servicio y paquetes de servicios) en nuevos paquetes de servicio para cumplir con los requisitos de negocio identificados.		Aplica	Parcial	3.5
5. Siempre que sea posible, relacionar demanda con paquetes de servicio y crear servicios estandarizados para obtener una eficiencia global.		Aplica	Parcial	3.5
6. Revisar el catálogo de servicios TI regularmente con la gestión del catálogo y la gestión de relaciones del negocio para identificar servicios obsoletos. Acordar la retirada de los mismos y proponer cambios.		Aplica	Completa	5
APO09.02	Catálogo servicios basados en TI.	Definir y mantener uno o más catálogos de servicios para grupos de clientes objetivo relevantes. Publicar y mantener los servicios TI activos en los catálogos.	3.50	
Actividad		Evaluación	Cobertura	Calificación
1. Publicar los servicios TI, paquetes de servicios y opciones de nivel del servicio activos de la cartera de servicios en los catálogos relevantes.		Aplica	Parcial	3.5
2. Asegurar de forma continua que los componentes de servicio en el portafolio y en los catálogos de servicio relacionados están completos y actualizados.		Aplica	Parcial	3.5
3. Informar al gestor de relaciones del negocio de las actualizaciones en los catálogos de servicios.		Aplica	Parcial	3.5
APO09.03	Definir y preparar acuerdos de servicio.	Definir y preparar los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Incluir acuerdos de nivel de operaciones interno.	3.50	
Actividad		Evaluación	Cobertura	Calificación
1. Analizar los requisitos para acuerdos de servicios nuevos o modificados recibidos desde la gestión de las relaciones con el negocio para asegurar que los requisitos puedan ser emparejados con los niveles de servicio. Considerar aspectos tales como tiempos del servicio, disponibilidad, rendimiento, capacidad, seguridad, continuidad, cumplimiento normativo y regulatorio, usabilidad y limitaciones de la demanda.		Aplica	Parcial	3.5

CONTINÚA →

2. Esbozar borradores de acuerdos de nivel de servicio con el cliente basados en los servicios, paquetes de servicios y opciones del nivel de servicio en los catálogos de servicio relevantes.			Aplica	Parcial	3.5
3. Determinar, acordar y documentar los acuerdos operativos internos para cimentar los acuerdos de servicio con clientes, siempre que sea aplicable.			Aplica	Parcial	3.5
4. Mantener una relación estrecha con la gestión de proveedores para asegurar que los contratos comerciales apropiados con proveedores de servicio externos cimentan los acuerdos de servicio con los clientes, siempre que sea aplicable.			Aplica	Parcial	3.5
5. Ultime acuerdos de servicio al cliente con la gestión de relaciones del negocio.			Aplica	Parcial	3.5
APO09.04	Supervisar e informar de los niveles de servicio.	Supervisar los niveles de servicio, informar de las mejoras e identificar tendencias. Proporcionar información de gestión adecuada para ayudar a la gestión del rendimiento.			3.50
Actividad			Evaluación	Cobertura	Calificación
1. Establecer y mantener medidas para supervisar y recolectar datos del nivel del servicio.			Aplica	Parcial	3.5
2. Evaluar el rendimiento y proporcionar informes regular y formalmente sobre el rendimiento del acuerdo del servicio, incluyendo desviaciones con respecto a los valores acordados. Distribuir estos informes a la gestión de las relaciones del negocio.			Aplica	Parcial	3.5
3. Hacer revisiones regulares para anticipar e identificar tendencias en el rendimiento del nivel de servicio.			Aplica	Parcial	3.5
4. Proporcionar información de gestión apropiada para ayudar en la gestión del rendimiento.			Aplica	Parcial	3.5
5. Acordar planes de acción y remedio para los incidentes del rendimiento o tendencias negativas del mismo.			Aplica	Parcial	3.5
APO09.05	Revisar acuerdos de servicio y contratos.	Llevar a cabo revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.			3.50
Actividad			Evaluación	Cobertura	Calificación
1. Revisar los términos de los acuerdos de servicio regularmente para asegurar que son efectivos y actuales y que los cambios en los requisitos, servicios TI, paquetes de servicios u opciones de nivel de servicio se tienen en cuenta cuando sea apropiado.			Aplica	Parcial	3.5

3.4.2.10 APO10:

La aplicación de la plantilla para el proceso APO10: Gestionar los Proveedores, se detalla en la Tabla 16.

Tabla 16

Plantilla para el proceso APO10

Código:	APO10	Área:	Gestión
Proceso:	Gestionar los Proveedores	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			

CONTINÚA →

Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.			
Declaración del Propósito del Proceso:			
Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI. • Frecuencia de actualización del perfil de riesgo. 		
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 		
09 Agilidad de las TI.	<ul style="list-style-type: none"> • Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos. • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas. • Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada. 		
Prácticas y Actividades			
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.	3.50
Actividad	Evaluación	Cobertura	Calificación
1. Establecer y mantener criterios relativo al tipo, relevancia y criticidad de los contratos y proveedores, focalizándose en aquellos de mayor importancia.	Aplica	Parcial	3.5
2. Establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente.	Aplica	Parcial	3.5
3. Identificar, registrar y categorizar los proveedores y contratos existentes de acuerdo al criterio definido para mantener un registro detallado de los proveedores que deben ser gestionados cuidadosamente.	Aplica	Parcial	3.5
4. Evaluar y comparar periódicamente el rendimiento de los proveedores actuales y alternativos para identificar oportunidades de mejora o la necesidad forzosa de reconsiderar los contratos con los proveedores actuales.	Aplica	Parcial	3.5
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.	4.79
Actividad	Evaluación	Cobertura	Calificación
1. Revisar todas las RFIs y RFPs para asegurar que: <ul style="list-style-type: none"> • Definen claramente los requisitos. • Incluyen un procedimiento para clarificar los requisitos. • Dan a los proveedores tiempo suficiente para elaborar sus propuestas. • Definen claramente los criterios y el proceso de decisión. 	Aplica	Completa	5

CONTINÚA →

2. Evaluar RFIs y RFPs de acuerdo al proceso y criterios aprobados y mantener evidencia documental de las evaluaciones. Verificar las referencias de los proveedores candidatos.		Aplica	Parcial	3.5
3. Seleccionar el proveedor que mejor cumpla la RFP. Documentar y comunicar la decisión alcanzada y firmar el contrato.		Aplica	Completa	5
4. En el caso específico de la adquisición de software, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir la propiedad y el licenciamiento de la propiedad intelectual, el mantenimiento, las garantías, los procesos de arbitraje, las condiciones de actualización y la aptitud para el propósito definido, incluyendo seguridad, depósito de garantía y derechos de acceso.		Aplica	Completa	5
5. En el caso específico de la adquisición de desarrollos, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir la propiedad y el licenciamiento de la propiedad intelectual; aptitud para el propósito definido, incluyendo metodologías, pruebas, procesos de gestión de la calidad, incluyendo los criterios de evaluación del rendimiento, formas de pago, garantías, los procesos de arbitraje, gestión de recursos humanos y cumplimiento con las políticas corporativas.		Aplica	Completa	5
6. Obtener asesoramiento legal sobre los acuerdo de adquisición de desarrollos en relación a la propiedad y el licenciamiento de propiedad intelectual.		Aplica	Completa	5
7. En el caso específico de la adquisición de infraestructuras, instalaciones y servicios relacionados, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir niveles de servicio, procedimientos de mantenimiento, controles de acceso, seguridad, revisiones de rendimiento, formas de pago y procesos de arbitraje.		Aplica	Completa	5
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.		3.25
Actividad	Evaluación	Cobertura	Calificación	
1. Asignar propietarios de la relaciones para cada proveedor y hacerles responsables de la calidad del servicio proporcionado.	Aplica	Parcial	3.5	
2. Especificar un proceso de comunicación formal y de revisión, que incluyan las interacciones con el proveedor y la planificación.	Aplica	Parcial	3.5	
3. Acordar, gestionar, mantener y renovar los contratos con los proveedores. Asegurar que los contratos son conformes con las normas corporativas y con los requisitos legales y regulatorios.	Aplica	Completa	5	
4. Incluir en los contratos con los proveedores de servicios clave disposiciones para revisar los lugares de trabajo y las prácticas y controles de la dirección o de terceras partes.	Aplica	Parcial	3.5	
5. Evaluar la eficiencia de la relación con los proveedores e identificar las mejoras necesarias.	Aplica	Parcial	3.5	
6. Definir, comunicar y acordar las maneras de implementar las mejoras requeridas en las relaciones.	Aplica	Parcial	3.5	
7. Hacer uso de los procedimientos establecidos para tratar los conflictos contractuales haciendo uso primero, siempre que sea posible, de relaciones y mecanismos de comunicación eficaces que permitan superar los problemas de servicio.	Aplica	Parcial	3.5	

CONTINÚA →

8. Definir y formalizar los roles y responsabilidades de cada proveedor. Cuando varios proveedores se combinan para proporcionar un servicio, considerar asignar un rol de proveedor líder a uno de los proveedores para que asuma la responsabilidad global del contrato.		No Aplica	Nula	0
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.		3.50
Actividad		Evaluación	Cobertura	Calificación
1. Identificar, supervisar y, cuando sea apropiado, gestionar los riesgos relacionados con la capacidad del proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua.		Aplica	Parcial	3.5
2. A la hora de definir el contrato, para los riesgos potenciales, incluir una descripción clara de todos los requisitos de servicio, incluyendo depósitos de garantía, proveedores alternativos o acuerdos en suspenso para mitigar el riesgo de un posible fallo del proveedor; los aspectos de seguridad, la propiedad intelectual y los requisitos legales y regulatorios.		Aplica	Parcial	3.5
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.		4.00
Actividad		Evaluación	Cobertura	Calificación
1. Definir y documentar los criterios para supervisar el rendimiento de los proveedores alineado con los acuerdos de nivel de servicio y asegurando que el proveedor informa según estos criterios de forma regular y transparente.		Aplica	Parcial	3.5
2. Supervisar y revisar la entrega de servicios para asegurar que el proveedor está proporcionando una calidad del servicio adecuada, cumpliendo los requisitos y las condiciones de los contratos.		Aplica	Parcial	3.5
3. Revisar el rendimiento y el coste de los proveedores para asegurar que son competitivos y fiables, en comparación con proveedores alternativos y condiciones de mercado.		Aplica	Parcial	3.5
4. Solicitar revisiones independientes de las prácticas internas y los controles, si se considera necesario.		Aplica	Parcial	3.5
5. Registrar y evaluar los resultados de la revisión periódica y discutirlos con el proveedor para identificar las necesidades y oportunidades de mejora.		Aplica	Completa	5
6. Supervisar y evaluar la información externa disponible sobre el proveedor.		Aplica	Completa	5

3.4.2.11 APO11:

La aplicación de la plantilla para el proceso APO11: Gestionar la Calidad, se detalla en la Tabla 17.

Tabla 17

Plantilla para el proceso APO11

Código:	APO11	Área:	Gestión
Proceso:	Gestionar la Calidad	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			

CONTINÚA →

Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.			
Declaración del Propósito del Proceso:			
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.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	<ul style="list-style-type: none"> • Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico. • Porcentaje de servicios TI donde se obtienen los beneficios esperados. • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados. 		
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 		
13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	<ul style="list-style-type: none"> • Número de programas/proyectos en tiempo y en presupuesto. • Porcentaje de interesados satisfechos con la calidad del programa/proyecto. • Número de programas que necesitan revisiones significativas debido a defectos de calidad. • Coste de mantenimiento de las aplicaciones respecto al coste TI global. 		
Prácticas y Actividades			
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.	2.38
Actividad	Evaluación	Cobertura	Calificación
1. Asegurar que el marco de control de TI, el negocio y los procesos de TI incluyen un enfoque estándar, formal y continuo de gestión de la calidad que está alineado con los requerimientos empresariales. Dentro del marco de control de TI y de los procesos de negocio y de TI, identificar los requisitos y criterios de calidad (por ejemplo, sobre la base de los requerimientos legales y los requisitos de los clientes).	No Aplica	Nula	0
2. Definir roles, tareas, capacidades de decisión y responsabilidades para la gestión de la calidad, dentro de la estructura organizativa.	Aplica	Completa	5
3. Definir planes de gestión de la calidad para los procesos, proyectos u objetivos importantes, que estén alineados con los criterios y políticas del sistema de la calidad a nivel corporativo. Registrar los datos relacionados con la calidad.	Aplica	Nula	0
4. Supervisar y medir la eficacia y la aceptación de la gestión de la calidad, y mejorarla cuando sea necesario.	Aplica	Parcial	3.5
5. Alinear la gestión de la calidad TI con la gestión de la calidad a nivel corporativo fomentando un enfoque de la calidad estandarizado y continuo.	Aplica	Parcial	3.5
6. Obtener los inputs necesarios de las partes interesadas internas y externas para la definición de los requisitos y los criterios de aceptación de la calidad.	Aplica	Parcial	3.5

CONTINÚA →

7. Comunicar de manera eficaz el enfoque (por ejemplo, mediante programas de formación en calidad formales y regulares).			Aplica	Parcial	3.5
8. Revisar periódicamente la relevancia, eficiencia y eficacia de los procesos específicos de gestión de calidad. Supervisar el cumplimiento de los objetivos de la calidad.			No Aplica	Nula	0
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.	1.75		
Actividad			Evaluación	Cobertura	Calificación
1. Definir las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI. Hacer uso de las mejores prácticas de la industria como referencia para la mejora y adaptación de los procesos de gestión de la calidad de la empresa.			Aplica	Parcial	3.5
2. Considerar los costes y los beneficios de las certificaciones de calidad.			No Aplica	Nula	0
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.	3.50		
Actividad			Evaluación	Cobertura	Calificación
1. Enfocar la gestión de la calidad en los clientes, mediante la determinación los requisitos de los clientes externos e internos y asegurando su el alineamiento de las normas y prácticas de TI. Definir y comunicar los roles y responsabilidades relativos a la resolución de conflictos entre clientes/ usuarios y la organización TI.			Aplica	Parcial	3.5
2. Gestionar las necesidades y las expectativas del negocio para cada proceso de negocio, servicio operativo y nuevas soluciones de TI y mantener sus criterios de aceptación de la calidad. Capturar los criterios de aceptación de la calidad para su inclusión en los ANS.			Aplica	Parcial	3.5
3. Comunicar los requisitos y expectativas del cliente por toda la organización de negocio y de TI.			Aplica	Parcial	3.5
4. Obtener periódicamente los puntos de vista del cliente sobre los procesos de negocio y la provisión de servicios y la entrega de soluciones TI, para determinar el impacto sobre las normas y prácticas de TI y garantizar que se cumplen las expectativas de los clientes y se actúa en consecuencia.			Aplica	Parcial	3.5
5. Supervisar y revisar regularmente que el SGC está de acuerdo a los criterios de aceptación de la calidad. Incluir los comentarios de los clientes, usuarios y la dirección. Responder a las discrepancias en los resultados de las revisiones para lograr una mejorar continua del SGC.			Aplica	Parcial	3.5
6. Capturar los criterios de aceptación de la calidad para su inclusión en los ANS.			Aplica	Parcial	3.5
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.	2.21		
Actividad			Evaluación	Cobertura	Calificación
1. Supervisar la calidad de los procesos y servicios de forma permanente y sistemática mediante la descripción, las métricas, los análisis, la mejora/ ingeniería y controles de los procesos.			No Aplica	Nula	0
2. Preparar y llevar a cabo revisiones de calidad.			Aplica	Completa	5

CONTINUA →

3. Informar de los resultados de las revisiones y poner en marcha las mejoras necesarias.		Aplica	Parcial	3.5
4. Supervisar la calidad de los procesos, así como el valor proporcionado por la calidad. Asegurar que la medición, supervisión y registro de la información es utilizada por los propietarios de los procesos para tomar las acciones correctivas y preventivas necesarias.		No Aplica	Nula	0
5. Supervisar las métricas de calidad basadas en objetivos alineadas con los objetivos generales de calidad y cubriendo la calidad de todos los servicios y los proyectos individuales.		Aplica	Parcial	3.5
6. Asegurar que la dirección y los propietarios de los procesos revisan periódicamente el rendimiento de la gestión respecto a las métricas de calidad definidas.		No Aplica	Nula	0
7. Analizar los resultados del rendimiento de la gestión de la calidad global.		Aplica	Parcial	3.5
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 desarrollo de soluciones y los servicios ofrecidos.		2.83
Actividad		Evaluación	Cobertura	Calificación
1. Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.		No Aplica	Parcial	0
2. Supervisar de manera continua los niveles de servicio e incorporar prácticas de gestión de la calidad en todos los procesos y prácticas de prestación de servicios.		Aplica	Parcial	3.5
3. Identificar y documentar las causas raíz de las no conformidades y comunicar los resultados a la dirección de TI y otras partes interesadas de manera oportuna para permitir que se adopten las medidas correctivas oportunas. Cuando sea necesario, realizar el seguimiento de las revisiones.		Aplica	Completa	5
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.		3.06
Actividad		Evaluación	Cobertura	Calificación
1. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua.		Aplica	Parcial	3.5
2. Establecer una plataforma para compartir las mejores prácticas y para capturar la información sobre los defectos y errores que permita aprender de ellos.		No Aplica	Nula	0
3. Identificar ejemplos recurrentes de los defectos de calidad, determinar su causa raíz, evaluar su impacto y resultado y acordar acciones de mejora con todos los miembros de los proyectos y los servicios.		Aplica	Parcial	3.5
4. Identificar ejemplos recurrentes de los defectos de calidad, determinar su causa raíz, evaluar su impacto y resultado y acordar acciones de mejora con todos los miembros de los proyectos y los servicios.		Aplica	Parcial	3.5
5. Promover una cultura de calidad y mejora continua.		Aplica	Parcial	3.5
6. Establecer un circuito de retroalimentación entre la gestión de la calidad y la gestión de problemas.		Aplica	Parcial	3.5
7. Proporcionar a los empleados la formación necesaria en los métodos y herramientas de mejora continua.		Aplica	Parcial	3.5
8. Realizar un análisis comparativo con los resultados de las revisiones de calidad internas frente a datos históricos, las directrices de la industria, las normas y datos de tipo similar en otras empresas.		Aplica	Parcial	3.5

3.4.2.12 APO12:

La aplicación de la plantilla para el proceso APO12: Gestionar el Riesgo, se detalla en la Tabla 18.

Tabla 18

Plantilla para el proceso APO12

Código:	APO12	Área:	Gestión
Proceso:	Gestionar el Riesgo	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.			
Declaración del Propósito del Proceso:			
Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	<ul style="list-style-type: none"> • Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación. • Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos. • Número de incumplimientos relacionados con proveedores de servicios TI. • Cobertura de evaluaciones de cumplimiento. 		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI. • Frecuencia de actualización del perfil de riesgo. 		
06 Transparencia de los costes, beneficios y riesgos de las TI.	<ul style="list-style-type: none"> • Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI 		
10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones.	<ul style="list-style-type: none"> • Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública. • Número de servicios TI sin requerimientos de seguridad destacables. • Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados. • Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías 		

CONTINÚA →

13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.		<ul style="list-style-type: none"> • Número de programas/proyectos en tiempo y en presupuesto. • Porcentaje de interesados satisfechos con la calidad del programa/proyecto. • Número de programas que necesitan revisiones significativas debido a defectos de calidad. • Coste de mantenimiento de las aplicaciones respecto al coste TI global. 		
Prácticas y Actividades				
APO12.01	Recopilar datos.	Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.		4.57
Actividad		Evaluación	Cobertura	Calificación
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.		Aplica	Parcial	3.5
2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.		Aplica	Parcial	3.5
3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.		Aplica	Completa	5
4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.		Aplica	Completa	5
5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes.		Aplica	Completa	5
6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.		Aplica	Completa	5
7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.		Aplica	Completa	5
APO12.02	Analizar el riesgo.	Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.		4.14
Actividad		Evaluación	Cobertura	Calificación
1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.		Aplica	Completa	5
2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.		Aplica	Parcial	3.5
3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.		Aplica	Completa	5
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.		Aplica	Parcial	3.5

CONTINÚA →

5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ capturar. Proponer la respuesta al riesgo óptima.		Aplica	Completa	5
6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.		Aplica	Parcial	3.5
7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.		Aplica	Parcial	3.5
APO12.03	Mantener un perfil de riesgo.	Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.		4.36
Actividad		Evaluación	Cobertura	Calificación
1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.		Aplica	Parcial	3.5
2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.		Aplica	Completa	5
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.		Aplica	Parcial	3.5
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.		Aplica	Parcial	3.5
5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.		Aplica	Completa	5
6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.		Aplica	Completa	5
7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.		Aplica	Completa	5
APO12.04	Expresar el riesgo.	Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.		4.10
Actividad		Evaluación	Cobertura	Calificación
1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.		Aplica	Parcial	3.5
2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.		Aplica	Completa	5
3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.		Aplica	Completa	5

CONTINÚA →

4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.		Aplica	Parcial	3.5
5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.		Aplica	Parcial	3.5
APO12.05	Definir un portafolio de acciones para la gestión de riesgos.	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.		4.00
Actividad		Evaluación	Cobertura	Calificación
1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.		Aplica	Completa	5
2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.		Aplica	Parcial	3.5
3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.		Aplica	Parcial	3.5
APO12.06	Responder al riesgo.	Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.		4.25
Actividad		Evaluación	Cobertura	Calificación
1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.		Aplica	Completa	5
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.		Aplica	Completa	5
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.		Aplica	Parcial	3.5
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.		Aplica	Parcial	3.5

3.4.2.13 APO13:

La aplicación de la plantilla para el proceso APO13: Gestionar la Seguridad, se detalla en la Tabla 19.

Tabla 19

Plantilla para el proceso APO13

Código:	APO13	Área:	Gestión
Proceso:	Gestionar la Seguridad	Dominio:	Alinear, Planificar y Orientar
Descripción del Proceso:			
Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.			
Declaración del Propósito del Proceso:			
Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	<ul style="list-style-type: none"> • Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación. • Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos. • Número de incumplimientos relacionados con proveedores de servicios TI. • Cobertura de evaluaciones de cumplimiento. 		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI. • Frecuencia de actualización del perfil de riesgo. 		
06 Transparencia de los costes, beneficios y riesgos de las TI.	<ul style="list-style-type: none"> • Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI 		
10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones.	<ul style="list-style-type: none"> • Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública. • Número de servicios TI sin requerimientos de seguridad destacables. • Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados. • Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías 		
14 Disponibilidad de información útil y relevante para la toma de decisiones.	<ul style="list-style-type: none"> • Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión. • Número de incidentes de procesos de negocio causados por la indisponibilidad de la información. • Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave. 		
Prácticas y Actividades			
APO13.01	Establecer y mantener un SGSI.	Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa.	3.64

CONTINÚA →

Actividad			Evaluación	Cobertura	Calificación
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.			Aplica	Completa	5
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.			Aplica	Parcial	3.5
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.			Aplica	Completa	5
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.			No Aplica	Nula	0
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.			Aplica	Parcial	3.5
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.			Aplica	Completa	5
7. Comunicar el enfoque de SGSI.			Aplica	Parcial	3.5
APO13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.			3.93
Actividad			Evaluación	Cobertura	Calificación
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riesgos identificados de seguridad de información.			Aplica	Parcial	3.5
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.			Aplica	Parcial	3.5
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.			Aplica	Parcial	3.5
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.			Aplica	Parcial	3.5
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.			Aplica	Parcial	3.5
6. Recomendar programas de formación y concienciación en seguridad de la información.			Aplica	Completa	5
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.			Aplica	Completa	5

CONTINÚA →

APO13.03	Supervisar y revisar el SGSI.	Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	3.50
Actividad	Evaluación	Cobertura	Calificación
1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.	Aplica	Parcial	3.5
2. Realizar auditorías internas al SGSI a intervalos planificados.	Aplica	Parcial	3.5
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.	Aplica	Parcial	3.5
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.	Aplica	Parcial	3.5
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.	Aplica	Parcial	3.5

3.4.3 Dominio Supervisar/Evaluar/Valorar (MEA).

El tercer dominio también es de Gestión de TI y se denomina Supervisar, Evaluar y Valorar, identificado por sus siglas en inglés como MEA, a continuación se expone el ejercicio de evaluación para los procesos del mismo.

3.4.3.1 MEA01:

La aplicación de la plantilla para el proceso MEA01: Supervisar, Evaluar y Valorar Rendimiento y Conformidad, se detalla en la Tabla 20.

Tabla 20

Plantilla para el proceso MEA01

Código:	MEA01	Área:	Gestión
Proceso:	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	Dominio:	Supervisar, Evaluar y Valorar
Descripción del Proceso:			
Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.			
Declaración del Propósito del Proceso:			

CONTINÚA →

Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen TI. • Frecuencia de actualización del perfil de riesgo. 		
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> • Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI 		
11 Optimización de activos, recursos y capacidades de las TI.	<ul style="list-style-type: none"> • 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 la alta dirección del negocio y de TI con los costes y capacidades TI. 		
15 Cumplimiento de las políticas internas por parte de las TI.	<ul style="list-style-type: none"> • Número de incidentes relacionados con el incumplimiento de políticas. • Porcentaje de interesados que entienden las políticas. • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas. • Frecuencia de revisión y actualización de políticas. 		
Prácticas y Actividades			
MEA01.01	Establecer un enfoque de la supervisión.	Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.	2.50
Actividad	Evaluación	Cobertura	Calificación
1. Identificar las partes interesadas (p. ej. dirección, propietarios de procesos o usuarios).	No Aplica	Nula	0
2. Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes (p. ej. glosario corporativo, metadatos y taxonomías), líneas de referencia y estudios comparativos (benchmarking).	Aplica	Parcial	3.5
3. Mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía así como las herramientas utilizadas para la obtención de datos y presentación de informes corporativos (p. ej. aplicaciones de inteligencia de negocio).	Aplica	Parcial	3.5
4. Acordar los objetivos y métricas (p. ej., cumplimiento, rendimiento, valor, riesgo), taxonomía (clasificación y relación entre objetivos y métricas) y la retención de datos (evidencias).	Aplica	Parcial	3.5

CONTINÚA →

5. Acordar un proceso de control de cambios y de gestión del ciclo de vida de la supervisión y la presentación de informes. Incluir oportunidades de mejora para la presentación de la información, métricas, enfoque, líneas de referencia y estudios comparativos.		No Aplica	Nula	0
6. Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).		Aplica	Parcial	3.5
7. Validar periódicamente el enfoque utilizado e identificar los nuevos o cambiantes grupos de interés, requisitos y recursos.		Aplica	Parcial	3.5
Prácticas y Actividades				
MEA01.02	Establecer los objetivos de cumplimiento y rendimiento.	Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.		3.50
Actividad		Evaluación	Cobertura	Calificación
1. Definir y revisar periódicamente los objetivos y métricas con las partes interesadas para identificar cualquier detalle significativo omitido y definir la razonabilidad de metas y tolerancias.		Aplica	Parcial	3.5
2. Comunicar los cambios propuestos en las metas y tolerancias de rendimiento y cumplimiento (referidos a las métricas) con las partes interesadas clave con la debida diligencia (p. ej., legal, auditoría, RR.HH., ética, cumplimiento y financiero).		Aplica	Parcial	3.5
3. Hacer público a los usuarios de la información los cambios en metas y tolerancias.		Aplica	Parcial	3.5
4. Evaluar si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).		Aplica	Parcial	3.5
Prácticas y Actividades				
MEA01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.		2.80
Actividad		Evaluación	Cobertura	Calificación
1. Recopilar datos de los procesos definidos, de forma automatizada, cuando sea posible.		No Aplica	Nula	0
2. Evaluar la eficiencia (esfuerzo en relación con la comprensión detallada proporcionada) y oportunidad (utilidad y significado) y validar la integridad (precisión y completitud) de los datos recopilados.		Aplica	Parcial	3.5
3. Consolidar los datos para soportar el cálculo de las métricas acordadas.		Aplica	Parcial	3.5
4. Alinear los datos consolidados a los enfoques y objetivos de presentación de información de la compa		Aplica	Parcial	3.5
5. Utilizar herramientas y sistemas apropiados para el procesamiento y formateo de datos para análisis.		Aplica	Parcial	3.5
Prácticas y Actividades				
MEA01.04	Analizar e informar sobre el rendimiento.	Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de Supervisión.		2.33
Actividad		Evaluación	Cobertura	Calificación

CONTINÚA →

1. Diseñar informes de rendimiento de procesos que sean concisos, fáciles de entender y ajustados a las diferentes necesidades de gestión y audiencias. Facilitar la toma efectiva y oportuna de decisiones (p. ej., cuadros de mando, informes con semáforos) y asegurar que la causa y el efecto entre objetivos y métricas se comunican de una forma comprensible.	No Aplica	Nula	0
2. Comparar los valores de rendimiento con metas y estudios comparativos internos (benchmarks) y, cuando sea posible, con estudios comparativos externos (tanto del sector, como respecto a competidores clave).	Aplica	Parcial	3.5
3. Recomendar cambios a los objetivos y métricas, cuando sea procedente	Aplica	Parcial	3.5
4. Distribuir los informes a las partes interesadas relevantes.	Aplica	Parcial	3.5
5. Analizar la causa de las desviaciones respecto a las metas, iniciar acciones correctivas, asignar responsabilidades para la remediación y realizar su seguimiento. En el momento oportuno, revisar todas las desviaciones y buscar causas raíz cuando sea necesario. Documentar las incidencias para contar con guía adicional si el problema vuelve a aparecer. Documentar los resultados.	Aplica	Parcial	3.5
6. Cuando sea factible, enlazar el cumplimiento de objetivos de desempeño con el sistema de compensación y gratificación de la organización.	No Aplica	Nula	0
Prácticas y Actividades			
MEA01.05	Asegurar la implantación de medidas correctivas.	Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.	4.63
Actividad	Evaluación	Cobertura	Calificación
1. Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores	Aplica	Completa	5
2. Asegurar que se mantiene la asignación de responsabilidades en las acciones correctivas.	Aplica	Completa	5
3. Hacer seguimiento de los resultados de las acciones comprometidas.	Aplica	Parcial	3.5
4. Informar de los resultados a las partes interesadas.	Aplica	Completa	5

3.4.3.2 MEA02:

La aplicación de la plantilla para el proceso MEA02: Supervisar, Evaluar y Valorar el Sistema de Control Interno, se detalla en la Tabla 21.

Tabla 21

Plantilla para el proceso MEA02

Código:	MEA02	Área:	Gestión
Proceso:	Supervisar, Evaluar y Valorar el Sistema de Control Interno	Dominio:	Supervisar, Evaluar y Valorar
Descripción del Proceso:			

CONTINÚA →

Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.			
Declaración del Propósito del Proceso:			
Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	<ul style="list-style-type: none"> • Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación. • Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos. • Número de incumplimientos relacionados con proveedores de servicios TI. • Cobertura de evaluaciones de cumplimiento. 		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen TI. • Frecuencia de actualización del perfil de riesgo. 		
15 Cumplimiento de las políticas internas por parte de las TI.	<ul style="list-style-type: none"> • Número de incidentes relacionados con el incumplimiento de políticas. • Porcentaje de interesados que entienden las políticas. • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas. • Frecuencia de revisión y actualización de políticas 		
Prácticas y Actividades			
MEA02.01	Supervisar el control interno.	Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.	3.93
Actividad	Evaluación	Cobertura	Calificación
1. Realizar actividades de evaluación y supervisión del control interno basadas en los estándares de gobierno organizativos y los marcos y prácticas aceptadas en la industria. Incluir el seguimiento y evaluación de la eficiencia y efectividad de las revisiones de supervisión de la Dirección.	Aplica	Parcial	3.5
2. Considerar las evaluaciones independientes del sistema de control interno (p. ej. por auditoría interna o iguales - peers).	Aplica	Parcial	3.5
3. Identificar los límites del sistema de control interno de TI (p. ej., considerar cómo los controles internos organizativos de TI toman en consideración las actividades de producción o desarrollo externalizadas y/o deslocalizadas).	Aplica	Completa	5
4. Asegurar que las actividades de control están operativas y que las excepciones son comunicadas puntualmente, seguidas y analizadas, y que se priorizan e implementan las acciones correctivas oportunas de acuerdo con el perfil de gestión del riesgo (p. ej., clasificar ciertas excepciones como riesgos clave y otras como riesgos no-clave).	Aplica	Completa	5

CONTINÚA →

5. Mantener el sistema de control interno de TI, considerando los cambios en curso en el negocio y el riesgo de TI, el entorno de control organizativo, los procesos de negocio y de TI relevantes y el riesgo de TI. Si existen lagunas, evaluar y recomendar cambios.	Aplica	Parcial	3.5
6. Evaluar regularmente el rendimiento del marco de control de TI, realizando estudios comparativos con los estándares y buenas prácticas aceptadas por la industria. Considerar la adopción formal de un enfoque de mejora continua en la supervisión de control interno.	Aplica	Parcial	3.5
7. Evaluar el estado de los controles internos de los proveedores externos de servicios y confirmar que dichos proveedores cumplen con los requisitos legales y regulatorios, así como las obligaciones contractuales.	Aplica	Parcial	3.5
Prácticas y Actividades			
MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.	5.00
Actividad	Evaluación	Cobertura	Calificación
1. Entender y priorizar el riesgo de acuerdo con los objetivos organizativos.	Aplica	Completa	5
2. Identificar los controles clave y desarrollar una estrategia adecuada para la validación de controles.	Aplica	Completa	5
3. Identificar la información que indica de forma convincente si el entorno de control interno está operando de forma efectiva.	Aplica	Completa	5
4. Desarrollar e implementar procedimientos eficientes para determinar si la información convincente está basada en los criterios de información	Aplica	Completa	5
5. Mantener evidencia de la efectividad del control.	Aplica	Completa	5
Prácticas y Actividades			
MEA02.03	Realizar autoevaluaciones de control.	Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.	4.14
Actividad	Evaluación	Cobertura	Calificación
1. Mantener planes y alcances e identificar los criterios de evaluación para la realización de las autoevaluaciones. Planificar la comunicación de resultados del proceso de autoevaluación al negocio, TI y Dirección General y al Consejo. Considerar estándares diseño de autoevaluaciones.	Aplica	Parcial	3.5
2. Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua.	Aplica	Parcial	3.5
3. Asignar la responsabilidad de la autoevaluación a las personas oportunas con el fin de asegurar la objetividad y la competencia.	Aplica	Parcial	3.5
4. Proporcionar revisiones independientes para asegurar la objetividad de la autoevaluación y hacer posible compartir las buenas prácticas de control interno con otras compañías.	Aplica	Completa	5

CONTINÚA →

5. Comparar los resultados de las autoevaluaciones con estándares y buenas prácticas de la industria.		Aplica	Parcial	3.5
6. Resumir y comunicar los resultados de las autoevaluaciones y los estudios comparativos para considerar acciones correctivas.		Aplica	Completa	5
7. Definir un enfoque consistente y consensuado para la realización de autoevaluaciones de control y para la coordinación con auditores internos y externos.		Aplica	Completa	5
Prácticas y Actividades				
MEA02.04	Identificar y las deficiencias de control.	Identificar deficiencias de control y analizar e identificar las causas raíz subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.		4.25
Actividad		Evaluación	Cobertura	Calificación
1. Identificar, comunicar y registrar las excepciones de los controles y asignar responsabilidad de su resolución y comunicación de los resultados.		Aplica	Completa	5
2. Considerar el riesgo para la empresa al establecer umbrales para el escalado de las excepciones y desajustes de los controles.		Aplica	Parcial	3.5
3. Comunicar los procedimientos de escalado de las excepciones de control, análisis de causas raíz e información a los propietarios del proceso y grupos de interés de TI.		Aplica	Parcial	3.5
4. Decidir qué excepciones de control deberían ser comunicadas a la persona responsable de la función y qué excepciones deberían ser escaladas. Informar a las partes interesadas y propietarios de los procesos afectados.		Aplica	Parcial	3.5
5. Hacer seguimiento de todas las excepciones para asegurar que se han contemplado las acciones acordadas.		Aplica	Completa	5
6. Identificar, iniciar, rastrear e implementar acciones correctivas que surjan de la evaluación de control e informes.		Aplica	Completa	5
Prácticas y Actividades				
MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.		5.00
Actividad		Evaluación	Cobertura	Calificación
1. Establecer la adhesión a los códigos de ética y estándares aplicables (p. ej., el Código de Ética Profesional de ISACA) y estándares de aseguramiento (relativos a la industria o ámbito geográfico), p. ej. Estándares de aseguramiento y auditoría de TI de ISACA y Marco Internacional para el Aseguramiento del Comité Internacional para los Estándares de Auditoría y Aseguramiento (IAASB).		Aplica	Completa	5
2. Establecer la independencia de los proveedores de aseguramiento.		Aplica	Completa	5
3. Establecer la competencia y cualificación de los proveedores de aseguramiento.		Aplica	Completa	5
Prácticas y Actividades				
MEA02.06	Planificar iniciativas de aseguramiento.	Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.		4.00

CONTINÚA →

Actividad				Evaluación	Cobertura	Calificación
1. Determinar los destinatarios de las salidas de la iniciativa de aseguramiento y el objeto de la revisión.				Aplica	Parcial	3.5
2. Realizar una evaluación del riesgo a alto nivel y/o evaluar la capacidad del proceso para diagnosticar el riesgo e identificar los procesos críticos de TI.				Aplica	Parcial	3.5
3. Seleccionar, adaptar y llegar a un acuerdo sobre los objetivos de control para los procesos críticos que serán la base para la evaluación de control.				Aplica	Completa	5
Prácticas y Actividades						
MEA02.07	Estudiar las iniciativas de las de aseguramiento.	Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.	3.80			
Actividad				Evaluación	Cobertura	Calificación
1. Definir el alcance actual mediante la identificación de los objetivos empresariales y de TI para el entorno bajo estudio, el conjunto de procesos y recursos de TI y todas las entidades auditables relevantes dentro de la compañía y externas a la compañía (p. ej. proveedores de servicios), si aplica.				Aplica	Parcial	3.5
2. Definir el plan de participación y los recursos necesarios				Aplica	Completa	5
3. Definir las prácticas de recolección y evaluación de la información de los procesos bajo revisión para identificar los controles a ser validados y los hallazgos reales (tanto aseguramiento positivo como cualquier deficiencia) para la evaluación del riesgo.				Aplica	Parcial	3.5
4. Definir prácticas para validar el diseño de controles y resultados y determinar si el nivel de efectividad es compatible con el riesgo aceptable (requerido por la evaluación de riesgos organizativos o de los procesos).				Aplica	Parcial	3.5
5. Donde la efectividad del control no es aceptable, definir prácticas para identificar el riesgo residual (en preparación para los informes).				Aplica	Parcial	3.5
Prácticas y Actividades						
MEA02.08	Ejecutar las iniciativas de aseguramiento.	Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.	3.50			
Actividad				Evaluación	Cobertura	Calificación
1. Refinar la comprensión en materia de aseguramiento de TI.				Aplica	Parcial	3.5
2. Refinar el alcance de los objetivos de control clave en materia de aseguramiento de TI.				Aplica	Parcial	3.5
3. Probar la efectividad del diseño de control de los objetivos clave de control.				Aplica	Parcial	3.5
4. Alternativamente/adicionalmente probar los resultados de los objetivos clave de control.				Aplica	Parcial	3.5
5. Documentar el impacto de las debilidades de control.				Aplica	Parcial	3.5
6. Comunicarse con la Dirección durante la ejecución de la iniciativa para que haya un entendimiento claro del trabajo realizado, así como conformidad y aceptación de los hallazgos preliminares y recomendaciones.				Aplica	Parcial	3.5
7. Supervisar las actividades de aseguramiento y asegurar que el trabajo realizado está completo, cumple con sus objetivos y tiene una calidad aceptable.				Aplica	Parcial	3.5

CONTINÚA →

8. Proveer a la Dirección de un informe (alineado con los términos de referencia, alcance y estándares de comunicación acordados) que respalde los resultados de la iniciativa y haga hincapié en las cuestiones clave y las acciones importantes.	Aplica	Parcial	3.5
--	--------	---------	-----

3.4.3.3 MEA03:

La aplicación de la plantilla para el proceso MEA03: Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos, se detalla en la Tabla 22.

Tabla 22

Plantilla para el proceso MEA03

Código:	MEA03	Área:	Gestión
Proceso:	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Dominio:	Supervisar, Evaluar y Valorar
Descripción del Proceso:			
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.			
Declaración del Propósito del Proceso:			
Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	<ul style="list-style-type: none"> • Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación. • Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos. • Número de incumplimientos relacionados con proveedores de servicios TI. • Cobertura de evaluaciones de cumplimiento. 		
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none"> • Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo. • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos. • Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI. • Frecuencia de actualización del perfil de riesgo. 		
Prácticas y Actividades			
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.	4.25
Actividad	Evaluación	Cobertura	Calificación

CONTINÚA →

1. Asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos aplicables a la utilización de recursos de TI y al procesamiento de la información dentro de las operaciones de negocio y de TI.	Aplica	Completa	5
2. Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de TI en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo.	Aplica	Completa	5
3. Valorar el impacto de los requisitos legales y regulatorios relacionados con TI sobre los contratos con terceros que afecten a las operaciones de TI, los proveedores de servicio y los socios de negocio.	Aplica	Completa	5
4. Obtener asesoramiento independiente, si procede, sobre las modificaciones en las legislaciones, regulaciones y estándares aplicables.	Aplica	Parcial	3.5
5. Mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales aplicables, su impacto y las acciones necesarias.	Aplica	Parcial	3.5
6. Mantener un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa.	Aplica	Parcial	3.5
Prácticas y Actividades			
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.	5.00
Actividad	Evaluación	Cobertura	Calificación
1. Revisar y ajustar con regularidad las políticas, los principios, los estándares, los procedimientos y las metodologías para que mantengan su eficacia en asegurar el cumplimiento requerido y la gestión del riesgo empresarial. Contar para ello con expertos internos y externos, según proceda.	Aplica	Completa	5
2. Comunicar los nuevos requisitos y las modificaciones de los existentes al personal que corresponda.	Aplica	Completa	5
Prácticas y Actividades			
MEA03.03	Confirmar el cumplimiento de los requisitos externos.	Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.	3.38
Actividad	Evaluación	Cobertura	Calificación
1. Evaluar regularmente las políticas, estándares, procedimientos y metodologías de la organización para todas las funciones corporativas con objeto de asegurar el cumplimiento de los requisitos legales y regulatorios aplicables al procesamiento de información.	Aplica	Parcial	3.5
2. Gestionar las deficiencias de cumplimiento en las políticas, estándares y procedimientos dentro de plazos razonables.	Aplica	Completa	5
3. Evaluar periódicamente los procesos y actividades tanto de TI como de negocio para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.	No Aplica	Nula	0
4. Revisar regularmente para detectar patrones reiterados de fallos de cumplimiento. Si procede, mejorar tanto las políticas, los estándares, los procedimientos y las metodologías como los procesos y actividades asociados.	Aplica	Completa	5

CONTINÚA →

Prácticas y Actividades			
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.	4.00
Actividad	Evaluación	Cobertura	Calificación
1. Obtener confirmación regularmente del cumplimiento de las políticas internas por parte de los propietarios de procesos de TI y de negocio, así como de los directores de las unidades.	Aplica	Completa	5
2. Realizar revisiones regulares internas y externas (y, si procede, independientes) para evaluar los niveles de cumplimiento.	Aplica	Completa	5
3. Si es necesario, obtener declaraciones de los proveedores de servicio TI externos acerca de su nivel de cumplimiento con las leyes y regulaciones aplicables.	Aplica	Parcial	3.5
4. Si es necesario, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento de las leyes y regulaciones en materia de transacciones electrónicas entre compañías.	Aplica	Parcial	3.5
5. Supervisar e informar de los incidentes de incumplimiento y, si es necesario, investigar la causa raíz.	Aplica	Parcial	3.5
6. Consolidar a nivel empresarial los informes sobre requisitos legales, regulatorios y contractuales, involucrando a todas las unidades de negocio.	Aplica	Parcial	3.5

3.4.4 Evaluación de Gestión y Gobierno:

Una vez que se han consolidado las matrices se obtiene el resultado de la evaluación en BanCodesarrollo para cada una de las prácticas de los procesos catalizadores, tanto en el ámbito de gobierno como en el ámbito de gestión de TI.

Las prácticas con puntuación inferior al límite se han sombreado de color rojo, mientras que los nombres de las prácticas de procesos de riesgos se han sombreado con color azul, las puntuaciones obtenidas se presentan en la Tabla 23.

Tabla 23

Resultados de las prácticas en los dominios evaluados.

Proceso	Práctica	Nombre	Evaluación
APO01	APO01.01	Definir la estructura organizativa	4,88
APO01	APO01.02	Establecer roles y responsabilidades	5,00
APO01	APO01.03	Mantener los elementos catalizadores del sistema de gestión	4,50
APO01	APO01.04	Comunicar los objetivos y la dirección de gestión	5,00
APO01	APO01.05	Optimizar la ubicación de la función de TI	5,00
APO01	APO01.06	Definir la propiedad de la información (datos) y del sistema	4,25
APO01	APO01.07	Gestionar la mejora continua de los procesos	0,00
APO01	APO01.08	Mantener el cumplimiento con las políticas y procedimientos	4,10
APO02	APO02.01	Comprender la dirección de la empresa.	4,50
APO02	APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	4,63
APO02	APO02.03	Definir el objetivo de las capacidades de TI	4,00
APO02	APO02.04	Realizar un análisis de diferencias.	3,50
APO02	APO02.05	Definir el plan estratégico y la hoja de ruta.	3,93
APO02	APO02.06	Comunicar la estrategia y la dirección de TI.	3,50
APO03	APO03.01	Desarrollar la visión de la arquitectura de empresa.	3,63
APO03	APO03.02	Definir la arquitectura de referencia.	3,28
APO03	APO03.03	Seleccionar las oportunidades y las soluciones.	3,50
APO03	APO03.04	Definir la implantación de la arquitectura.	5,00
APO03	APO03.05	Proveer los servicios de arquitectura empresarial.	3,50
APO04	APO04.01	Crear un entorno favorable para la innovación.	0,70
APO04	APO04.02	Mantener un entendimiento del entorno de la empresa.	1,17
APO04	APO04.03	Supervisar y explorar el entorno tecnológico.	3,50

CONTINÚA →

APO04	APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	3,50
APO04	APO04.05	Recomendar iniciativas apropiadas adicionales.	1,75
APO04	APO04.06	Supervisar la implementación y el uso de la innovación.	0,00
APO05	APO05.01	Establecer la mezcla del objetivo de inversión.	4,10
APO05	APO05.02	Determinar la disponibilidad y las fuentes de fondos.	5,00
APO05	APO05.03	Evaluar y seleccionar los programas a financiar.	4,00
APO05	APO05.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	3,50
APO05	APO05.05	Mantener los portafolios.	2,33
APO05	APO05.06	Gestionar la consecución de beneficios.	2,33
APO06	APO06.01	Gestionar las finanzas y la contabilidad.	5,00
APO06	APO06.02	Priorizar la asignación de recursos.	5,00
APO06	APO06.03	Crear y mantener presupuestos.	4,36
APO06	APO06.04	Modelar y asignar costes.	3,75
APO06	APO06.05	Gestionar costes.	4,33
APO07	APO07.01	Mantener la dotación de personal suficiente y adecuada.	4,70
APO07	APO07.02	Identificar personal clave de TI.	3,88
APO07	APO07.03	Mantener las habilidades y competencias del personal.	3,93
APO07	APO07.04	Evaluar el desempeño laboral de los empleados.	4,44
APO07	APO07.05	Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	3,88
APO07	APO07.06	Gestionar el personal contratado.	3,06
APO08	APO08.01	Entender las expectativas del negocio.	3,93
APO08	APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	3,50
APO08	APO08.03	Gestionar las relaciones con el negocio.	3,50
APO08	APO08.04	Coordinar y comunicar.	3,88
APO08	APO08.05	Proveer datos de entrada para la mejora continua de los servicios.	2,33
APO09	APO09.01	Identificar servicios TI.	3,17
APO09	APO09.02	Catalogar servicios basados en TI.	3,50
APO09	APO09.03	Definir y preparar acuerdos de servicio.	3,50
APO09	APO09.04	Supervisar e informar de los niveles de servicio.	3,50
APO09	APO09.05	Revisar acuerdos de servicio y contratos.	3,50
APO10	APO10.01	Identificar y evaluar las relaciones y contratos con proveedores.	3,50
APO10	APO10.02	Seleccionar proveedores.	4,79
APO10	APO10.03	Gestionar contratos y relaciones con proveedores.	3,25
APO10	APO10.04	Gestionar el riesgo en el suministro.	3,50
APO10	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	4,00
APO11	APO11.01	Establecer un sistema de gestión de la calidad (SGC).	2,38

CONTINÚA →

APO11	APO11.02	Definir y gestionar los estándares, procesos y prácticas de calidad.	1,75
APO11	APO11.03	Enfocar la gestión de la calidad en los clientes.	3,50
APO11	APO11.04	Supervisar y hacer controles y revisiones de calidad.	2,21
APO11	APO11.05	Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	2,83
APO11	APO11.06	Mantener una mejora continua.	3,06
APO12	APO12.01	Recopilar datos.	4,57
APO12	APO12.02	Analizar el riesgo.	4,14
APO12	APO12.03	Mantener un perfil de riesgo.	4,36
APO12	APO12.04	Expresar el riesgo.	4,10
APO12	APO12.05	Definir un portafolio de acciones para la gestión de riesgos.	4,00
APO12	APO12.06	Responder al riesgo.	4,25
APO13	APO13.01	Establecer y mantener un SGSI.	3,64
APO13	APO13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	3,93
APO13	APO13.03	Supervisar y revisar el SGSI.	3,50
EDM01	EDM01.01	Evaluar el sistema de gobierno.	4,06
EDM01	EDM01.02	Orientar el sistema de gobierno.	3,42
EDM01	EDM01.03	Supervisar el sistema de gobierno.	4,00
EDM02	EDM02.01	Evaluar la optimización de valor.	3,69
EDM02	EDM02.02	Orientar la optimización del valor.	3,00
EDM02	EDM02.03	Supervisar la optimización de valor.	4,40
EDM03	EDM03.01	Evaluar la gestión de riesgos.	3,75
EDM03	EDM03.02	Orientar la gestión de riesgos.	3,42
EDM03	EDM03.03	Supervisar la gestión de riesgos.	3,38
EDM04	EDM04.01	Evaluar la gestión de recursos.	3,80
EDM04	EDM04.02	Orientar la gestión de recursos.	4,10
EDM04	EDM04.03	Supervisar la gestión de recursos.	3,50
EDM05	EDM05.01	Evaluar los requisitos de elaboración de informes de las partes interesadas.	3,50
EDM05	EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	3,50
EDM05	EDM05.03	Supervisar la comunicación con las partes interesadas.	3,50
MEA01	MEA01.01	Establecer un enfoque de la supervisión.	2,50
MEA01	MEA01.02	Establecer los objetivos de cumplimiento y rendimiento.	3,50
MEA01	MEA01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	2,80
MEA01	MEA01.04	Analizar e informar sobre el rendimiento.	2,33
MEA01	MEA01.05	Asegurar la implantación de medidas correctivas.	4,63
MEA02	MEA02.01	Supervisar el control interno.	3,93

CONTINÚA →

MEA02	MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	5,00
MEA02	MEA02.03	Realizar autoevaluaciones de control.	4,14
MEA02	MEA02.04	Identificar y comunicar las deficiencias de control.	4,25
MEA02	MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	5,00
MEA02	MEA02.06	Planificar iniciativas de aseguramiento.	4,00
MEA02	MEA02.07	Estudiar las iniciativas de aseguramiento.	3,80
MEA02	MEA02.08	Ejecutar las iniciativas de aseguramiento.	3,50
MEA03	MEA03.01	Identificar requisitos externos de cumplimiento.	4,25
MEA03	MEA03.02	Optimizar la respuesta a requisitos externos.	5,00
MEA03	MEA03.03	Confirmar el cumplimiento de requisitos externos.	3,38
MEA03	MEA03.04	Obtener garantía del cumplimiento de requisitos externos.	4,00

Para facilitar la identificación de los resultados y distinguir los puntajes inferiores al límite se ha generado La Figura 10 donde se muestra el valor final para cada una de las prácticas de los procesos catalizadores COBIT 5.

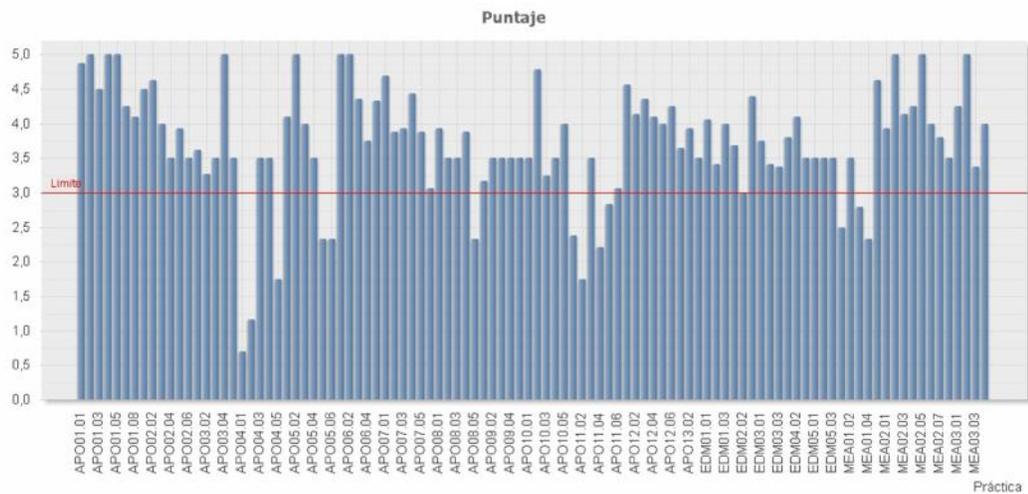


Figura 10: Resultado General de la Evaluación Tecnológica.

3.4.5 Nivel de aplicación de COBIT 5:

BanCodesarrollo no ha definido formalmente la adopción de COBIT 5, no obstante, por la naturaleza del negocio y el cumplimiento de las resoluciones del ente de control Superintendencia de Bancos y Seguros y por sus políticas de gobierno corporativo se puede apreciar un porcentaje alto de entendimiento, formalidad y aplicación implícita de COBIT 5, expresando el promedio general se alcanza el 73.17% de aplicación como se ilustra en la Figura 11.



Figura 11: Porcentaje de aplicación implícita de COBIT 5®.

Se ha considerado de mucha utilidad calcular el promedio de las prácticas agrupándolas por proceso, de tal forma que se identifiquen aquellos procesos con evaluación inferior al límite, esto es el proceso APO04 Gestionar la Innovación con 1.77 puntos y el proceso APO11 Gestionar la Calidad con 2.62 puntos como lo evidencia la Figura 12.

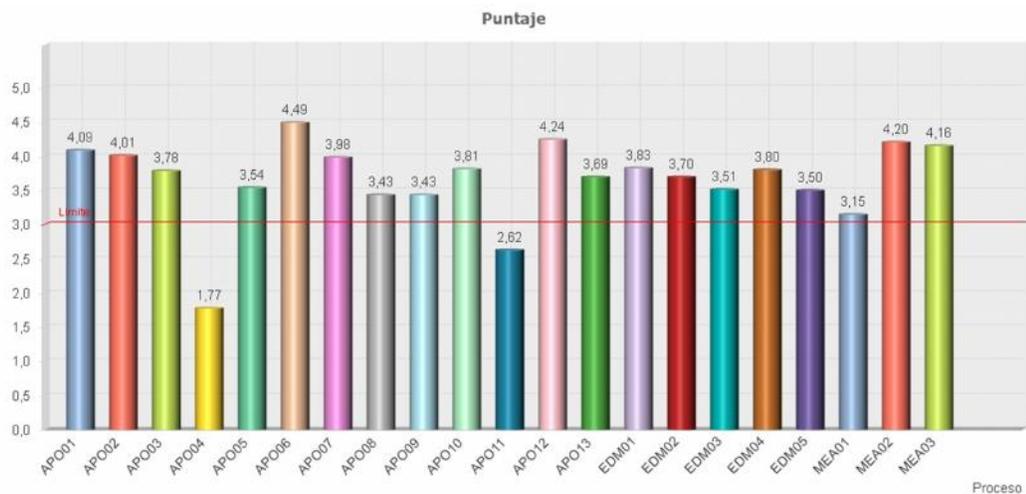


Figura 12: Resultado de Evaluación Tecnológica por Procesos.

3.5 Hallazgos de la Evaluación Tecnológica.

Se ha determinado muy útil promediar los resultados e ir revelando los hallazgos para cada dominio, sugiriendo dirigir el enfoque aquellos que reflejen valores inferiores al límite establecido, a continuación se presentan los descubrimientos por dominio.

3.5.1 Dominio Evaluar/Orientar/Supervisar (EDM).

A nivel de procesos del dominio EDM no se registran puntuaciones bajo el límite, tal como lo muestra la Figura 13.

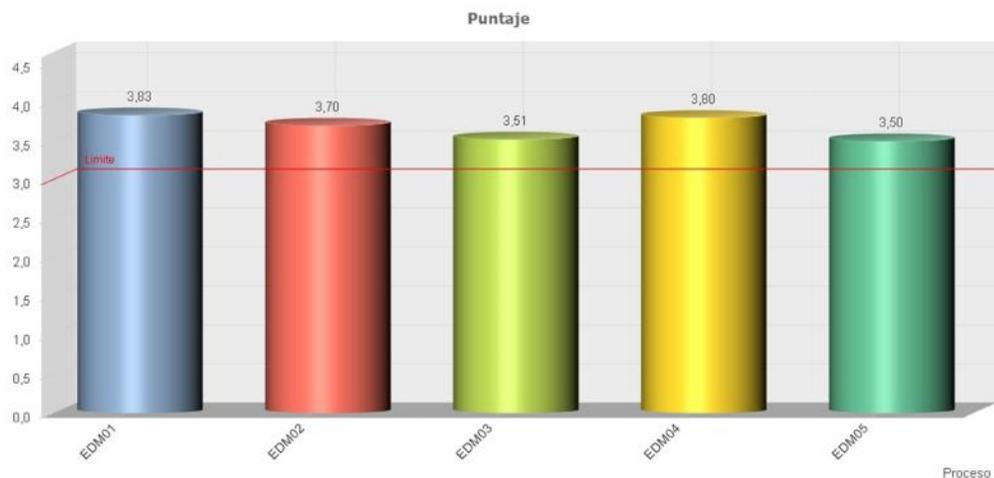


Figura 13: Evaluación Tecnológica Dominio EDM.

3.5.2 Dominio Alinear/Planear/Organizar (APO).

En el dominio APO se obtuvieron dos (2) procesos con puntuaciones bajo el límite; APO04 Gestionar la Innovación y APO 11 Gestionar la Calidad como se visualiza en la Figura 14.

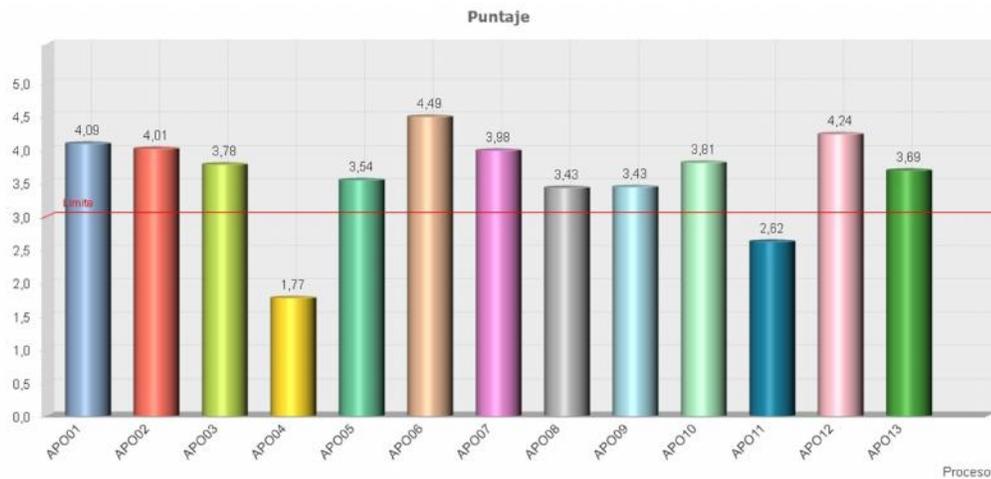


Figura 14: Evaluación Tecnológica Dominio APO.

El proceso APO04 Gestionar la Innovación, develó los hallazgos en prácticas relacionadas con el entorno de innovación, entendimiento del mismo en la empresa y la recomendación de iniciativas apropiadas, mismas que se pueden identificar en la Figura 15.

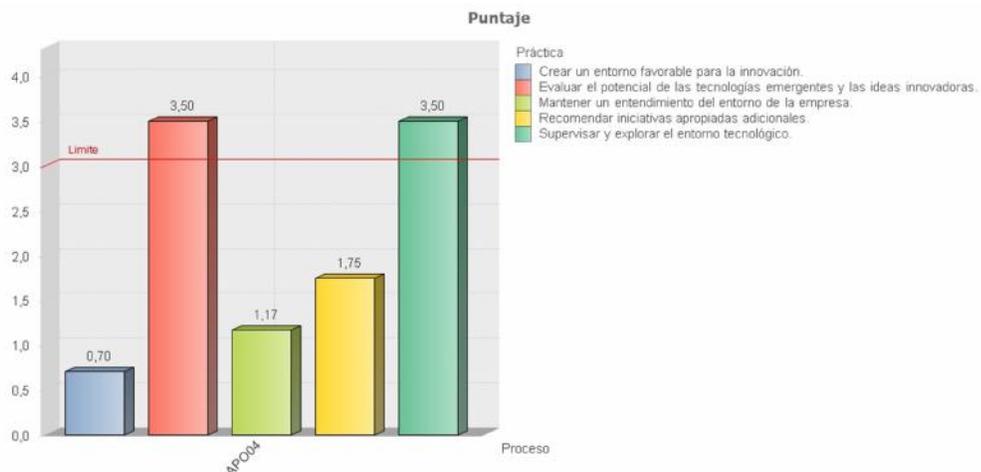


Figura 15: Hallazgos Proceso APO04.

El resultado se motiva en que en BanCodesarrollo no se aplican las siguientes actividades:

- Creación de un plan de innovación donde se incluya el apetito por el riesgo, presupuesto destinado para invertir en innovación y sus objetivos.
- Creación de un entorno que fomente la innovación manteniendo iniciativas de recursos humanos relevantes, tales como el reconocimiento de la innovación y programas de reconocimiento, la rotación apropiada en los puestos de trabajo y tiempo prudencial para la experimentación.
- Mantenimiento de un programa que permita a los empleados presentar ideas innovadoras y crear una estructura adecuada de toma de decisiones para evaluar y aplicar estas ideas.
- Animar a innovar a los clientes, proveedores y socios comerciales.
- Comprensión de los motores del negocio y de la industria, de la estrategia corporativa, operaciones corporativas y otras incidencias de modo que los potenciales valores añadidos tecnológicos o innovaciones TI puedan ser identificadas.
- Entendimiento los parámetros de inversiones corporativas para la innovación y las nuevas tecnologías, de modo que se desarrollen las estrategias adecuadas.
- Seguimiento de las pruebas de concepto para medir el grado en que las iniciativas han influenciado en las inversiones reales.
- Supervisión de la implementación y uso de la innovación.

De igual manera se encontraron novedades en el proceso APO11 Gestionar la Calidad, que se originan en el nivel de cobertura de las prácticas para la definición, seguimiento, implementación y gestión de calidad que se muestran en la Figura 16.

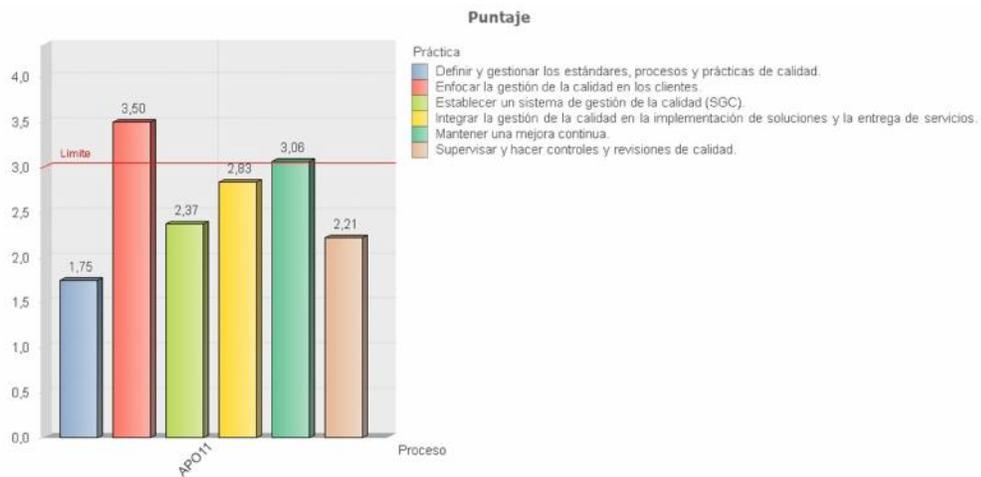


Figura 16: Hallazgos Proceso APO11.

En este caso las actividades que no se ejecutan son las siguientes:

- Aseguramiento del marco de control de TI, el negocio y los procesos de TI incluyen un enfoque estándar, formal y continuo de gestión de la calidad que está alineado con los requerimientos empresariales. Dentro del marco de control de TI y de los procesos de negocio y de TI, identificar los requisitos y criterios de calidad (por ejemplo, sobre la base de los requerimientos legales y los requisitos de los clientes).
- Definición de planes de gestión de la calidad para los procesos, proyectos u objetivos importantes, que estén alineados con los criterios y políticas del sistema de la calidad a nivel corporativo. Registrar los datos relacionados con la calidad.
- Revisión periódica de la relevancia, eficiencia y eficacia de los procesos específicos de gestión de calidad y supervisión del cumplimiento de los objetivos de la calidad.
- Consideración de los costes y los beneficios de las certificaciones de calidad.
- Supervisión y control de revisiones de calidad.
- Integración de las prácticas de gestión de calidad en los procesos de desarrollo de soluciones.

En síntesis los hallazgos hacen referencia a:

- Que la empresa identifique sus necesidades, genere estrategias que promuevan la investigación e innovación, sugiriendo emprender en iniciativas que propicien la implementación, uso y supervisión de la innovación, de manera que genere desarrollo y competitividad en el negocio.
- Se fortalezca el Sistema de Gestión de Calidad, lo que se puede alcanzar con el diseño, implementación y mejora continua de procesos donde se cuide la calidad en la implementación de soluciones y la entrega de servicios.

3.5.3 Dominio Supervisar/Evaluar/Valorar (MEA).

En el dominio MEA ninguno de los procesos registra puntuaciones bajo el límite, tal como lo revela la Figura 17.

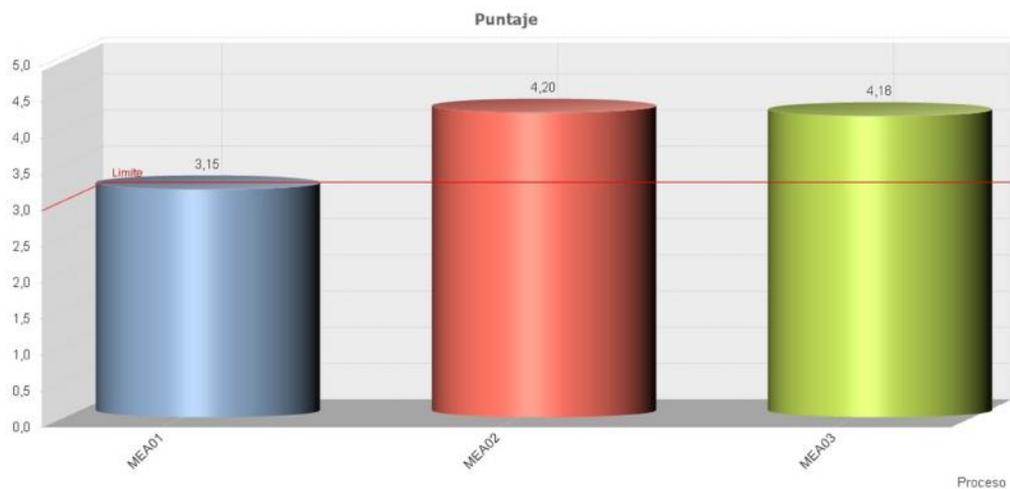


Figura 17: Evaluación Tecnológica Dominio MEA.

3.5.4 Procesos COBIT de riesgos.

Dentro de los treinta y siete (37) procesos de COBIT 5 se destacan dos procesos orientados al riesgo, sin que se deba asumir que en los demás procesos no se realice enfoque a riesgos.

A continuación se presenta el análisis realizado acorde con la metodología de trabajo.

3.5.4.1 EDM03 Asegurar la Optimización del Riesgo.

Este proceso gobierno tiene como propósito “Asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.” (ISACA, 2012)

Dicho de otra manera busca se evalúe, oriente y supervise acertadamente la gestión de riesgos, en ese contexto la institución tiene bastante atención a lo que especifica COBIT 5, como resultado de la evaluación se identificó todas las prácticas asociadas alcanzaron puntuación superior al límite, como se puede apreciar en la Figura 18.

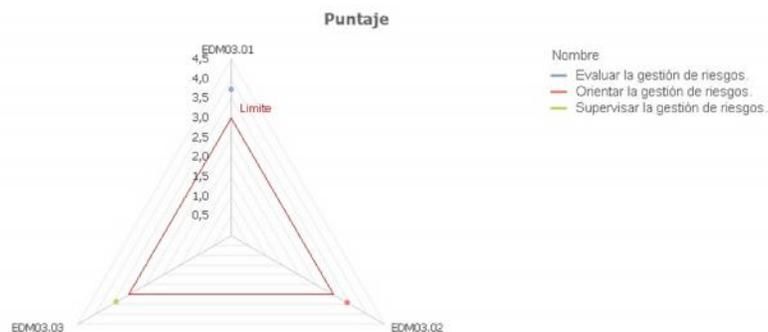


Figura 18: Riesgos en proceso EDM03.

3.5.4.2 APO 12 Gestionar el Riesgo.

Este proceso gestión tiene como propósito “Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.” (ISACA, 2012)

Es decir, la institución debe registrar datos y ocurrencia de riesgos, analizarlos, definir y mantener un perfil de riesgo para la institución, expresar transparentemente los resultados obtenidos y la exposición que la empresa tiene, para que mediante un portafolio de acciones para la gestión del riesgo de respuesta oportuna a los mismos.

De la evaluación realizada se desprende que no existen prácticas con valores bajo el límite, como lo muestra la Figura 19.

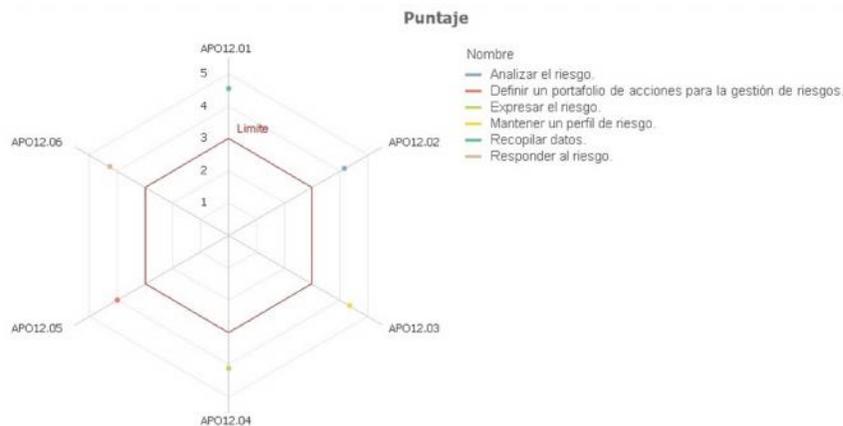


Figura 19: Riesgos en proceso APO12.

3.5.5 Controles implementados.

Después de realizado el levantamiento de información se pudo conocer que a lo largo de toda la estructura organizacional de BanCodesarrollo se han implementado controles, en observancia a la reserva que la institución ha pedido se mantenga solo se presenta una enumeración general de estos,

donde se describen el área y control, el detalle se puede conocer en la Tabla 24.

Tabla 24

Listado De Controles por Área de Negocio

LISTADO DE CONTROLES POR AREA DE NEGOCIO	
Área	Control
Desarrollo	Acceso a datos y programas
Desarrollo	Aprobación de Requerimiento de Desarrollo
Desarrollo	Autenticación e integridad en transacciones
Desarrollo	Chequeos de Integridad, Exactitud y Autenticidad
Desarrollo	Control de cambios
Desarrollo	Control de versionamiento
Desarrollo	Integridad y Validez en procesamiento
Desarrollo	Manejo de documentación
Desarrollo	Metodología desarrollo de sistemas
Desarrollo	Revisión de salidas y manejo de errores
Desarrollo	Validación de Requerimiento de Desarrollo
Operaciones	Bitácoras de operación
Operaciones	Control a contabilidad y cálculos
Operaciones	Cuadros
Operaciones	Eficiencia Operativa
Operaciones	Gestión de Calidad
Operaciones	Monitoreo de operaciones
Operaciones	Piloto
Operaciones	Planificación de salida a producción
Operaciones	Pruebas en ambientes controlados
Operaciones	Revisión de conformidad
Operaciones	Seguimiento a contratos
Operaciones	Seguimiento Postimplementación
Producción	Acceso a recursos de TI
Producción	Antivirus
Producción	Bitácoras de procesamiento
Producción	Contingencias
Producción	Cumplimiento SLAs
Producción	Firewall
Producción	Generación de respaldos
Producción	Inventario y Mantenimiento de Equipos
Producción	Monitoreo de condiciones ambientales
Producción	Monitoreo de enlaces
Producción	Procedimientos de Operación
Producción	Prueba de respaldos
Producción	Registro de respaldos

CONTINÚA →

Producción	Seguridad física en centros de datos
Riesgos	Capacitación
Riesgos	Definición de tiempos de operación y recuperación
Riesgos	Planeación de continuidad de negocios
Riesgos	Pruebas de contingencias
Riesgos	Pruebas de cumplimiento
Riesgos	Revisiones independientes de TI
Riesgos	Simulacros
Riesgos	Tratamiento de Riesgos
Seguridad Física	Autorización de Acceso
Seguridad Física	Políticas y Procedimientos de Seguridad física y lógica
Seguridad Física	Registro de Visitantes
Seguridad Física	Solicitud de identificación
Seguridad Física	Video vigilancia
Seguridad Informática	Control de privilegios
Seguridad Informática	Incompatibilidad de funciones
Seguridad Informática	Registro de incidentes de seguridad
Seguridad Informática	Registro de pistas de auditoría
Seguridad Informática	Registro de violaciones de acceso
Seguridad Informática	Seguridad perimetral
Subgerencia de Operaciones	Control presupuestario
Subgerencia de Operaciones	Continuidad del Negocio
Subgerencia de Operaciones	Gestión de adquisiciones
Subgerencia de Operaciones	Planificación Estratégica
Subgerencia de Operaciones	Revisión de políticas y procedimientos
Subgerencia de Operaciones	Segregación de funciones
Talento Humano	Políticas de Capacitación
Talento Humano	Políticas de Selección
Talento Humano	Políticas de Vinculación y Desvinculación

4 CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES.

4.1 Conclusiones.

- Tras tener un entendimiento global del negocio en BanCodesarrollo, entrevistar a personal clave, revisar la información proporcionada, validar la existencia y consistencia de la evidencia y finalmente evaluar a profundidad las actividades y prácticas relacionadas con TI se concluye que BanCodesarrollo lleva a cabo en sus prácticas de gobierno y gestión de TI alineadas a COBIT 5 para los dominios Evaluar, Orientar y Supervisar (EDM); Alinear, Planear y Organizar (APO) y Supervisar, Evaluar y Valorar (MEA).
- La aplicación de la herramienta de trabajo denominada “Plantilla Cobit” junto con el marco metodológico empleado para esta evaluación tecnológica han revelado que BanCodesarrollo tiene un nivel de alineamiento de 73.17% a COBIT 5.
- Se pudo determinar que el gobierno y gestión de tecnología de información en esta institución se alinea a marcos de referencia y buenas prácticas, puntualmente COBIT 5, no obstante que la institución aún no haya manifestado formalmente su decisión de adoptarlo.
- La focalización en procesos de incidencia directa a riesgos, reflejó que se consideran adecuadamente los lineamientos para administración y gestión de riesgo en BanCodesarrollo, como lo refleja el puntaje de 3.51/5 para el proceso EDM03 Asegurar la Optimización del Riesgo y 4.24/5 para el proceso APO12 Gestionar el Riesgo. Pese a que la institución no permitió se revelen a detalle los controles, se ha identificado la implementación de estos en varias áreas de BanCodesarrollo que aportan sustancialmente a la gestión de riesgo, sin que eso signifique que no puedan ser reevaluados y validados periódicamente para perfeccionarlos.

- Del análisis de resultados obtenidos para actividades, prácticas, procesos y dominios se establece que BanCodesarrollo podría fortalecer su gobierno y gestión de TI, en todos los procesos, con mayor intensidad en dos de ellos que presentan puntuación baja, estos es: APO04 Gestionar la Innovación con 1.77/5 y APO11 Gestionar la Calidad con 2.62/5, debido a que no se llevan a cabo las actividades y prácticas relacionadas con la profundidad que el marco de referencia sugiere..

4.2 Recomendaciones.

- Partiendo del nivel alineamiento identificado se sugiere la adopción del marco de trabajo COBIT 5® en BanCodesarrollo puesto que así no solo formalizaría sus prácticas sino también fortalecería su gobierno y gestión de TI, lo que en consecuencia le permitiría alcanzar adaptabilidad a buenas prácticas de la industria, el entendimiento y cumplimiento de resoluciones, disposiciones y recomendaciones emanadas por el ente de control. Encaminando firmemente los esfuerzos para que el negocio afiance sus resultados y asegure su permanencia en el mercado, muy de la mano del uso adecuado de las tecnologías de información.
- Con base en los hallazgos se recomienda a BanCodesarrollo analizar su estructura organizacional con la finalidad de que se adapte de mejor manera a las prácticas de COBIT 5 en lo referente a:
 - Levantamiento e implementación de procesos, definición y seguimiento de métricas que facilite el cumplimiento tanto de metas del negocio y metas relacionadas con Tecnología de Información, por ejemplo con la creación de un área de procesos y planificación a nivel institucional que incorporen desde luego aspectos de TI y trabajen en la implementación de un robusto Sistema de Gestión de Calidad.

- Diseño de procesos y roles para llevar a cabo actividades de innovación, gestión de proyectos y análisis de la capacidad que posicionen a BanCodesarrollo como uno de los primeros referentes en el sector financiero.
- Se recomienda emprender en un proyecto integral para implementación de COBIT 5® en la medida que le sea factible, prestando especial atención a actividades importantes como:
 - Análisis, gestión y aprobación de un presupuesto para capacitación al personal en materia de COBIT 5.
 - Determinación de una hoja de ruta para implementación progresiva que sea incorporada a la Planificación Estratégica Institucional.
- Toda vez que se cuente con un experiencia en la aplicación de COBIT 5® sería ideal realizar la medición del nivel madurez y capacidad de los procesos, lo que consecuentemente elevaría los niveles de gestión integral de riesgo en BanCodesarrollo.
- Por último es importante realizar un estudio de la carga de trabajo, estructura y procesos en TI, con la finalidad de determinar si el personal es suficiente para cumplir con los objetivos de la institución y planificación estratégica de tecnología considerando que BanCodesarrollo recientemente está participando como banco en el sistema financiero nacional.

5 Bibliografía

- Bermeo, P. (Marzo de 2012). Auditoría Tecnológica. Quito.
- Bermon, L. (2014). *Universidad Nacional de Colombia - Sede Manizales*. Recuperado el 10 de Julio de 2014, de <http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060030/lecciones/Capitulo%202/tecnicas.html>
- Carrión, R. G. (25 de Abril de 2013). Auditoría de Tecnología Basada en Riesgos. Quito, Pichincha, Ecuador.
- Castelo, R. (26 de Juio de 2013). *slideshare*. Obtenido de <http://es.slideshare.net/RicardoCastelo1987/cobit-24671358>
- Computacionales, A. d. (Diciembre de 2011). *uaeh.edu.mx*. Recuperado el 19 de Febrero de 2015, de http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf
- Córdova, R. (Octubre de 2012). Auditoría de Tecnología Basada en Riesgos. Quito, Ecuador.
- Definicion. (s.f.). *Definicion*. Recuperado el 16 de 08 de 2014, de Definicion: <http://definicion.de/evaluacion/>
- Definicion. (s.f.). *Definicion*. Recuperado el 20 de 08 de 2014, de Definicion: <http://definicion.mx/?s=tecnica>
- gerencie*. (09 de Octubre de 2013). Recuperado el 31 de Marzo de 2015, de *gerencie*: <http://www.gerencie.com/auditoria-financiera.html>
- ISACA. (2012). COBIT5 Procesos Catalizadores. Madrid.
- ISACA. (2012). COBIT5-Framework-Spanish. Madrid, España.
- ISACA. (2014). Recuperado el 20 de Julio de 2014, de <http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt>
- ISO. (02 de 1947). *iso.org*. Recuperado el 15 de 06 de 2014, de *iso.org*: <http://www.iso.org/iso/home>
- Martínez, V. (19 de 03 de 2013). *portafolio.co*. Recuperado el 30 de 07 de 2014, de *portafolio.co*: <http://www.portafolio.co/opinion/blogs/buenas->

practicas-auditoria-y-control-interno-las-organizaciones/el-riesgo-auditoria-in

- Mejia, V. D. (13 de 08 de 2013). *diplomadoin*. Recuperado el 12 de 07 de 2014, de diplomadoin:
http://diplomadoin.weebly.com/uploads/4/1/5/7/4157201/seminario_de_investigacion_1.pdf
- Navarro, J. (Marzo de 2012). COBIT. Quito, Ecuador.
- olacefs. (11 de Octubre de 2011). *olacefs.com*. Recuperado el 1 de marzo de 2015, de olacefs.com:
http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HA_SH0155.dir/ManualAuditoriaGestionTICs.pdf
- puce. (31 de Marzo de 2015). Recuperado el 31 de Marzo de 2015, de puce:
ftp://ftp.puce.edu.ec/Departamentales/DIRH/AUDITORIA%20INTERN/A/OPERATIVIDAD/05_EXAMENES_ESPECIALES.pdf
- Quimbiulco Carrillo, A. E. (2012). Diseño de un Manual de Gestión de Tecnologías de Información para el Consejo de Gobierno de Régimen Especial de Galápagos aplicando COBIT 4.1 en el Dominio Adquirir e Implementar. *Repositorio Digital ESPE*, 11.
- Sociales, A. d. (1 de 06 de 2011). *uaeh.edu.mx*. Recuperado el 10 de 08 de 2014, de uaeh.edu.mx:
http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf
- TOPA&ASOCIADOS, T. . (20 de 01 de 2009). *tya*. Recuperado el 15 de 08 de 2014, de tya: <http://tya.com.co/pdfs/GT15.pdf>

ANEXOS