UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULO DE INGENIERO EN INFORMÁTICA

Definición de un marco de referencia para gobernanza de TI utilizando las mejores prácticas de los estándares ISO 38500, COBIT, ISO/IEC 27002 para Memorial International.

TRABAJO DE TITULACIÓN

AUTOR: Ramos Tapia, Diego Javier

DIRECTOR: Benítez Hurtado Segundo Raymundo, Mgtr.

CENTRO UNIVERSITARIO VILLAFLORA

2016

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE TITULACIÓN

Mgtr.

Segundo Raymundo Benítez Hurtado

DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo titulación: Definición de un marco de referencia para gobernanza de TI utilizando las mejores prácticas de los estándares ISO 38500, COBIT, ISO/IEC 27002 para Memorial International, realizado por Diego Javier Ramos Tapia, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, 22 de septiembre del 2016

f) .....

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

“ Yo Ramos Tapia Diego Javier declaro ser autor del presente trabajo de titulación: Definición de un marco de referencia para gobernanza de TI utilizando las mejores prácticas de los estándares ISO 38500, COBIT, ISO/IEC 27002 para Memorial International , de la Titulación de Sistemas Informáticos y Computación, siendo el Mgtr. Segundo Raymundo Benítez Hurtado director del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado o trabajos de titulación que se realicen con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

f. .....

Autor Ramos Tapia Diego Javier

Cédula 1710903442

DEDICATORIA

Dedicado para mi familia que me apoyo en este largo recorrido. A mi esposa que me dio las fuerzas necesarias, su ánimo, su aliento y me inyectó constancia para culminar esta meta trazada. A mis hijos que me dedicaron su tiempo, su inocencia, su alegría e infinito amor, a ellos mi motor principal y fuente de vitalidad. A mis padres que con sus enseñanzas de humildad, respeto, valores han trazado el camino para alcanzar cualquier meta trazada. A mis suegros por compartir su tiempo, cariño y amor con mis hijos y permitirme avanzar y culminar esta meta.

AGRADECIMIENTO

A mi esposa por ser mi compañera en este largo camino y ser mi apoyo constante. A mi madre por darme la constancia y entereza de culminar lo iniciado. A mi padre por brindarme su sabiduría, fe y esperanza. A mi tutor que me guío para la culminación exitosa de este proyecto.

A todos ustedes de corazón mis más profundos y sinceros agradecimientos.

ÍNDICE DE CONTENIDOS

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE TITULACIÓN ii
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS iii
DEDICATORIA iv
AGRADECIMIENTO v
ÍNDICE DE CONTENIDOS vi
ÍNDICE DE FIGURAS viii
ÍNDICE DE TABLAS x
RESUMEN 1
ABSTRACT 2
INTRODUCCIÓN 3
CAPITULO 1. FUNDAMENTO TEÓRICO 5
1.1. Descripción de fundamentos para la Gobernanza TI 6
1.1.1. Introducción al Gobierno TI. 6
1.1.2. Gobierno Corporativo o Gobernanza Corporativa 7
1.1.3. Definición de Gobierno de las TI 10
1.1.4. Un marco de referencia de gestión de TI 15
1.2. COBIT 5. 17
1.3. ISO /IEC 38500:2015 25
1.4. ISO/IEC 27002:2013 30
CAPITULO 2. INFORMACIÓN DE LA EMPRESA SELECCIONADA 33
2.1. Introducción: 34
2.2. Misión 34
2.3. Visión 34
2.4. Valores 34
2.5. Organigrama empresarial 34
2.6. Tecnologías de la información 35
2.6.1. Organigrama TI 35
2.6.2. Aplicaciones de negocio 36
2.6.3. Diagrama de redes y comunicaciones 37
CAPITULO 3. TRABAJO SOBRE LA EMPRESA SELECCIONADA 38
3.1. Realizar análisis del estado actual 39
3.2. Definición del marco de gobernanza TI 51
3.2.1. PRINCIPIO 1 RESPONSABILIDAD: 70
3.2.1.1. Responsabilidades y Matrices RACI 70
3.2.1.2. EDM05. Asegurar la transparencia hacia las partes interesadas 73
3.2.2. PRINCIPIO 2 ESTRATEGIA: 74
3.2.2.1. EDM02. Asegurar la Entrega de Beneficios 76
3.2.2.2. APO02. Gestionar la Estrategia 76
3.2.2.3. APO03. Gestionar la Arquitectura Empresarial: 77
3.2.2.4. APO04. Gestionar la innovación: 79
3.2.2.5. APO06. Gestionar el presupuesto y los costes: 80
3.2.2.6. APO08. Gestionar las relaciones: 81
3.2.2.7. APO11. Gestionar la Calidad: 82
3.2.2.8. APO12. Gestionar el Riesgo: 83
3.2.2.9. APO13. Gestionar la seguridad: 84
3.2.3. PRINCIPIO 3 ADQUISICIÓN: 87
3.2.3.1. EDM04 Asegurar la optimización de recursos: 88
3.2.3.2. EDM05 Asegurar la transparencia hacia las partes interesadas. 89
3.2.3.3. APO03 Gestionar la arquitectura empresarial. 89
3.2.3.4. APO05 Gestionar el portafolio. 90
3.2.3.5. APO06 Gestionar el presupuesto y los costes. 91
3.2.3.6. APO11 Gestionar la calidad. 92
3.2.3.7. APO12 Gestionar el riesgo. 93
3.2.3.8. BAI02 Gestionar la definición de requisitos. 93
3.2.3.9. BAI03 Gestionar la identificación y construcción de soluciones. 94
3.2.3.10. BAI06 Gestionar los cambios. 97
3.2.3.11. BAI09 Gestionar los activos. 99
3.2.3.12. BAI10 Gestionar la configuración. 101

3.2.4. PRINCIPIO 4 DESEMPEÑO: 102
3.2.4.1. APO02 Gestionar la Estrategia 103
3.2.4.2. APO09 Gestionar los acuerdos de servicio 104
3.2.4.3. MEA01 Supervisar, Evaluar y Valorar el rendimiento y la conformidad. 104
3.2.5. PRINCIPIO 5 CONFORMIDAD: 105
3.2.5.1. APO02 Gestionar la estrategia 106
3.2.5.2. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno: 107
3.2.5.3. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos. 109
3.2.6. PRINCIPIO 6 CONDUCTA HUMANA: 111
3.2.6.1. APO07 Gestionar los Recursos Humanos 112
3.2.6.2. BAI02 Gestionar la Definición de Requisitos 114
3.2.6.3. BAI05 Gestionar la Facilitación del Cambio Organizativo. 114
3.2.6.4. BAI08 Gestionar el conocimiento 115
CAPITULO 4 NIVEL ACTUAL Y NIVEL DESEADO 117
4.1. Principio 1 Responsabilidad 118
4.2. Principio 2 Estrategia 119
4.3. Principio 3 Adquisición 120
4.4. Principio 4 Desempeño 121
4.5. Principio 5 Conformidad 122
4.6. Principio 6 Conducta Humana 123
4.7. Controles ISO/IEC 27002:2013 124
CONCLUSIONES 128
RECOMENDACIONES 129
BIBLIOGRAFÍA 130
ANEXOS 132
ANEXO 1. Autoevaluación de nivel de madurez del Gobierno TI 133
ANEXO 2. Formato para toma de resultados de Autoevaluación del nivel de madurez de Gobierno TI 139
ANEXO 3. Formato de análisis de resultados de la Autoevaluación del nivel de madurez de Gobierno TI individual y global 140
ANEXO 4. Actividades para el marco de Gobierno TI de procesos COBIT 5 141

ÍNDICE DE FIGURAS

Figura 1. Gobierno corporativo y Gobierno de negocio 9
Figura 2. Marco de Gobierno de TI 12
Figura 3. Áreas de enfoque de Gobierno TI 14
Figura 4. Principios de COBIT 5 17
Figura 5. Visión general de la Cascada de Metas de COBIT 5 18
Figura 6. Gobierno y Gestión en COBIT 5 19
Figura 7. Roles, Actividades y Relaciones Clave 20
Figura 8. Marco de Referencia Único Integrado COBIT 5 21
Figura 9. Catalizadores Corporativos COBIT 5 22
Figura 10. Las Áreas Clave de Gobierno y gestión de COBIT 5 23
Figura 11. Modelo de Referencia de Procesos de COBIT 5 25
Figura 12. Modelo de Gobernanza Corporativa de las TI 29
Figura 13 Directrices de la norma ISO/IEC 38500:2015 30
Figura 14. ISO/IEC 27002:2013, dominios, objetivos de control y controles 32
Figura 15. Estructura Orgánica Memorial International of Ecuador 35
Figura 16. Organigrama TIC's de Memorial International of Ecuador S.A. 35
Figura 17. Diagrama de comunicaciones Memorial International of Ecuador 37
Figura 18. Evaluación de nivel de madurez de Gobierno TI basado en ISO/IEC 38500 e ISO9004 39
Figura 19. Formato de toma de resultados de nivel de madurez de gobierno TI 39
Figura 20. Formato de análisis individual de resultados del nivel de madurez de gobierno TI 40
Figura 21. Formato de análisis global de resultados del nivel de madurez de gobierno TI 41
Figura 22. Resultados de nivel de madurez de gobierno TI. Principio 1 42
Figura 23. Resultados de nivel de madurez de gobierno TI. Principio 2 43
Figura 24. Resultados de nivel de madurez de gobierno TI. Principio 3 44
Figura 25. Resultados de nivel de madurez de gobierno TI. Principio 4 46
Figura 26. Resultados de nivel de madurez de gobierno TI. Principio 5 47
Figura 27. Resultados de nivel de madurez de gobierno TI. Principio 6 49
Figura 28. Resultados de nivel de madurez global de gobierno TI 50
Figura 29. GEIT para Organización Memorial 69
Figura 30. Roles y estructuras organizativas para Memorial International of Ecuador 71
Figura 31. Partes interesadas internas en el GEIT 72
Figura 32. Partes interesadas en el GEIT externas 73
Figura 33. Matriz RACI EDM05 74
Figura 34 Matriz RACI del proceso EDM02 de COBIT 5 76
Figura 35 Matriz RACI del proceso APO02 de COBIT 5 77
Figura 36 Matriz RACI del proceso APO03 de COBIT 5 78
Figura 37 Proceso APO03 de COBIT 5 y controles ISO 27002 79
Figura 38 Matriz RACI del proceso APO04 de COBIT 5 80
Figura 39 Matriz RACI del proceso APO06 de COBIT 5 81
Figura 40 Matriz RACI del proceso APO08 de COBIT 5 82
Figura 41 Matriz RACI del proceso APO11 de COBIT 5 83
Figura 42 Matriz RACI del proceso APO12 de COBIT 5 84
Figura 43 Proceso APO12 de COBIT 5 y controles ISO 27002 84
Figura 44 Matriz RACI del proceso APO13 de COBIT 5 85
Figura 45 Proceso APO13 de COBIT 5 y controles ISO 27002 86
Figura 46 Matriz RACI del proceso EDM04 de COBIT 5 88
Figura 47 Matriz RACI del proceso EDM05 de COBIT 5 89
Figura 48 Matriz RACI del proceso APO03 de COBIT 5 90
Figura 49 Matriz RACI del proceso APO05 de COBIT 5 91
Figura 50 Matriz RACI del proceso APO06 de COBIT 5 92
Figura 51 Matriz RACI del proceso APO11 de COBIT 5 92
Figura 52 Matriz RACI del proceso APO12 de COBIT 5 93
Figura 53 Matriz RACI del proceso BAI02 de COBIT 5 94
Figura 54 Matriz RACI del proceso BAI03 de COBIT 5 95
Figura 55 Proceso BAI03 de COBIT 5 y controles ISO 27002 95
Figura 56 Matriz RACI del proceso BAI06 de COBIT 5 98

Figura 57 Proceso BAI06 de COBIT 5 y controles ISO 27002 98
Figura 58 Matriz RACI del proceso BAI09 de COBIT 5 99
Figura 59 Proceso BAI09 de COBIT 5 y controles ISO 27002 100
Figura 60 Matriz RACI del proceso BAI10 de COBIT 5 101
Figura 61 Matriz RACI del proceso APO02 de COBIT 5 103
Figura 62 Matriz RACI del proceso APO09 de COBIT 5 104
Figura 63 Matriz RACI del proceso MEA01 de COBIT 5 105
Figura 64 Matriz RACI del proceso APO02 de COBIT 5 107
Figura 65 Matriz RACI del proceso MEA02 de COBIT 5 108
Figura 66 Proceso MEA02 de COBIT 5 y controles ISO 27002 108
Figura 67 Matriz RACI del proceso MEA02 de COBIT 5 110
Figura 68 Proceso MEA03 de COBIT 5 y controles ISO 27002 110
Figura 69 Matriz RACI del proceso APO07 de COBIT 5 112
Figura 70 Proceso APO07 de COBIT 5 y controles ISO 27002 113
Figura 71 Matriz RACI del proceso BAI02 de COBIT 5 114
Figura 72 Matriz RACI del proceso BAI02 de COBIT 5 115
Figura 73 Matriz RACI del proceso BAI08 de COBIT 5 116
Figura 74 Proceso BAI08 de COBIT 5 y controles ISO 27002 116
Figura 75 Nivel de madurez actual, deseado y brecha de Gobierno TI..... 118

ÍNDICE DE TABLAS

Tabla 1. Comparativa de modelos para Gobierno de las TI. 16
Tabla 2. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 1 de la norma ISO/IEC 38500. 41
Tabla 3. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 2 de la norma ISO/IEC 38500. 43
Tabla 4. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 3 de la norma ISO/IEC 38500. 44
Tabla 5. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 4 de la norma ISO/IEC 38500. 45
Tabla 6. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 5 de la norma ISO/IEC 38500. 47
Tabla 7. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 6 de la norma ISO/IEC 38500. 48
Tabla 8. Controles de las mejores prácticas de seguridad de la ISO 27002. 124

RESUMEN

Un marco de gobierno de las Tecnologías de Información ayuda en la dirección y control de las TI actuales y su previsión futura, permite además que las organizaciones mejoren su efectividad y eficiencia apoyando al cumplimiento de los objetivos organizacionales, esto permite tener una ventaja competitiva con empresas que brindan los mismos servicios.

Un buen manejo de las TI no solo permite tener ahorros en inversión de tecnología sino que abre camino a innovaciones, nuevas alianzas, incrementar el portafolio de productos y servicios, establecer normas, políticas, procesos y procedimientos de TI que las lleven a ser el principal socio estratégico de las organizaciones.

Este aporte permitirá a Memorial International of Ecuador disponer de un marco de gobierno basado en la norma internacional ISO/IEC 38500 y COBIT 5, además de tener controles de seguridad de las mejores prácticas de la ISO 27002.

PALABRAS CLAVE: marco de gobierno, gobierno TI, GEIT, TIC, COBIT 5, ISO/IEC 38500, ISO/IEC 27002

ABSTRACT

A framework of government of the technologies of information helps in the direction and control of it today and its future forecast, also allows organizations to improve their effectiveness and efficiency to support the implementation of the organizational objectives, this allows you to have a competitive advantage with companies that offer the same services.

A good management of IT not only allows you to have savings into investment of technology but that opens the way to innovations, new alliances, increase the portfolio of products and services, establishing standards, policies, processes and IT procedures which lead them to be the main strategic partner organizations.

This contribution will allow to Memorial International of Ecuador have a framework for government based on the international standard ISO/IEC 38500 and COBIT 5, in addition to having security checks on the best practices of the ISO 27002.

Key words: governance framework, IT governance, GEIT, ICT, COBIT 5, ISO/IEC 38500, ISO/IEC 27002

INTRODUCCIÓN

La gobernanza de las Tecnologías de la Información (TI) es un tema que ha estado difundiéndose durante los últimos años y ha hecho que empresas mejoren su efectividad y eficiencia apoyándose conjuntamente con las TI para el cumplimiento de los objetivos empresariales y lograr los resultados esperados.

La información es el activo más importante en una organización, por lo que debemos tomar las precauciones para protegerla. Es por eso que se va a desarrollar este proyecto utilizando el estándar ISO/IEC 38500:2015 como principal referente o marco para la gobernanza de TI, se profundizará con COBIT 5 en cuanto a los procesos para la gobernanza de las TI y con el estándar ISO/IEC 27002:2013 se desarrollará directrices para la gestión de la seguridad de la información para Memorial International of Ecuador utilizando las mejores prácticas de los estándares antes mencionados.

CAPITULO 1 FUNDAMENTO TEÓRICO: en este capítulo se analizan todas las definiciones, conceptos, estándares y marcos que se necesitan para el desarrollo del trabajo.

CAPITULO 2 INFORMACIÓN DE LA EMPRESA SELECCIONADA: en este capítulo se realiza una investigación preliminar de la empresa, su misión, visión, organigrama empresarial, organigrama de TI y las funciones de las persona que componen el departamento de TI.

CAPITULO 3 TRABAJO SOBRE LA EMPRESA SELECCIONADA: en este capítulo se realiza el trabajo en sí, se hace un análisis del estado actual de la empresa, se desarrolla el marco de gobierno en base a la norma ISO/IEC38500, COBIT 5 y la norma ISO/IEC27002.

CAPITULO 4 NIVEL ACTUAL Y NIVEL DESEADO: este capítulo describe el estado actual de madurez de la empresa a través de encuestas formuladas a personas que componen el departamento de TI además de incluir el estado deseado de madurez de Gobierno de las TI al que desea llegar la organización.

CAPITULO 5 CONCLUSIONES: este capítulo describe las conclusiones halladas al realizar el trabajo en la organización.

CAPITULO 6 RECOMENDACIONES: el último capítulo describe las recomendaciones para alcanzar el nivel deseado de madurez por la organización.

OBJETIVO GENERAL

Definir un marco de referencia para gobernanza de TI utilizando las mejores prácticas de los marcos y estándares ISO 38500, COBIT, ISO/IEC 27002 para Memorial International of Ecuador.

OBJETIVOS ESPECÍFICOS

- Realizar el análisis de la situación actual de la empresa.
- Analizar los marcos y estándares en torno a la gobernanza de TI para la empresa
- Definir los controles de seguridad para las TI de la empresa.
- Definir el marco de gobierno TI.
- Establecer las actividades necesarias para implementación del marco de gobierno.

JUSTIFICACIÓN

Memorial International trabaja sin ningún tipo de marco o estándar, los procedimientos para el desarrollo de diferentes actividades son reducidos, no existe el entrenamiento a los usuarios sobre el uso de los recursos de TI, existe controles reducidos en cuanto a seguridad, control de activos de TI, etc. por lo que se ve la necesidad de desarrollar un gobierno TI de la empresa (GEIT, Governance of Enterprise IT) que según la ISACA (2012) un GEIT efectivo requiere de una serie de catalizadores con los roles, responsabilidades y obligación de rendir cuentas cuidadosamente establecidos, en línea con el estilo y las normas operativas específicas así como la responsabilidad y supervisión de que se ejecuten las normas de estilo y operativas específicas para cada empresa.

ALCANCE

Memorial International of Ecuador cuenta con políticas y controles reducidos que ayuden a la gestión de las TI y en consecuencia que apoyen al cumplimiento de los objetivos empresariales por lo que se definirá por completo el marco de gobierno basándo en la norma internacional ISO/IEC 38500:2015 con sus seis principios, estos principios se los trabajará con procesos relacionados de COBIT 5 y en lo que se refiere a seguridades de la información se lo desarrollará con las mejores prácticas de los controles de la norma ISO/IEC 27002:2012 mapeados a las prácticas de COBIT 5.

CAPITULO 1. FUNDAMENTO TEÓRICO

1.1. Descripción de fundamentos para la Gobernanza TI.

1.1.1. Introducción al Gobierno TI.

Ross y Weill, (2002), manifiestan que han observado la frustración que muchos directivos de empresas sienten hacia las tecnologías de la información y comunicación (TIC) y hacia sus departamentos de TI. Muchos altos directivos dicen que no consiguen extraer mucho valor empresarial del alto costo de las tecnologías instaladas en sus empresas. Adicional la lista de capacidades aparentemente necesarias de TI van incrementando siendo un valor considerable en el presupuesto de la empresa.

El IT Governance Institute (ITGI, 2003), menciona que en el corazón de las responsabilidades de gobierno, de la definición de la estrategia, de la gestión de riesgos, de la entrega de valor y de la medición del desempeño, son los grupos de interés, quienes impulsan la estrategia empresarial y de TI. Mantener el negocio y el crecimiento en nuevos modelos de negocio son sin duda las expectativas de los interesados y sólo se pueden lograr con la gobernanza adecuada de la infraestructura de TI de la empresa.

La investigación de las prácticas de gestión de TI realizada por Ross y Weill (2002) indican que: "Las empresas que gestionan sus inversiones con mayor éxito consiguen unos rendimientos que llegan a ser superiores hasta en un 40% a los de sus competidores" (p. 1).

Ross y Weill (2004) nos mencionan que las empresas con alto rendimiento buscan de manera proactiva el valor de TI de diferentes maneras:

- Aclaran las estrategias de negocio y el papel de las TIC en el logro de ellos.
- Miden y gestionan la cantidad gastada y el valor recibido de TI
- Asignan responsabilidades para los cambios organizativos requeridos en beneficio de las nuevas capacidades de TI.
- Aprenden de cada aplicación, cada vez más adeptos a compartir y reutilizar los activos de TI.

El estrepitoso desarrollo de la tecnología hace que procesos se automaticen, facilitan el procesamiento de información, se han roto barreras geográficas, y un sin número de aplicaciones que se pueden mencionar donde la tecnología está inmersa.,es por eso que las empresas deben estar de la mano con los avances tecnológicos para ser competitivas y tener herramientas que ayuden a que estas sean más eficientes y competitivas.

Pero el estar a la vanguardia tecnológica no implica que se tenga un éxito seguro, por el contrario el mayor problema que se tiene es que los objetivos de TI no están alineados con los objetivos estratégicos de la organización conduciéndonos a un fracaso rotundo.

El IT Governance Institute (ITGI, 2003) indica:

> El uso de TI tiene el potencial para ser el mayor impulsor de riqueza económica en el siglo 21. Además de que TI ya es crítica para el éxito empresarial, proporciona oportunidades para obtener una ventaja competitiva y ofrece medios para incrementar la productividad, e incluso hará aún más en el futuro.
>
> TI también implica riesgos. Es evidente que en estos días de negocios globales, la caída de los sistemas y las redes puede resultar muy costosa para cualquier empresa. En algunas industrias, TI es un recurso competitivo necesario para diferenciarse y obtener una ventaja competitiva, mientras que en otras, no sólo determina la prosperidad sino la supervivencia. (p. 14)

Fueron varios los esfuerzos que se realizaron para definir lo que es gobierno TI y según Muñoz y Ulloa (2011):

> Producir el concepto de gobierno de TI y todo lo relacionado con él para lograr la alineación e integración con el gobierno corporativo ha sido un gran esfuerzo de la academia, firmas consultoras, asociaciones de investigación, organizaciones de estándares y entidades reguladoras.
>
> Entre otros esfuerzos se puede mencionar los que realizan entidades especializadas como: **ISACA** (Information Systems Audit and Control Association), **ITGI** (IT Governance Institute) **ITSMF** (IT Service Management Forum) IT GOVUK (IT Governance UK) y **ECGI** (European Corporate Governance Institute) y organizaciones desarrolladoras de estándares como: **ISO/IEC** (International Organization for Standardization / International Electrotechnical Commission) y **BSI** (The British Standards Institution). (p.p. 3,4)

1.1.2. Gobierno Corporativo o Gobernanza Corporativa

Para una mejor comprensión de lo que es Gobierno Corporativo o Gobernanza Corporativa se listará varios conceptos:

Según el Instituto de Gobernanza Empresarial y Pública (IGEP, 2015):

La **gobernanza** estudia todos los mecanismos, procesos y reglas a través de los cuales se ejerce la autoridad económica, política y administrativa de una organización, tanto empresarial como estatal o del tercer sector (ONGs). Busca comprender cómo queda determinada la conducta de las instituciones por todo el variado conjunto de agentes y reglas que influyen sobre ella.

Según la Organización para la Cooperación y el Desarrollo Económico, OCDE (2015):

El **gobierno corporativo** es el sistema por el cual las sociedades son dirigidas y controladas. La estructura del gobierno corporativo especifica la distribución de los derechos y responsabilidades entre los diferentes participantes de la sociedad, tales como el directorio, los gerentes, los accionistas y otros agentes económicos que mantengan algún interés en la empresa. El gobierno corporativo también provee la estructura a través de la cual se establecen los objetivos de la empresa, los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento a su desempeño.

Según The Committee on the Financial Aspects of Corporate Governance. (Cadbury Report, 1992):

El **gobierno corporativo** es el sistema por el cual las empresas son dirigidas y controladas. El consejo de la administración es el responsable de la gestión de sus empresas. El papel de los accionistas en el gobierno es nombrar a los directores y los auditores para cerciorarse de que una estructura de gobernanza adecuada está en su lugar. Las responsabilidades de la junta incluyen el establecimiento de la compañía y objetivos estratégicos que proporcionan el liderazgo para ponerlas en marcha, la supervisión de la gestión de la empresa e informar a los accionistas sobre su gestión. El comportamiento de la junta está en sujeción a las leyes, los reglamentos y la Junta General de Accionistas.

Para The Bank for International Settlements (BIS, 1999):

La **gobernabilidad** son arreglos que abarca el conjunto de las relaciones entre la gestión de la entidad y de su órgano rector, sus dueños y sus grupos de interés y proporcionan la estructura mediante la cual:

- Se establecen los objetivos generales de la entidad
- Se describen el método para alcanzar estos objetivos
- Se describe la forma en que el rendimiento se supervisará.

Luego de tener claro los conceptos mencionados, se revisará la propuesta de Ross y Weill (2004) para la vinculación de la gestión empresarial y la gestión de TI.

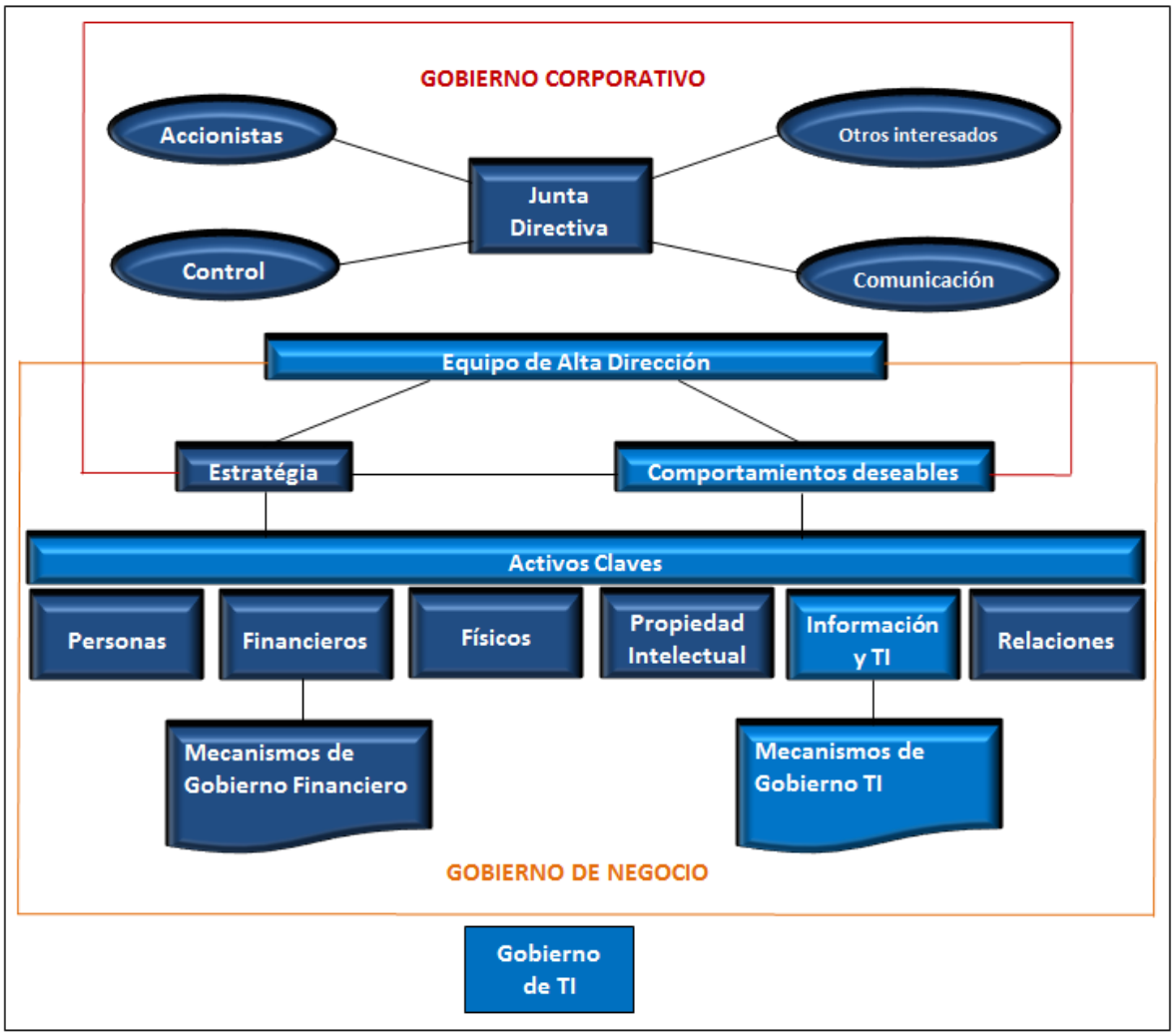


Figura 1. Gobierno corporativo y Gobierno de negocio
Fuente: adaptado de Weill, P. & J. Ross, (2004).

Como indican Ross y Weill (2004), en la parte superior del marco indicado en la Figura 1, se muestra las relaciones del Consejo. El equipo de Alta Dirección, que actúa como agente del Consejo o Junta Directiva, articula Estrategias y Comportamientos deseables para poder cumplir con los mandatos que propone el Consejo. A continuación en la mitad inferior de la figura podemos identificar los seis activos a través de los cuales las empresas desarrollarán sus estrategias y podrá generar valor para el negocio.

El Equipo de Alta Dirección crea los mecanismos para la gestión de gobierno, además del uso de cada activo tanto independientes como juntos (Ross y Weill, 2004).
Los elementos clave de cada activo según Ross y Weill (2004) incluyen:

- **Activos humanos**: personas, habilidades, trayectorias profesionales, capacitación, nivel de comunicación, tutorías, competencias, etc.
- **Activos financieros**: efectivo, inversiones, pasivos, flujos de efectivo, cuentas por cobrar, etc.
- **Activos físicos**: edificios, fábricas, equipamiento, soportes, seguridades, etc.
- **Activos de propiedad intelectual**: incluidos los productos, servicios y procesos formalmente patentados, derechos de autor, o sistemas empresariales o personales embebidos.
- **Información y activos de TI**: datos digitalizados, la información y el conocimiento acerca de los clientes, rendimiento de los procesos, finanzas, sistemas de información, etc.
- **Activos de relación**: relaciones con la empresa así como las relaciones en la empresa, marca y la reputación con los clientes, proveedores, unidades de negocio, regulaciones, competidores, socios, etc. (p. 4)

1.1.3. Definición de Gobierno de las TI

Según lo indica la Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) ISO/IEC 38500 (2015): El término gobernanza de la TI es equivalente a los términos de gobierno corporativo de TI, gobierno empresarial de TI (GEIT, Governance of Enterprise IT) y gobierno de la organización de TI. Para nuestro caso utilizaremos al término GEIT para referirnos a Gobierno de TI. A continuación se revisarán varias definiciones de Gobierno de TI:

La definición de la Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) ISO/IEC 38500 (2015) sobre gobernanza corporativa de la TI es:
El sistema por el cual está dirigido y controlado el uso actual y futuro de las TI. Esta norma internacional establece principios para el uso eficaz, eficiente y aceptable de TI. Los órganos de gobierno garantizan que sus organizaciones siguen estos principios, serán asistidos en la gestión de riesgos y el fomento de la explotación de las oportunidades derivadas del uso de las TI. (p. 14)

La definición sobre Gobierno corporativo en Itera (2003) es:

> El Gobierno TI es un conjunto de procedimientos, estructuras y comportamientos utilizados para dirigir y controlar la organización hacía el logro de sus objetivos.

El IT Governance Institute (ITGI, 2003), manifiesta:

> El gobierno de TI consiste en el liderazgo, estructuras de organización y procesos que aseguran que las TI sostienen y amplían las estrategias y objetivos de la empresa. El gobierno de TI es la responsabilidad del consejo de administración y la dirección ejecutiva. Es una parte integral de la gobernanza empresarial y consta de las estructuras de dirección, de organización y procesos que aseguren que TI sostiene y extiende las estrategias y objetivos de la organización.

ISACA (2012b) define gobierno como:

> El gobierno asegura que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar los objetivos de empresa acordados y equilibrados que han de ser alcanzados; establecer la dirección mediante la priorización y toma de decisiones; y supervisando el rendimiento y el cumplimiento respecto a la dirección y objetivos acordados. (p.13)

El propósito del gobierno de TI es dirigir esfuerzos, asegurando que el rendimiento de TI cumpla con los siguientes objetivos según el ITGI (2003):

- Alineación de TI con la empresa y la realización de la promesa de beneficios.
- Uso de TI para permitir a la empresa aprovechar las oportunidades y maximizar beneficios.
- Uso responsable de los recursos de TI.
- Manejo apropiado de riesgos relacionados con TI.

A continuación en la Figura 2 se tiene el proceso de gobernanza descrito por el ITGI (2003), mismo que comienza con el establecimiento de los objetivos de TI para la empresa, proporcionando la dirección inicial de la misma. A partir de entonces, se establece un bucle continuo para medir el desempeño, en comparación con los objetivos, y dando lugar a la reorientación de las actividades en caso de ser necesario y un cambio de objetivos apropiados. Si bien los objetivos son fundamentalmente responsabilidad de la junta y las medidas de desempeño son de la gestión, es evidente que deben ser desarrollados en conjunto para que los objetivos sean alcanzables y las medidas representen a los objetivos correctamente.

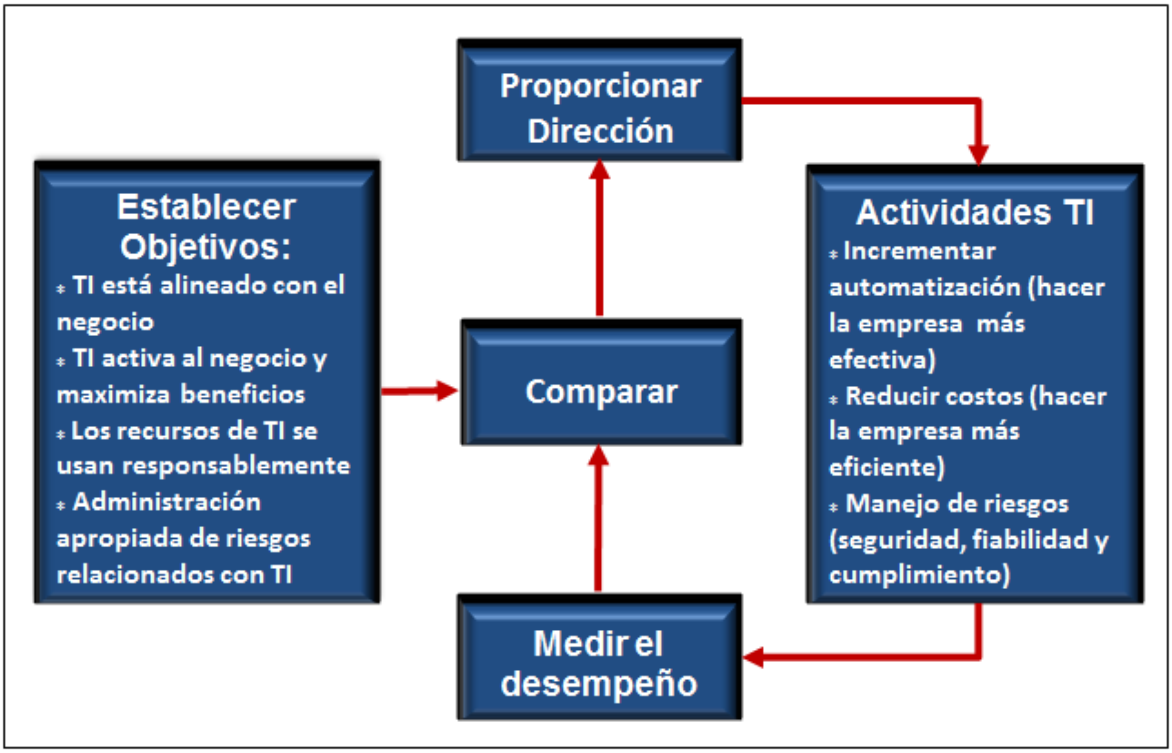


Figura 2. Marco de Gobierno de TI
Fuente: adaptado de IT Governance Institute (ITGI, 2003).

La importancia del Gobierno TI radica en que en la actualidad el uso de las TI es el principal motor de riqueza económica, su uso proporciona ventajas y oportunidades frente a otras empresas de similares características dando valor agregado a los productos y servicios ofrecidos; además incrementa la productividad automatizando procesos, teniendo sistemas más fiables, mejora en la gestión de recursos de la empresa tanto para clientes como para proveedores, haciendo transacciones cada vez más globales y desmaterializadas. Las TI son importantes pues en ellas se almacena y difunde el conocimiento del negocio. Muchas empresas han hecho la transición de lo tangible (inventario, instalaciones, etc.) a lo intangible (información, el conocimiento, la experiencia, la reputación, la confianza, patentes, etc.), muchos de estos activos giran en torno al uso de las TI. (ITGI, 2003)

COBIT 5 (2012b), nos indica que el gobierno empresarial de TI (GEIT) está preocupado principalmente en tres aspectos:

- **Realización de beneficios.-** creación de nuevo valor para la empresa a través de TI, manteniendo e incrementando el valor derivado de inversiones existentes de TI y eliminando las iniciativas y los activos TI que no están generando un valor suficiente para la empresa. Los principios básicos del valor de TI son entregas de soluciones y servicios ajustados a los objetivos, en tiempo y dentro del presupuesto,

y la generación de los beneficios financieros y no financieros que fueron establecidos. El valor que TI entrega debería estar alineado directamente con los valores sobre los cuales el negocio se centra y medido de un modo que muestre transparentemente los impactos y contribución de las inversiones de TI en el proceso de creación de valor de la empresa.

- **Optimización del riesgo.**- considerando el riesgo de negocio asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de TI en una empresa. El riesgo de negocio relacionado con TI consiste en eventos relacionados con TI que podrían impactar potencialmente en el negocio. Mientras que la entrega de valor se enfoca en la creación del valor, la gestión del riesgo se centra en la conservación del valor. La gestión del riesgo relacionado con TI debería estar integrado en el enfoque de la gestión del riesgo de la empresa, para asegurar un foco en TI por parte de la empresa y ser medido de modo que transparentemente se muestren los impactos y la contribución de la optimización del riesgo del negocio relacionado con TI para preservar el valor.
- **Optimización de recursos.-** asegurando que las capacidades adecuadas están en funcionamiento para ejecutar el plan estratégico y que los recursos que se proporcionan son suficientes, adecuados y eficaces. La optimización de recursos garantiza que la infraestructura de TI proporcionada es económica e integrada, que se incorpora nueva tecnología cuando es necesario para el negocio y que los sistemas obsoletos son actualizados o reemplazados. Se reconoce la importancia de las personas, además del hardware y el software, y, por lo tanto, se centra en proporcionar formación, en la retención de promoción y en asegurar la competencia de personal TI clave. (p.15)

Estos aspectos guiarán a las cinco áreas de enfoque principales para el gobierno de TI, todos impulsados por el valor para los accionistas. Dos de ellos son los resultados: la Entrega de Valor y la Gestión del Riesgo, las otras tres son conductores: Alineamiento Estratégico, Gestión de Recursos y Medición del Desempeño (figura 3).

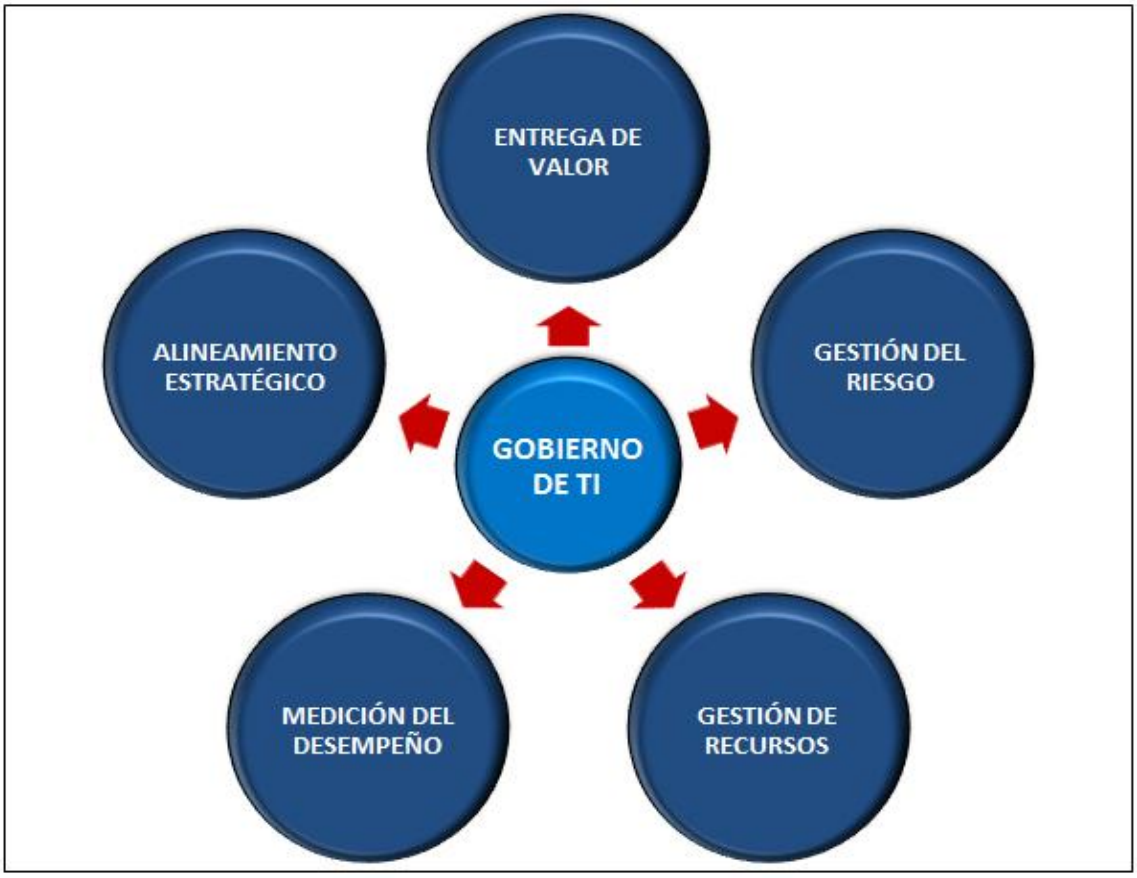


Figura 3. Áreas de enfoque de Gobierno TI
Fuente: adaptado de IT Governance Institute (ITGI, 2003).

Cada una de las áreas del enfoque de Gobierno de TI según el ITGI (2007, 2008) y el Grupo Ctemagob. (2015) son:

- El **alineamiento estratégico**, centrado en el alineamiento de TI con el negocio y con soluciones colaborativas; definir, mantener y validar la propuesta de valor de TI, alinear las operaciones de TI con las operaciones del negocio.
- La **entrega de valor**, concentrado en la optimización de costos y en la demostración del valor de TI para accionistas, clientes, proveedores y empleados. En el caso de las organizaciones públicas se deberá generar valor para los ciudadanos.
- **La gestión de riesgos**, considerando el resguardo de los activos de TI (incluyendo la inversión en proyectos), recuperación de desastres y la continuidad de las operaciones. Todo esto es posible con una buena implementación de controles efectivos de TI, además se requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa.
- La **gestión de recursos**, realizar la inversión óptima además de la administración adecuada de recursos críticos de TI, información, aplicaciones,

infraestructura y personal. Los aspectos claves son la optimización de conocimiento e infraestructura.

- **La medición del desempeño**, el seguimiento de la entrega de proyectos, uso de recursos, desempeño de procesos y la supervisión de servicios de TI. Los elementos anteriormente mencionados deben ser monitoreados y medibles en base a métricas que establece la organización.

1.1.4. Un marco de referencia de gestión de TI

Las empresas se deben ajustar a la utilización de estándares y prácticas de acuerdo a sus requerimientos individuales. Es así que hoy en día la creciente adopción de mejores prácticas de TI requieren mejorar la administración de la calidad y la confiabilidad de TI en los negocios y responder a un creciente número de requerimientos regulatorios y contractuales. Es así que las organizaciones que desean implantar las mejores prácticas de TI necesitan un marco de referencia de gestión eficaz el mismo que proporcione un enfoque general consistente y que posibilite asegurar resultados exitosos al utilizar TI para apoyar la estrategia de la empresa.

Un marco de control debe tener las siguientes características, recomendadas por ISACA para cualquier marco de referencia de control (ITGI, 2007):

- **Brindar un fuerte enfoque en el negocio.** La medición del desempeño de TI debe enfocarse sobre su contribución para hacer posible y expandir la estrategia de negocios.
- **Definir un lenguaje común.** Construye seguridad y confianza entre los participantes, para tener a todos sintonizados en el mismo canal, al definir términos críticos y brindar un glosario que aclare alguna duda existente.
- **Ayudar a alcanzar requerimientos regulatorios.** Permite dar respuesta a los controles internos necesarios para evitar un mal manejo de la información generada para el gobierno corporativo.
- **Contar con la aceptación general entre la organización.** Permite ser probado y globalmente aceptado para incrementar la contribución de TI al éxito de la organización.
- **Asegurar la orientación a procesos.** Aprovechando la propiedad de los procesos estos están definidos, asignados y aceptados y la organización está en mejor capacidad para mantener el control durante los períodos de cambios rápidos o crisis organizacionales.

En la siguiente tabla se puede encontrar una comparativa de varios modelos, marcos, estándares varios de los cuales se seleccionaron para realizar este trabajo.

Tabla 1. Comparativa de modelos para Gobierno de las TI.

MARCO	ALCANCE Y OBJETIVOS	ESTRUCTURA	VENTAJAS	DESVENTAJAS
COBIT 5	**Alcance:** Gobernanza de las TI. **Objetivo:** provee de un marco integral de gobierno y gestión de las TI, que ayuda a las empresas a crear un valor óptimo desde TI, manteniendo un equilibrio entre la generación de beneficios, optimización de los niveles de riesgo y el uso de recursos.	COBIT 5 se basa en 5 dominios, cada uno con procesos y actividades. Evaluar, Orientar y Supervisar. Alinear, Planificar y Organizar. Construir, Adquirir e Implementar. Entregar, Dar Servicio y Soporte. Supervisar, Evaluar y Valorar.	Se aprecian resultados en indicadores de la eficiencia y efectividad. Permite el desarrollo de políticas claras y buenas prácticas para el control de las TI. Resalta el cumplimiento de las normas, ayuda a las organizaciones a aumentar el valor obtenido de TI.	No es una norma certificable. Resulta un modelo ambicioso que requiere de profundidad en el estudio.
ISO IEC 38500	**Alcance:** Gobernanza de las TI. **Objetivo:** Esta Norma está diseñada para que las organizaciones que utilizan como referencia la selección de los controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 o como un documento de orientación para las organizaciones que efectúan controles de seguridad de la información generalmente aceptadas.	**Evaluar** el uso actual y futuro de las TI. **Dirigir** la preparación y ejecución de planes y políticas para asegurar que el uso de la TI satisface los objetivos de la organización. **Monitorizar** el cumplimiento de las políticas y el desempeño con relación a lo planificado.	Asegurar que las partes interesadas, siguen los principios y las prácticas propuestas por la norma, pueden tener la confianza en el gobierno de la organización de TI. Informar y orientar a los órganos de gobierno en el que rige el uso de las TI en su organización. El establecimiento de un vocabulario para la gobernanza de TI.	No posee un nivel de detalle de los procesos a implementarse. La norma no es certificable
ISO IEC 27002	**Alcance:** seguridad de las TI. **Objetivo:** provee de un marco integral de gobierno y gestión de las TI, que ayuda a las empresas a crear un valor óptimo desde TI, manteniendo un equilibrio entre la generación de beneficios, optimización de los niveles de riesgo y el uso de recursos.	La norma se compone de 14 dominios, 35 objetivos de control y 114 controles	Seleccionar controles a través de implementación de procesos en un sistema de gestión de la seguridad de la información basados en ISO/IEC 27001. Implementar controles de seguridad comúnmente aceptados. Desarrollar sus propias directrices de gestión de la seguridad de la información.	Convencer a la dirección la implementación e importancia de la norma. Elección, aprobación e identificaciín clara de los procesos sensibles del negocio.

Fuente: adaptado de ISACA (2012a), ISO/IEC (2015), ISO/IEC 2013

1.2. COBIT 5.

Como manifiesta la Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información ISACA, 2012a):

> COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de otra manera, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (p.13)

Figura 4. Principios de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012a).

Como se revisó en la Figura 4, COBIT 5 se basa en cinco principios claves para el Gobierno y la Gestión de las TI, tal como lo indica ISACA (2012a):

- **Principio 1. Satisfacer las Necesidades de las Partes Interesadas**: las empresas existen para crear valor para sus accionistas. Crear valor significa el equilibrio entre la realización de beneficios a un costo óptimo de los recursos y la optimización de los riesgos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. (p.14)

La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas, soportando así la alineación entre las necesidades de la empresa y las soluciones y servicios de TI. (p.17)

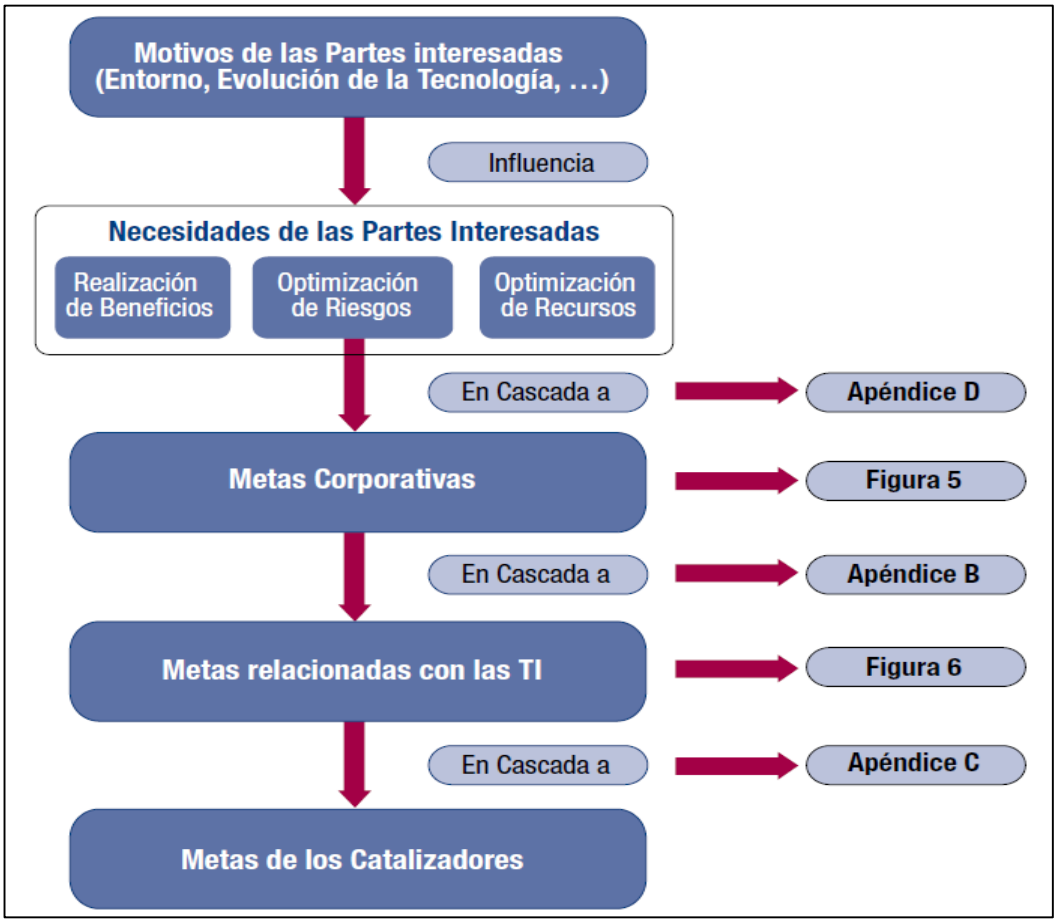


Figura 5. Visión general de la Cascada de Metas de COBIT 5
Fuente: Information Systems Audit and Control Association (ISACA, 2012a).

- **Principio 2: Cubrir la Empresa Extremo-a-Extremo:** COBIT 5 contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo-a-extremo y para toda la empresa. Esto significa que COBIT 5:

- Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto por COBIT 5 se integra sin problemas en cualquier sistema de gobierno. COBIT 5 se alinea con las últimas visiones sobre gobierno.
- Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos. (p. 23)

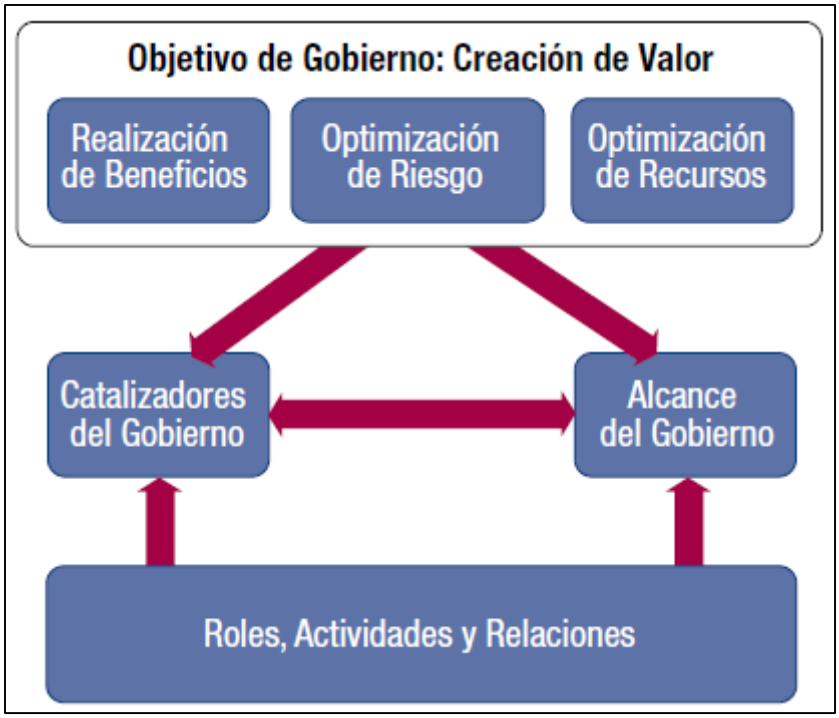


Figura 6. Gobierno y Gestión en COBIT 5
Fuente: Information Systems Audit and Control Association (ISACA, 2015a).

Los ***Catalizadores de Gobierno*** son los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que o hacia los que las acciones son dirigidas y los objetivos pueden ser alcanzados.

El **Alcance de Gobierno** puede ser aplicado a toda la empresa, a una entidad, a un activo tangible o intangible, etc.

Roles, Actividades y Relaciones, definen quién está involucrado en el gobierno, como se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno. (p. 24)

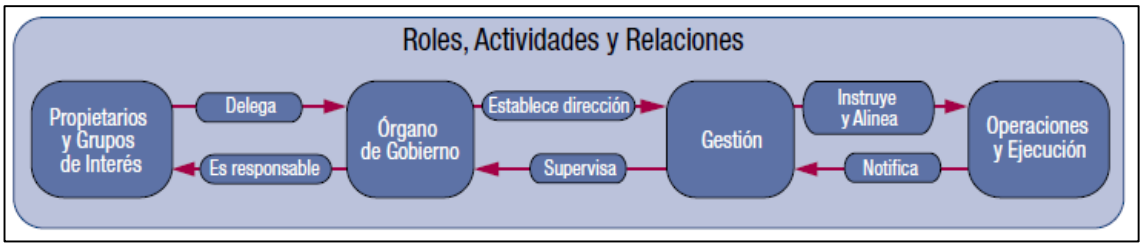


Figura 7. Roles, Actividades y Relaciones Clave
Fuente: Information Systems Audit and Control Association (ISACA, 2012a).

- **Principio 3: Aplicar un Marco de Referencia único integrado:** COBIT 5 es un marco de referencia único e integrado por:
  - Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno.
  - Es completo en cuanto a la cobertura de la empresa, proporciona una base que integra de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico.
  - Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.
  - Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA, como son: COBIT, Val IT, Risk IT, BMIS, la publicación *Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance)* e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento. (p. 25)

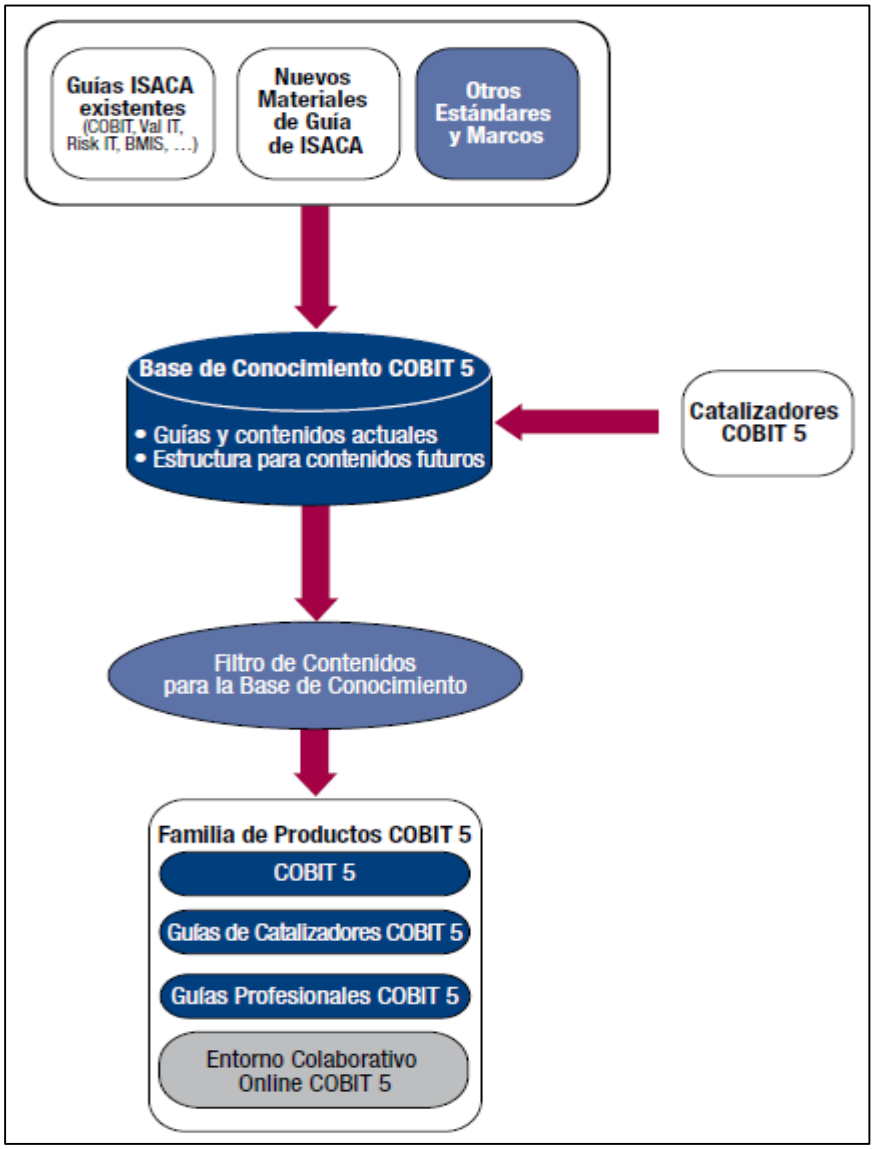


Figura 8. Marco de Referencia Único Integrado COBIT 5
Fuente: Information Systems Audit and Control Association (ISACA, 2012a).

- **Principio 4: Hacer Posible un Enfoque Holístico:** un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. (p. 14)

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel

relacionados con TI definen lo que los diferentes catalizadores deberían conseguir. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

- **Principios, políticas y marcos de referencia** son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los **procesos** describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- Las **estructuras organizativas** son las entidades de toma de decisiones clave en una organización.
- La **Cultura, ética y comportamiento** de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La **información** impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
- Los **servicios, infraestructuras y aplicaciones** incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las **personas, habilidades y competencias** están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas. (p. 27)

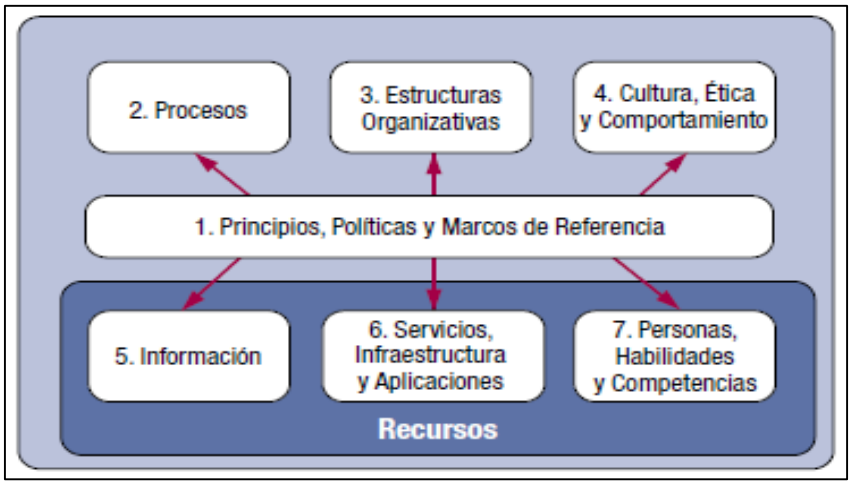


Figura 9. Catalizadores Corporativos COBIT 5
Fuente: Information Systems Audit and Control Association (ISACA, 2012a).

- **Principio 5: Separar el Gobierno de la Gestión:** El marco de trabajo COBIT 5 realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban

diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La posición de COBIT 5 hace esta fundamental distinción entre gobierno y gestión es:

- **Gobierno**

  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.

  En la mayoría de corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

- **Gestión**

  La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

  En la mayoría de empresas, la gestión es responsabilidad de la dirección ejecutiva bajo la dirección de la dirección ejecutiva del Director General Ejecutivo (C*hief Executive Officer, CEO*). (p. 31)

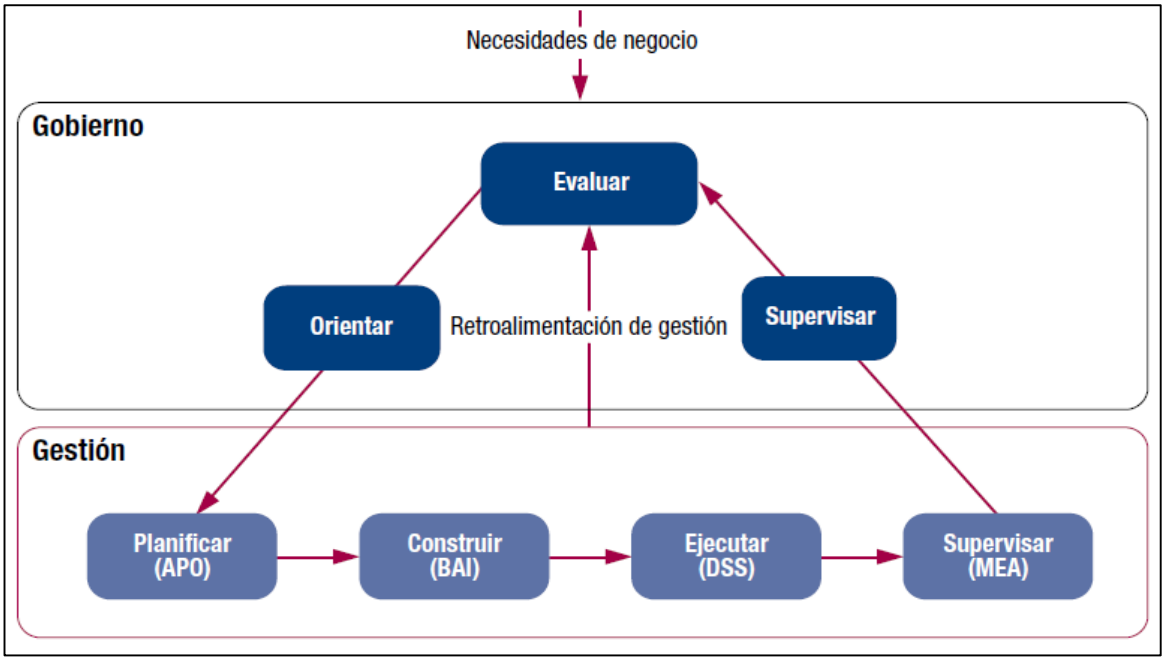


Figura 10. Las Áreas Clave de Gobierno y gestión de COBIT 5
Fuente: Information Systems Audit and Control Association (ISACA, 2012a).

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 cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (**EDM**).
- **Gestión**—Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (*Plan, Build, Run and Monitor* - **PBRM**), y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:
  – Alinear, Planificar y Organizar (*Align, Plan and Organise, **APO***)
  – Construir, Adquirir e Implementar (*Build, Acquire and Implement, **BAI***)
  – Entregar, dar Servicio y Soporte (*Deliver, Service and Support, **DSS***)
  – Supervisar, Evaluar y Valorar (*Monitor, Evaluate and Assess, **MEA***) (p. 32)

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas. (p.14)

La Figura 11 nos muestra los 37 procesos de Gobierno y de Gestión en COBIT 5:

Figura 11. Modelo de Referencia de Procesos de COBIT 5
Fuente: Information Systems Audit and Control Association (ISACA, 2012a).

1.3. ISO /IEC 38500:2015

Según la ISO/IEC 38500(2015):

> El objetivo de esta norma es proporcionar principios, definiciones, y un modelo para los órganos de gobierno a la hora de utilizar, evaluar, dirigir y monitorear el uso de tecnología de la información (TI) en sus organizaciones.
>
> Esta Norma Internacional proporciona principios, definiciones y un modelo para el buen gobierno de las TI, a ayudar aquellos en el más alto nivel de las organizaciones a entender y cumplir con sus obligaciones legales, regulatorios y obligaciones éticas relativas a la utilización de las TI de sus organizaciones.
>
> Esta Norma Internacional está dirigida principalmente al órgano rector. En algunos (típicamente más pequeños) las organizaciones, los miembros del órgano de gobierno también pueden ser gerentes ejecutivos. Esta Norma Internacional es aplicable a todas las organizaciones, desde el más pequeño al más grande, independientemente de ello, el diseño y la estructura de propiedad. (p. 3)

Además la ISO/IEC 38500 (2015) nos indica sobre la norma:

> Esta norma internacional establece los principios rectores para los miembros de los órganos de las organizaciones (que puede comprender los propietarios, directores, socios, gerentes ejecutivos, o similar) sobre el uso eficaz, eficiente y aceptable de la tecnología de la información (TI) dentro de sus organizaciones.
>
> También proporciona orientación a las asesorar, informar, o ayudar a los órganos de gobierno. Estos incluyen los siguientes:
>
> - Directores ejecutivos;
> - Miembros de grupos de vigilancia de los recursos dentro de la organización;
> - Especialistas en negocios o técnicos externos, tales como especialistas jurídicos y contables, asociaciones comerciales o industriales, u organismos profesionales;
> - Proveedores internos y externos de servicios (incluidos los consultores)
> - Auditores.
>
> La ISO/IEC 38500 se aplica a la gobernanza de uso actual y futuro de la organización de TI incluyendo procesos y decisiones relacionadas con el uso actual y futuro de la gestión de TI. Estos procesos pueden ser controlados por especialistas en TI dentro de la organización, los proveedores de servicios externos, o unidades de negocio dentro de la organización.
>
> La ISO/IEC 38500 define la gobernanza de TI como un subconjunto o dominio de gobierno de la organización, o en el caso de una corporación, gobierno corporativo.
>
> La ISO/IEC 38500 es aplicable a todas las organizaciones, incluidas las públicas y las empresas privadas, entidades gubernamentales y organizaciones sin fines de lucro. ISO/IEC 38500 es aplicable a las organizaciones de todos los tamaños desde el más pequeño hasta el más grande, independientemente de la extensión de su uso de las TI.
>
> El propósito de la ISO/IEC 38500 es promover el uso eficaz, eficiente y aceptable de TI en todas las organizaciones de:

- Asegurando las partes interesadas que, si se siguen los principios y las prácticas propuestas por la norma, pueden tener la confianza en el gobierno de la organización de TI,
- Informar y orientar a los órganos de gobierno en el que rige el uso de las TI en su organización, y
- El establecimiento de un vocabulario para la gobernanza de TI. (p. 1)

La ISO/IEC 38500 establece 6 principios para la gobernanza corporativa de las TI; los principios expresan el comportamiento deseado que orienten la toma de decisiones en la organización. Según la ISO/IEC (2015) estos principios son:

- **Principio 1: Responsabilidad**

  Los individuos y grupos dentro de la organización entienden y aceptan sus responsabilidades en relación con la oferta y la demanda de TI. Los responsables de las acciones también tienen la autoridad para llevar a cabo esas acciones.
- **Principio 2: Estrategia**

  La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de TI; los planes estratégicos de TI satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.
- **Principio 3: Adquisición**

  Las adquisiciones de TI se hacen por razones válidas, basándose en un análisis apropiado y continuo, con las decisiones claras y transparentes. Hay un equilibrio apropiado entre los beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.
- **Principio 4: Rendimiento**

  La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.
- **Principio 5: Conformidad**

  La función de TI cumple con todas las leyes y normas aplicables. Las políticas y prácticas están claramente definidas, implementadas y exigidas.
- **Principio 6: Comportamiento Humano**

  Las políticas de TI, prácticas y decisiones demuestran respeto por el comportamiento humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada. (p. 8)

Además de los principios la norma ISO/IEC 38500 se basa en un modelo con tres tareas principales, la ISO/IEC (2015) expresa:

- **Evaluar** el uso actual y futuro de las TI. Los administradores deberían valorar la situación y formular juicios sobre el uso actual y futuro de la TI, incluyendo estrategias, propuestas y acuerdos de prestación de servicios (ya sean internos, externos o ambos)

  Al evaluar el uso de la TI, los administradores deberían considerar las presiones externas o internas que actúan sobre el negocio como pueden ser los cambios tecnológicos, las tendencias económicas y sociales y las influencias políticas. Dado que dichas influencias cambian, los administradores deberían realizar evaluaciones de forma continua.

  Los administradores también deberían tener en cuenta las necesidades actuales y futuras del negocio, los objetivos organizativos actuales y futuros que deben alcanzar, tales como el mantenimiento de la ventaja competitiva, así como los objetivos específicos de las estrategias y propuestas que están evaluando.

- **Orientar (dirigir)** la preparación y ejecución de planes y políticas para asegurar que el uso de la TI satisface los objetivos de la organización. Los administradores deberían asignar responsabilidades y dirigir la preparación e implantación de planes y políticas. Los planes deberían fijar el rumbo de inversiones en proyectos y operaciones de TI. Las políticas deberían establecer una conducta responsable en el uso de la TI.

  Los administradores deberían asegurar que la transición de los proyectos a un estado operativo se planifique y gestione adecuadamente, teniendo en cuenta el impacto en el negocio y las prácticas operativas, y los sistemas e infraestructura de TI existentes.

  Los administradores deberían fomentar una cultura de gobernanza de la TI en su organización, exigiendo a la dirección que suministre puntualmente la información adecuada, con el fin de cumplir con los objetivos establecidos y ajustarse a los seis principios de gobernanza.

Si fuera necesario los administradores deberían controlar la presentación de propuestas a aprobar para responder a las necesidades identificadas.

- **Supervisar** el cumplimiento de las políticas y el desempeño con relación a lo planificado. Los administradores deberían monitorizar el desempeño de la TI, a través de sistemas de medición adecuados. Deberían asegurarse de que dicho desempeño esté en conformidad con los planes, en particular con respecto a los objetivos de negocio.

  Los administradores deberían también asegurar que la TI cumple con las obligaciones externas (normativa, legislación, derecho consuetudinario, contractuales) y las prácticas internas de trabajo. (p.p. 11, 12)

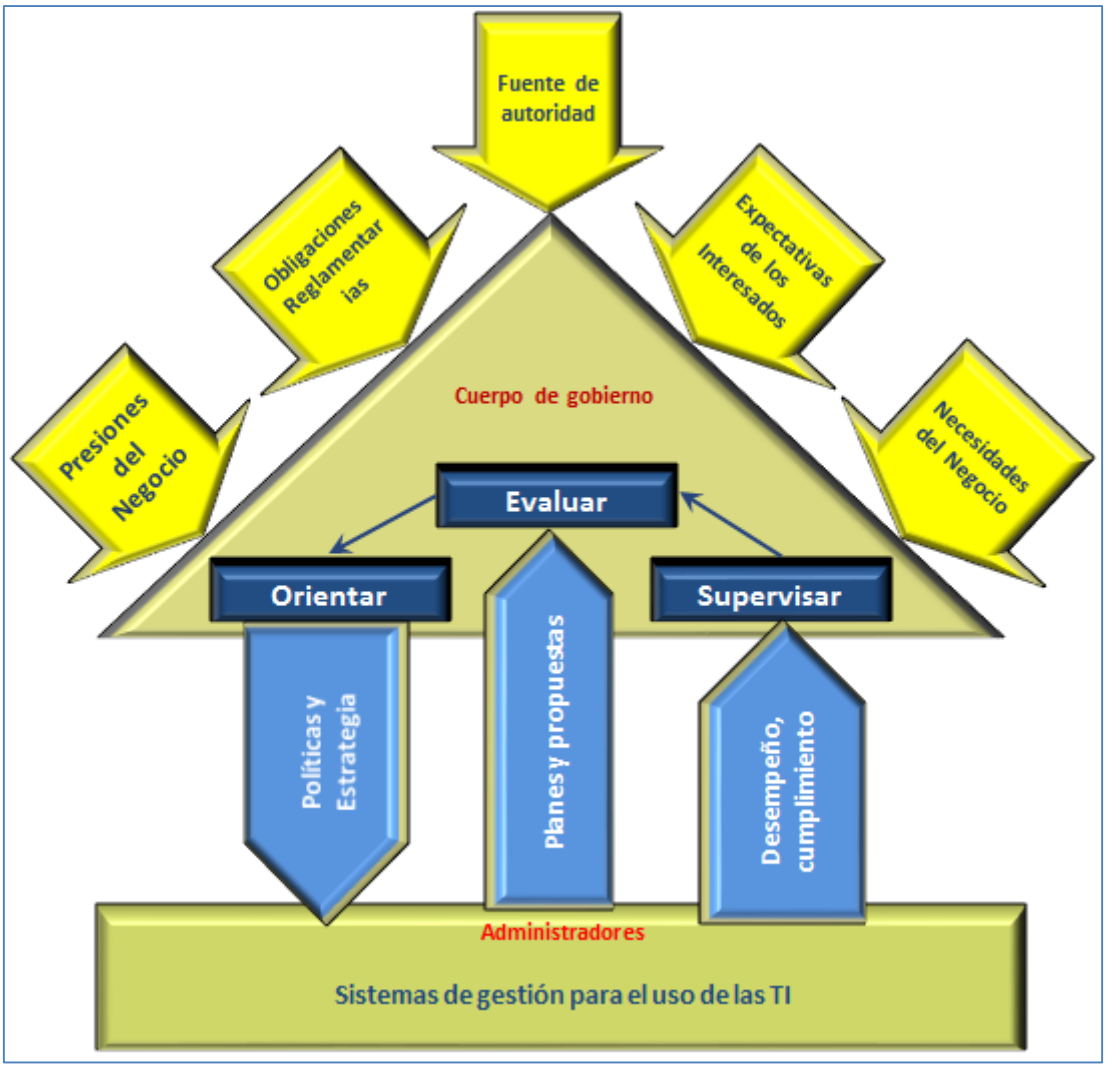


Figura 12. Modelo de Gobernanza Corporativa de las TI
Fuente: adaptado de International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2008).

A continuación la Figura 13 resume las tareas y principios de la norma ISO /IEC 38500-2015:

PRINCIPIOS	EVALUAR	ORIENTAR	SUPERVISAR
RESPONSABILIDAD	• Asignación de responsabilidades • Competencias de responsabilidades	• Planes con responsabilidad asignada • Recibir información y rendir cuentas	• Mecanismos establecidos de Gobierno TI • Asignación de responsabilidades • Desempeño de responsabilidades de Gobierno TI
ESTRATEGIA	• Evolución de la TI y procesos de negocio • Actividades de TI y su alineamiento con objetivos de la organización • Mejores prácticas • Satisfacción de interesados • Valoración y evaluación del riesgo	• Creación y uso de planes y políticas • Alentar propuestas innovadoras • Mejorar procesos actuales de negocio • Emprender nuevos procesos de negocio	• Monitorizar el progreso de propuestas aprobadas • Asegurar alcanzar objetivos en plazos establecidos • Uso de recursos asignados • Uso de TI alcance beneficios esperados
ADQUISICIÓN	• Alternativas propuestas de TI • Propuestas aprobadas • Análisis de riesgo / valor • Inversiones propuestas	• Activos de TI se adquieren de manera apropiada • Elaboración de documentación adecuada con capacidades requeridas • Acuerdos de provisiones soporten las necesidades de la organización	• Inversiones de TI proveen las capacidades requeridas • Entendimiento interno y externo del propósito de la organización
DESEMPEÑO	• TI sustenta procesos de negocio con capacidades y aptitudes requeridas • Riesgos para la continuidad del negocio • Riesgos para la integridad de la información y proyección de activos • Decisiones uso TI para alcanzar objetivos del negocio • Eficacia y desempeño de gobernanza de la TI	• Asignación de recursos suficientes • Asignación de prioridades y restricciones • Satisfacer necesidades del negocio • Información sea correcta, actualizada y protegida	• Grado que TI sustenta el negocio • Grado que los recursos e inversiones son priorizados con objetivos del negocio • Política de precisión de datos (fiabilidad, exactitud e integridad) • Política uso eficiente de TI
CUMPLIMIENTO	• Grado que TI cumple con obligaciones, políticas internas, normas y directrices • Conformidad con la gobernanza TI	• TI cumple con obligaciones, normas y políticas establecidas. • Establecer y aplicar políticas (uso interno TI) • Personal de TI cumple con directrices, desarrollo y conducta profesional • Ética rija acciones relacionadas con TI	• Cumplimiento y conformidad de la TI (auditorias / informes) • Las revisiones sean oportunas, completas y adecuadas (evaluación satisfacción del negocio) • Actividades TI
CONDUCTA HUMANA	• Las actividades TI que aseguren que las conductas humanas se identifican y se consideran adecuadamente	• Actividades TI compatibles con la conducta humana • Informar cualquier individuo y en cualquier momento sobre riesgos, problemas y preocupaciones del negocio • Administración riesgos según políticas y procedimientos • Comunicar a los responsables de toma decisiones	• Actividades de TI que aseguren conductas humanas adecuadas y oportunas • Prácticas de trabajo son consistentes con el uso apropiado de TI

Figura 13 Directrices de la norma ISO/IEC 38500:2015
Fuente: adaptado de la International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2015)

1.4. ISO/IEC 27002:2013

La ISO/IEC (2013) nos menciona que el estándar ISO/IEC 27002 describe cómo gestionar la seguridad de la información para una empresa. Además el estándar ayuda a las organizaciones a establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

Según la ISO/IEC 27002(2013):

Esta Norma está diseñada para que las organizaciones que utilizan como referencia la selección de los controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 o como un documento de orientación para las organizaciones que efectúan controles de seguridad de la información generalmente aceptadas. Esta norma también está destinada para su uso en la elaboración de directrices de gestión de seguridad de la información y la industria específicas de la organización, teniendo en cuenta su entorno de riesgo seguridad de la información específica (s).

La seguridad de la información eficaz reduce estos riesgos mediante la protección de la organización contra las amenazas y vulnerabilidades, y luego reduce los impactos de sus activos. La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizativas y de software y funciones del hardware. La seguridad de la información eficaz también asegura la gestión y otras partes interesadas que los activos de la organización son razonablemente seguros y protegidos contra daños, lo cual actúa como un habilitador de negocios.

Selección de los controles

La selección de los controles depende de decisiones de la organización sobre la base de los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque general de gestión de riesgos aplicado a la organización, y también debe estar sujeta a todas las leyes y regulaciones nacionales e internacionales relevantes. La selección de controles también depende de la manera en que los controles interactúan para proporcionar una defensa en profundidad.

Consideraciones del ciclo de vida

La información tiene un ciclo de vida natural, desde la creación y la emisión hasta su almacenamiento, procesamiento, uso y transmisión a su eventual destrucción o deterioro. El valor de la información y riesgos para los activos pueden variar durante su vida, pero la seguridad de la información sigue siendo importante hasta cierto punto en todas las etapas. Los sistemas de información tienen ciclos de vida dentro de la cual se conciben, se especifican, son diseñados, desarrollados, probados, implementados, utilizados, mantenidos y, finalmente, retirados del servicio y eliminados.

Alcance

Esta norma internacional nos da las guías para los estándares de la seguridad de la información organizacional y prácticas para la gestión de la seguridad de la información, incluyendo la selección, implementación y gestión de controles, tomando en consideración el riesgo de seguridad de la información en el entorno de la organización.

El estándar está diseñado para ser usado por organizaciones que pretenden:

a) Seleccionar controles a través de implementación de procesos en un sistema de gestión de la seguridad de la información basados en ISO/IEC 27001.
b) Implementar controles de seguridad comúnmente aceptados
c) Desarrollar sus propias directrices de gestión de la seguridad de la información. (p.p. 3-5)

En la Figura 14 se detalla los 114 controles de la norma ISO/IEC 27002:2013:

Figura 14. ISO/IEC 27002:2013, dominios, objetivos de control y controles
Fuente: ISO27000.ES. (2016).

CAPITULO 2. INFORMACIÓN DE LA EMPRESA SELECCIONADA

2.1. Introducción:

Memorial International of ecuador S.A. es una organización Ecuatoriana líder e innovadora en servicios exequiales tanto en previsión como en necesidad inmediata, con asistencia nacional e internacional.

Más de quince años en el mercado nos han convertido en la mejor y la más grande organización del sector funerario del país.

2.2. Misión

Apoyar a la familia ante la pérdida de un ser querido, ofreciendo servicios profesionales tanto de previsión y en necesidad inmediata con profundo contenido humano y espiritual, generando un vínculo afectivo con la comunidad.

2.3. Visión

Ser reconocidos a nivel internacional por la excelencia en el servicio siendo el símbolo de la asistencia exequial internacional, actuando con ética y seriedad, contando con recurso humano comprometido**.**

2.4. Valores

Compromiso
Transparencia
Espiritualidad
Alegría
Tenacidad

2.5. Organigrama empresarial

Por motivos académicos se presenta el diagrama de la Figura 15, pero adicionalmente se tiene varios roles para poder realizar este trabajo y a continuación se listan:

- Gerencia Legal
- Gerencia de Talento Humano
- Ejecutivos de negocio: gerentes de las diferentes agencias y departamentos.
- Propietarios o dueños de proceso de negocio: asistentes administrativos, asistentes de contabilidad, asistentes de cobranzas, asistentes de servicio al cliente, asistente de archivo, asesores call center.

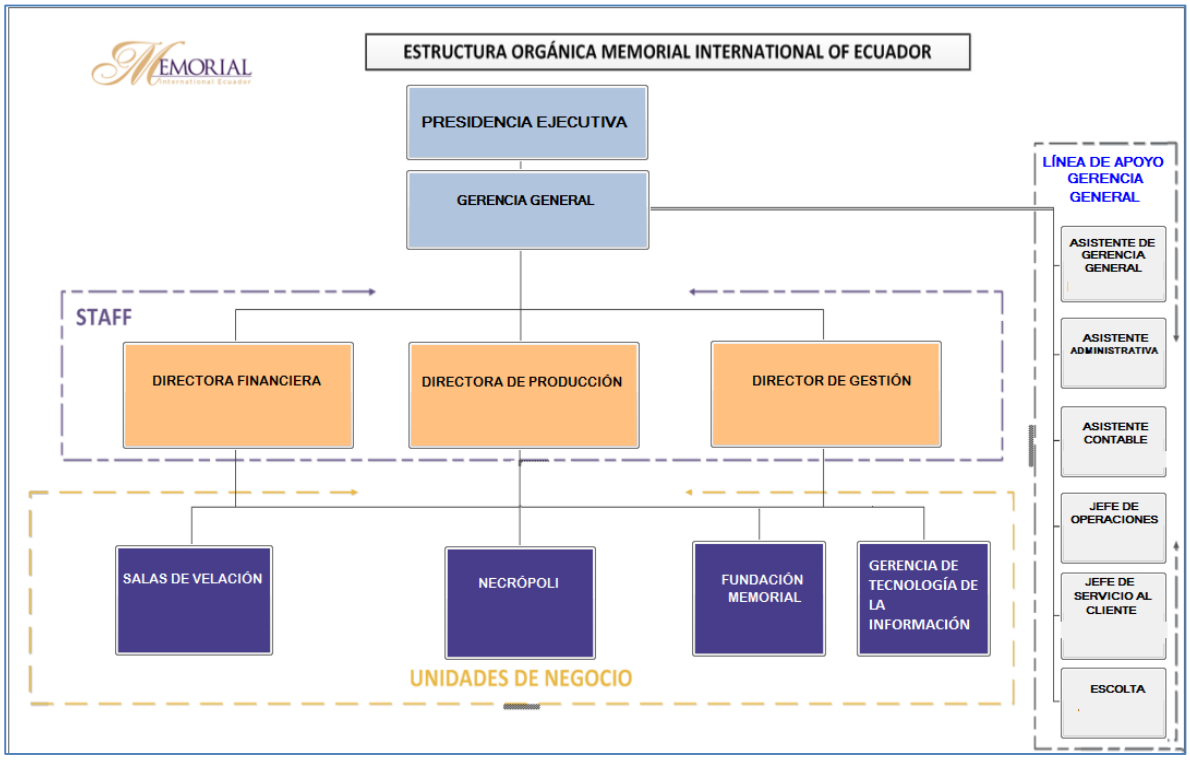


Figura 15. Estructura Orgánica Memorial International of Ecuador
Fuente: Memorial International of Ecuador

2.6. Tecnologías de la información

Las Tecnologías de la Información (TI) de Memorial International ayudan a la consecución de los objetivos empresariales, para ello vamos a describir la organización de las mismas.

2.6.1. Organigrama TI

Figura 16. Organigrama TIC's de Memorial International of Ecuador S.A.
Fuente: el autor

El organigrama de la Figura 16 se tiene las posiciones a continuación descritas:

- **Gerente de Sistemas**: mantener operativa la plataforma informática a nivel de hardware, software y comunicaciones implementando proyectos tecnológicos dependiendo de las necesidades de la organización a fin de garantizar efectividad en todos los procesos y resultados de la información
- **Administrador de Base de Datos**: administrar y monitoreas los servidores, aplicaciones y datos que posee la Organización, para mantener la integridad, seguridad y disponibilidad de cada uno de estos.
- **Soporte Help Desk:** realizar trabajos de ensamblado de equipos de cómputo, instalaciones y cableado estructurado, así como la instalación y mantenimiento de hardware y software a fin de garantizar el funcionamiento adecuado de los equipos y sistemas informáticos de la Organización**.**
- **Asistente de Sistemas:** mantener operativas las comunicaciones de la empresa tanto a nivel de redes como de telefonía IP, a fin de asegurar el funcionamiento normal de las mismas.

2.6.2. Aplicaciones de negocio

Memorial International of Ecuador S.A. tiene las siguientes aplicaciones para el desarrollo de sus actividades:

- **Mine**: desarrollo propio de la empresa, sirve para la gestión de clientes y las ventas de la Organización a nivel de Ecuador. La utiliza la parte de producción de la empresa.
- **Mine International**: desarrollo propio de la empresa, sirve para la gestión de clientes y las ventas de la Organización a nivel de las filiales internacionales de la Organización. La utiliza la parte de producción de la empresa.
- **SAFI**: sistema propietario utilizado para la gestión contable de la empresa utilizado por el área financiera de la Organización.
- **Teleya**: sistema propietario, se utiliza para gestión del Call Center de la Organización.
- **ContacVox**: sistema propietario, se utiliza para gestión del Call Center.
- **Gameda:** sistema propietario, se utiliza para consultas de la contabilidad de años anteriores.
- **Linux:** software libre, utilizado para la gestión de correos de la organización.
- **Motor de llamadas:** software propietario, se utiliza para la gestión de motores de llamadas de la Organización.
- **WatchGuard**: firewall empresarial, utilizado para seguridades periféricas e internas de la Organización.

- **Kaspersky Enterprise Security:** software propietario, antivirus empresarial, utilizado para seguridades de cada computador personal de la Organización.
- **Cpanel:** gestor de dominios de la organización, utilizado para administrar cuentas de correo, listas de correo, FTP.
- **PRTG:** monitor de los enlaces de datos e internet que posee la Organización con sus sucursales en Ecuador.
- **Columbarios**: sistema para administración de columbarios en Necrópoli.
- **Sistema de salas**: desarrollo propio de la empresa, sirve para la gestión de los clientes en salas de velación.
- **RMX Policom**: sistema propietario, sirve para gestionar video conferencias ente las filiales nacionales e internacionales de la Organización.

2.6.3. Diagrama de redes y comunicaciones

La Figura 16 muestra cómo se conectan las diferentes sucursales que tiene la empresa.

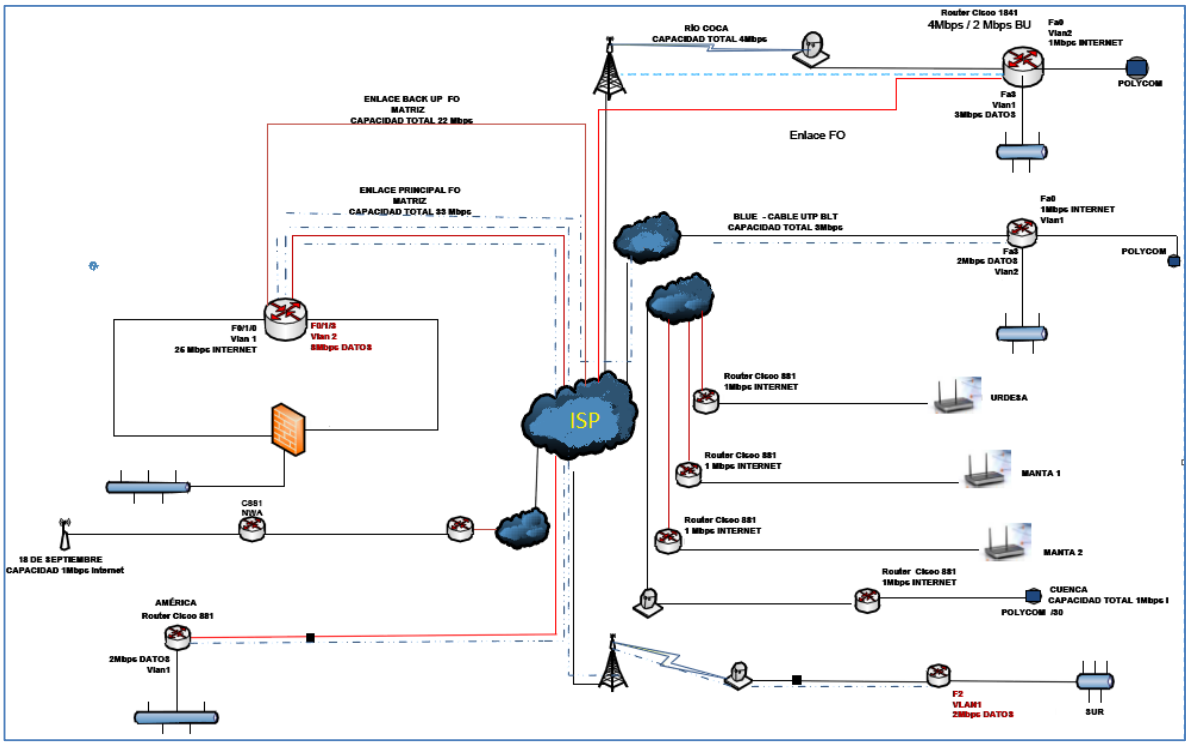


Figura 17. Diagrama de comunicaciones Memorial International of Ecuador
Fuente: Memorial International of Ecuador

CAPITULO 3. TRABAJO SOBRE LA EMPRESA SELECCIONADA

3.1. Realizar análisis del estado actual

Para tener conocimiento del estado actual de la empresa se realizará un análisis basando en los modelos de madurez de la ISO 9004 analizados para cada principio de la ISO/IEC 38500 y sus respectivas tareas. Este análisis será desarrollado por encuestas a 5 personas, 4 de las mismas conforman el departamento de TI y la persona restante se realizó la encuesta al Director de Gestión, quien es la persona que está en un nivel más alto que el Gerente de TI de la organización. El instrumento utilizado para la encuesta se lo tiene en el ANEXO 1. En la Figura 18, se tiene un ejemplo del instrumento que se utilizará:

Principio	Tarea	Nivel de Madurez					Nivel actual	Nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
2. Estrategia	Evaluar	Los directores de TI, evalúan y brindan soporte a las necesidades actuales del negocio.	Los directores de TI estudian los avances de la tecnología de la información y los procesos del negocio con el fin de asegurarse de que TI brinda soporte a las necesidades futuras del negocio. (Los resultados de dicha evaluación se encuentran documentadas)	Los directores de TI evalúan y monitorean las actividades de TI, pero no aseguran que estas se mantengan (con el paso del tiempo) alineadas con los objetivos de la organización.	Los directores de TI cuentan con un plan estratégico de TI, el cual tiene en cuenta los planes y las políticas de la organización. Los directores de TI evalúan periódicamente que las actividades de TI se mantengan alineadas con los objetivos de la organización. (Los resultados de dicha evaluación y alineación con los objetivos de la organización se encuentran documentados)	Los directores de TI garantizan que sus procesos podrían ser (en cualquier momento), verificados, auditados y/o evaluados tal como se describe en normas nacionales e internacionales pertinentes.		
	Dirigir	Los usuarios conocen los procesos de TI de la Organización.	Los usuarios de la Organización están autorizados para presentar propuestas de innovación para TI	La Organización fomenta y estimula la presentación de propuestas de innovación de TI. (Se tiene establecido un procedimiento, formato lineamiento, etc., que evidencie la forma como se fomenta dicha actividad)	Los directores de TI tienen establecidos procedimientos y/o formatos para la presentación y recepción de propuestas de innovación en TI.	Los directores de TI fomentan y evalúan que estas propuestas permitan a la organización responder a oportunidades, nuevos retos, mejorar los procesos de la organización y/o estén alineadas con los objetivos del negocio.		
	Supervisar	La Organización cuenta con una metodología para la ejecución de proyectos	Todos los proyectos de la organización (incluidos los de TI) son monitoreados para supervisar el progreso de los mismas	Los directores de TI conocen y supervisan el progreso de los proyectos de TI. (Dicha supervisión se encuentra debidamente documentada)	Los directores de TI no solo supervisan el progreso del avance de los proyectos de TI, sino que se asegura que se estén cumpliendo los objetivos y beneficios planteados.	Los directores de TI, supervisan el uso de TI para asegurar que de ésta, se obtienen los beneficios previstos y que continúen alineados con los objetivos de la organización.		

Figura 18. Evaluación de nivel de madurez de Gobierno TI basado en ISO/IEC 38500 e ISO9004
Fuente: adaptado de Correa, M., & Parra B. (2012). .

Luego de las evaluaciones del ANEXO 1, se realizó un formato para toma de resultados obtenidos en las encuestas, mismo que se lo puede encontrar en el ANEXO 2, a continuación en la Figura 19 un ejemplo del formato de análisis:

Principio	Tarea	Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
		Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
1. Responsabilidad	Evaluar												
	Dirigir												
	Supervisar												

Figura 19. Formato de toma de resultados de nivel de madurez de gobierno TI
Fuente: adaptado de Correa, M., & Parra B. (2012).

Para los resultados tanto del nivel actual como del nivel deseado de la Figura 19 se realizó un promedio de los 5 encuestados. En el ANEXO 3 se tiene el formato para los análisis individual y global de los resultados obtenidos a las encuestas. Los resultados de cada principio de la ISO/IEC 38500 se los presentará como se muestra en la Figura 20:

Nivel de madurez de Gobierno de TI Principio 1. Responsabilidad			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	0	0	5
Dirigir	0	0	5
Supervisar	0	0	5

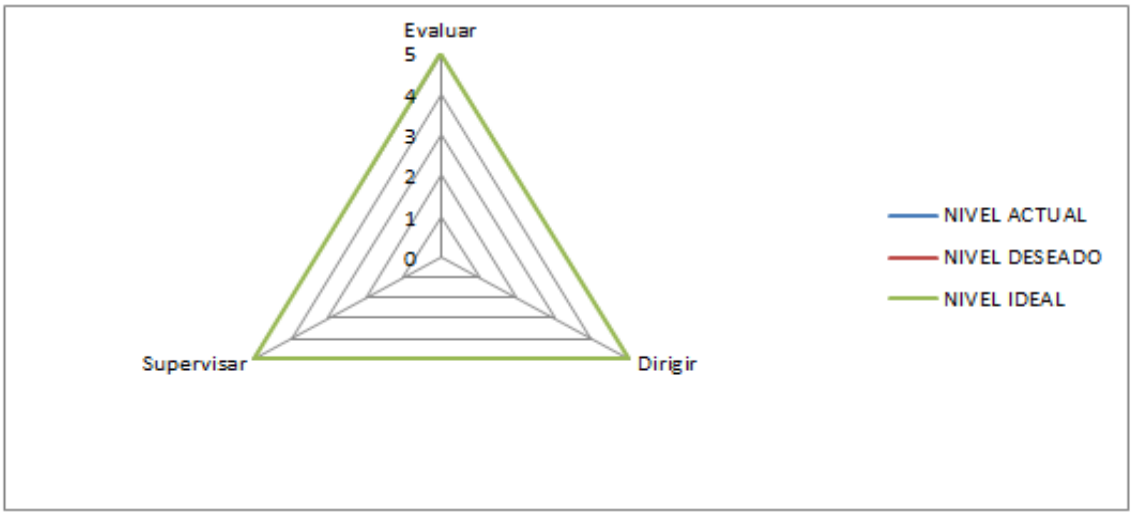


Figura 20. Formato de análisis individual de resultados del nivel de madurez de gobierno TI
Fuente: adaptado de Correa, M., & Parra B. (2012).

En la Figura 20 se copia los resultados obtenidos del promedio obtenido para cada principio con sus respectivas tareas del ANEXO 2, luego se muestra en un gráfico que permite visualizar los resultados de cada principio con sus respectivas tareas.

Finalmente en el ANEXO 3 se tiene un formato de análisis global del nivel de madurez de gobierno TI, en este formato se realiza un promedio de los resultados obtenidos para cada principio de la norma ISO/IEC 38500 con sus tres tareas respectivas, tanto del nivel actual como del nivel deseado y a continuación un gráfico de los resultados para una mejor visualización de los mismos. La Figura 21 mostrará los resultados globales de los principios de la norma ISO/IEC 38500:

Nivel de madurez de Gobierno de TI			
Principios	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
1. Responsabilidad	0	0	5
2. Estrategia	0	0	5
3. Adquisición	0	0	5
4. Dsempeño	0	0	5
5. Cumplimiento	0	0	5
6. Comportamiento Humano	0	0	5

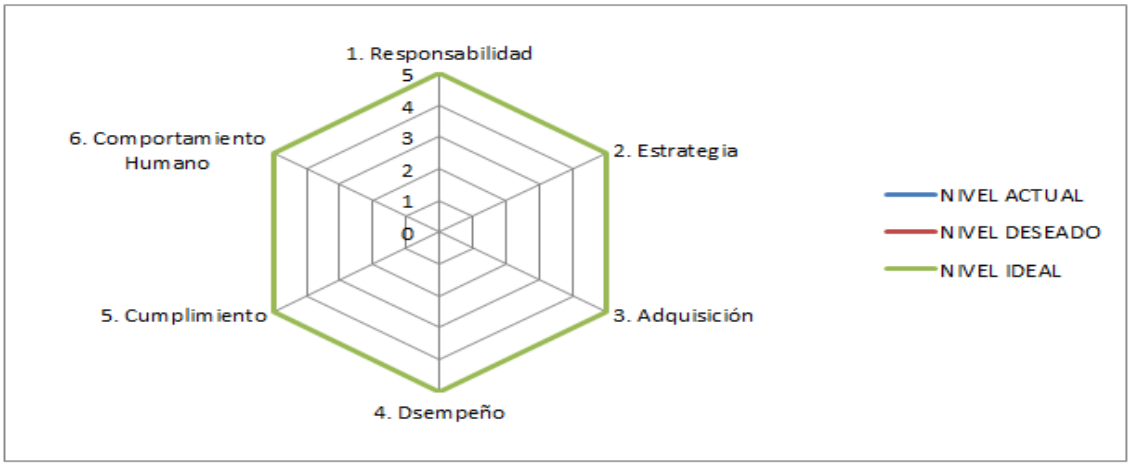


Figura 21. Formato de análisis global de resultados del nivel de madurez de gobierno TI
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados de las encuestas del nivel de madurez de Gobierno TI basado en la ISO/IEC 38500 e ISO 9004 del ANEXO 1 que se realizó a todo el personal de TI de la empresa más el Gerente de Desarrollo de Memorial International of Ecuador, se detalla para cada principio de la norma ISO/IEC 38500:2015.

La Tabla 2 muestra los resultados para el primer principio de la ISO/IEC 38500 y se muestra a continuación:

Tabla 2. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 1 de la norma ISO/IEC 38500.

Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
1. Responsabilidad	Evaluar	4	5	3	5	1	4	2	5	1	3	**2.2**	**4.4**
	Dirigir	3	5	4	5	2	4	1	5	1	4	**2.2**	**4.6**
	Supervisar	2	5	4	5	2	4	2	5	1	3	**2.2**	**4.4**

Fuente: adaptado de Correa, M., & Parra B. (2012).

La Figura 22 es la representación gráfica de los resultados obtenidos para el primer principio de la ISO/IEC 38500 y se muestra a continuación:

Nivel de madurez de Gobierno de TI Principio 1. Responsabilidad			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	2.2	4.4	5
Dirigir	3	4.8	5
Supervisar	2.4	4.4	5

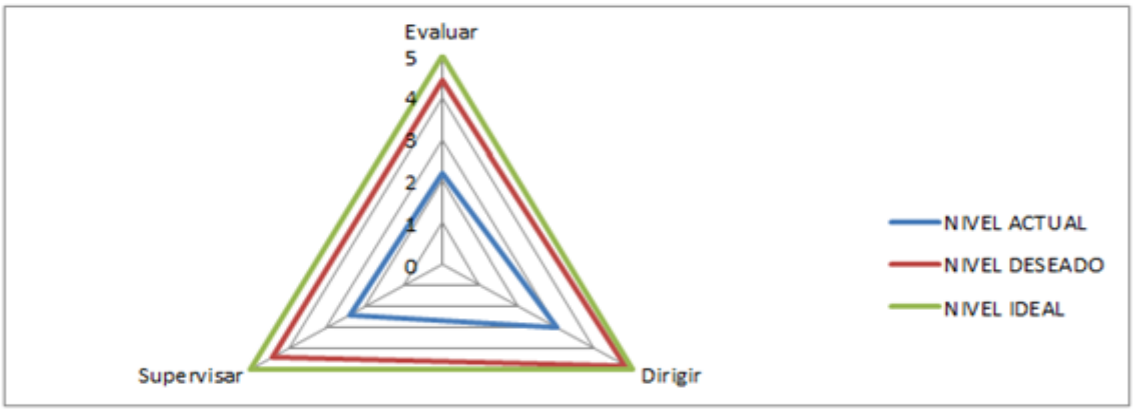


Figura 22. Resultados de nivel de madurez de gobierno TI. Principio 1
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados obtenidos para el Principio 1 indican que en el nivel actual de la empresa, los individuos o grupos dentro de la organización no tienen claras sus responsabilidades con respecto al suministro y demanda de la información. El gerente de TI establece reglas y responsabilidades con relación al uso actual y futuro de las tecnologías de la información de la organización. El gerente de TI dirige todos los proyectos de tecnología de la organización y cuenta con autoridad parcial para solicitar información de otras dependencias. El gerente de TI tiene algún conocimiento acerca de gobierno de TI, además conoce y supervisa que se hayan establecido los mecanismos adecuados para el gobierno de TI.

El nivel al que desea llegar la empresa es que el gerente de TI tendrá alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encontrará documentado. El gerente de TI verificará que todos los proyectos de tecnología, estén alineadas con las responsabilidades asignadas al área de TI y exigirá que se le entregue la información que necesita para cumplir su responsabilidad, incluidas las relativas a acciones y toma de decisiones. El gerente de TI supervisará y/o auditará periódicamente el desempeño de aquellos a quienes se ha asignado responsabilidad en el gobierno de TI.

La Tabla 3 muestra los resultados para el segundo principio de la ISO/IEC 38500 y se muestra a continuación:

Tabla 3. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 2 de la norma ISO/IEC 38500.

Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
2. Estrategia	Evaluar	3	5	2	4	1	4	2	5	1	4	**1.8**	**4.4**
	Dirigir	1	5	4	5	0	4	1	5	1	3	**1.4**	**4.4**
	Supervisar	2	5	4	5	1	4	0	5	0	3	**1.4**	**4.4**

Fuente: adaptado de Correa, M., & Parra B. (2012).

La Figura 23 es la representación gráfica de los resultados obtenidos para el segundo principio de la ISO/IEC 38500 y se muestra a continuación:

Nivel de madurez de Gobierno de TI Principio 2. Estrategia			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	1.8	4.4	5
Dirigir	1.4	4.4	5
Supervisar	1.4	4.4	5

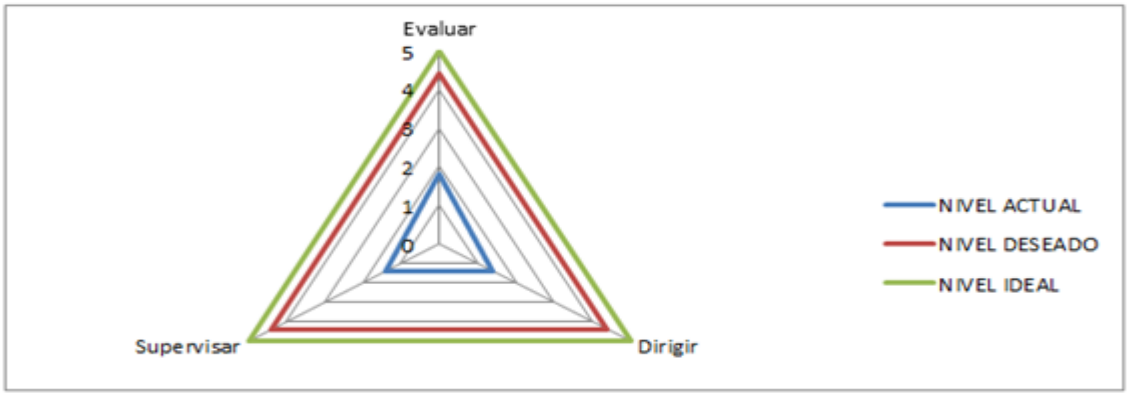


Figura 23. Resultados de nivel de madurez de gobierno TI. Principio 2
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados obtenidos para el Principio 2 indican que el nivel actual de la empresa el gerente de TI, evalúa y brinda soporte a las necesidades actuales del negocio. El gerente de TI estudia los avances de la tecnología de la información y los procesos del negocio con el fin de asegurarse que TI brinda soporte a las necesidades futuras del negocio. Los usuarios conocen los procesos de TI de la Organización.

El nivel al que desea llegar la empresa es que la organización cuente con una metodología para la ejecución de proyectos. El gerente de TI cuente con un plan estratégico de TI, el cual tendrá en cuenta los planes y las políticas de la organización. El gerente de TI evaluará periódicamente que las actividades de TI se mantengan

alineadas con los objetivos de la organización. El gerente de TI tendrá establecidos procedimientos y/o formatos para la presentación y recepción de propuestas de innovación en TI. El gerente de TI no solo supervisará el progreso del avance de los proyectos de TI, sino que se asegurará que se estén cumpliendo los objetivos y beneficios planteados.

La Tabla 4 muestra los resultados para el tercer principio de la ISO/IEC 38500 y se muestra a continuación:

Tabla 4. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 3 de la norma ISO/IEC 38500.

Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
3. Adquisición	Evaluar	4	5	2	5	1	4	1	5	1	4	**1.8**	**4.6**
	Dirigir	3	5	3	5	1	4	1	5	1	4	**1.8**	**4.6**
	Supervisar	2	5	2	5	1	5	2	5	0	3	**1.4**	**4.6**

Fuente: adaptado de Correa, M., & Parra B. (2012).

La Figura 24 es la representación gráfica de los resultados obtenidos para el tercer principio de la ISO/IEC 38500 y se muestra a continuación:

Nivel de madurez de Gobierno de TI Principio 3. Adquisición			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	1.8	4.6	5
Dirigir	1.8	4.6	5
Supervisar	1.4	4.6	5

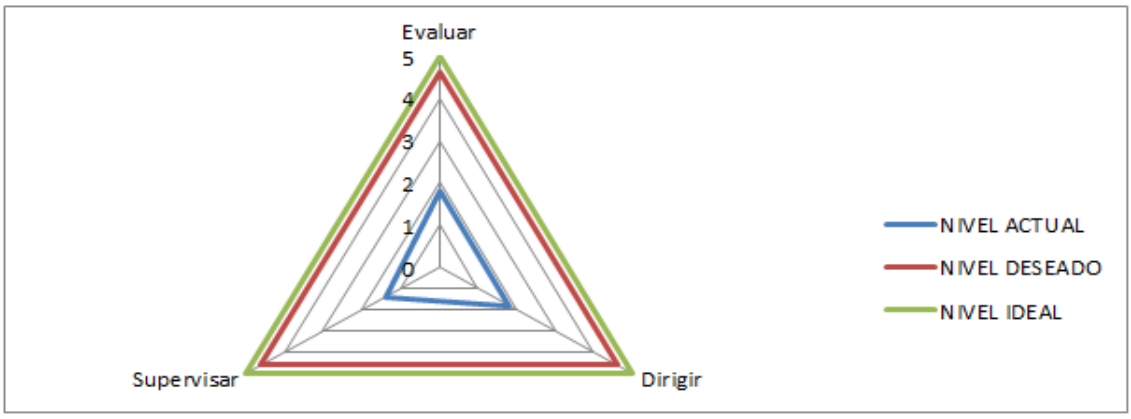


Figura 24. Resultados de nivel de madurez de gobierno TI. Principio 3
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados obtenidos para el Principio 3 indican que cualquier proceso dentro de la Organización puede solicitar un requerimiento para la adquisición tecnología. El gerente de TI evalúa diferentes opciones al momento de adquirir tecnología, pero no es el único encargado de aprobar la propuesta. El gerente de TI gestiona y mantiene los activos de TI (sistemas e infraestructura), además adquiere tecnología de forma correcta, clara y transparente, teniendo en cuenta los requerimientos planteados. La organización cuenta con mecanismos para supervisar que las inversiones, en términos generales, están acordes con las requeridas.

El nivel al que desea llegar la empresa es que el gerente de TI apruebe la mejor propuesta que dé cumplimiento a los requerimientos planteados, además que garantice el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo. Se cuente con un procedimiento documentado y/o formatos que evidencien el cumplimiento del equilibrio mencionado. El gerente de TI gestionará los acuerdos de nivel de servicio (tanto internos como externos) de modo que asegure que estos soportan las necesidades del negocio, se contará con un procedimiento documentado y/o formatos que evidencien el cumplimiento de los acuerdos de nivel de servicio. El gerente de TI supervisará (auditará) que las inversiones en TI, proporcionan las capacidades requeridas para las cuales fueron adquiridas, se tendrá algún tipo de procedimiento y/o formato que permita evidenciar el resultado de la supervisión realizada en las inversiones de TI. El gerente de TI tendrá contacto y/o alianzas estratégicas con los todos los proveedores de tecnología.

La Tabla 5 muestra los resultados para el cuarto principio de la ISO/IEC 38500 y se muestra a continuación:

Tabla 5. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 4 de la norma ISO/IEC 38500.

Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
4. Desempeño	Evaluar	2	5	3	5	1	4	1	5	1	3	**1.6**	**4.4**
	Dirigir	2	5	2	4	1	5	1	5	0	3	**1.2**	**4.4**
	Supervisar	2	5	1	5	1	4	0	5	1	3	**1**	**4.4**

Fuente: adaptado de Correa, M., & Parra B. (2012).

La Figura 25 es la representación gráfica de los resultados obtenidos para el cuarto principio de la ISO/IEC 38500 y se muestra a continuación:

Nivel de madurez de Gobierno de TI Principio 4. Desempeño			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	1.6	4.4	5
Dirigir	1.2	4.4	5
Supervisar	1	4.4	5

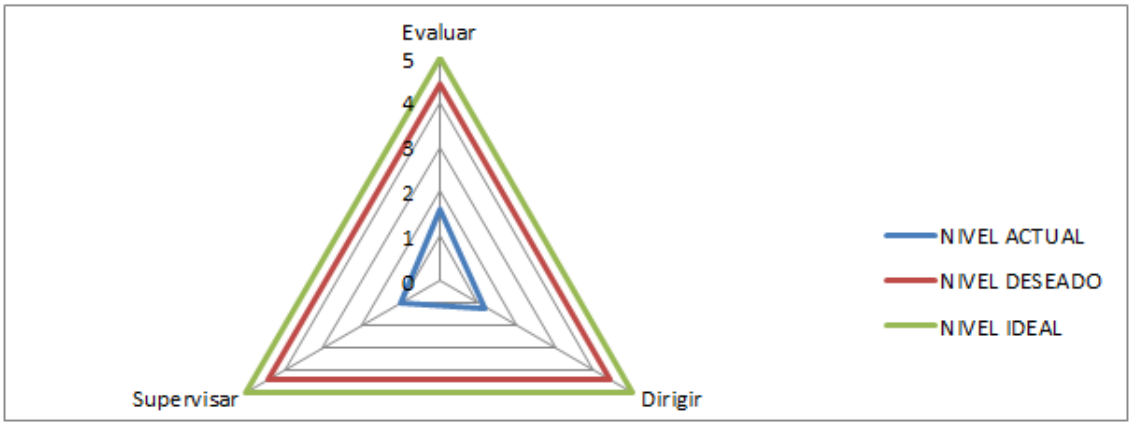


Figura 25. Resultados de nivel de madurez de gobierno TI. Principio 4
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados obtenidos para el Principio 4 indican que el gerente de TI evalúa que la tecnología de la información apoya los procesos de negocio con la habilidad y capacidad requeridas. El gerente de TI tiene políticas dirigidas hacia la continuidad de la operación normal del negocio y del tratamiento de los riesgos asociados con el uso de la tecnología de la información. La organización cuenta con un mecanismo de asignación de recursos para sus diferentes procesos. El gerente de TI supervisa la vida útil de la tecnología de la información que da soporte al negocio.

El nivel al que desea llegar la organización es que el gerente de TI garantizará que la tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, los acuerdos de niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio, soportando las metas del negocio. El gerente de TI garantizará que los recursos que le son asignados, satisfacen las necesidades de la organización. La información que soporta al negocio, se encontrará disponible cuando se requiere, con datos correctos y actualizados y están protegidos contra pérdida o mal uso. Se tendrá establecido un cronograma, el cual se encuentra supervisado, con renovación de la tecnología de la información, de igual forma se tendrá asegurado los recursos para dicha renovación.

El gerente de TI poseerá, controlará y supervisará el presupuesto asignado por la organización para la inversión de TI

La Tabla 6 muestra los resultados para el quinto principio de la ISO/IEC 38500 y se muestra a continuación:

Tabla 6. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 5 de la norma ISO/IEC 38500.

Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
5. Conformidad	Evaluar	2	5	1	5	1	4	1	5	0	3	**1**	**4.4**
	Dirigir	2	5	3	5	1	5	1	5	1	2	**1.6**	**4.4**
	Supervisar	1	5	4	5	1	4	0	5	0	3	**1.2**	**4.4**

Fuente: adaptado de Correa, M., & Parra B. (2012).

La Figura 26 es la representación gráfica de los resultados obtenidos para el quinto principio de la ISO/IEC 38500 y se muestra a continuación:

Nivel de madurez de Gobierno de TI Principio 5. Cumplimiento			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	1	4.4	5
Dirigir	1.6	4.4	5
Supervisar	1.2	4.4	5

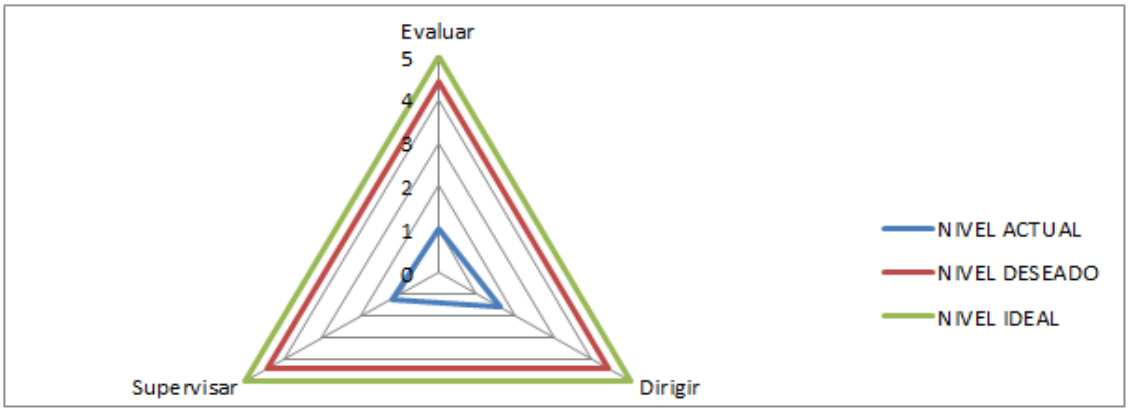


Figura 26. Resultados de nivel de madurez de gobierno TI. Principio 5
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados obtenidos para el Principio 5 indican que el gerente de TI garantiza que le tecnología de la Información cumple con todos lineamientos establecidos por la

organización. La organización garantiza que se cumple con las obligaciones legales pertinente. El gerente de TI colabora con la Alta Gerencia para establecer mecanismos regulares y rutinarios que garanticen que el uso de la tecnología de la información cumple con las obligaciones pertinentes, las normas y las directrices. El gerente de TI supervisa la conformidad y el cumplimiento de las obligaciones de TI a través de prácticas adecuadas de auditoría.

El nivel al que desea llegar la organización es que esta cuente con políticas y prácticas claras, las cuales se encuentren documentadas y detallen los requerimientos legales de TI que rigen a la Organización. El gerente de TI supervisará periódicamente que se cumplen dichas prácticas y políticas expresadas por la organización. El gerente de TI supervisará periódicamente que se cumpla con las obligaciones internas y externas en el uso de la tecnología de la información, los resultados de estas supervisiones se encontrarán documentadas y son analizadas periódicamente en busca de la mejora continua. El gerente de TI supervisará la conformidad y el cumplimiento a través de prácticas de auditoría, dichas auditorias se encontrarán debidamente programadas, serán oportunas, exhaustivas y adecuadas y evaluarán el grado de satisfacción de las tecnologías de la información con los objetivos, políticas y/o directrices de la organización. Las auditorias incluirán la supervisión de los activos de TI y los datos (información) de la organización. También se incluirá la verificación del cumplimiento de todas las obligaciones legales pertinentes y las suscritas con clientes y proveedores.

La Tabla 7 muestra los resultados para el sexto principio de la ISO/IEC 38500 y se muestra a continuación:

Tabla 7. Resultados obtenidos de encuesta de niveles de madurez del gobierno TI para el principio 6 de la norma ISO/IEC 38500.

Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
6. Comportamiento Humano	Evaluar	3	5	3	5	0	4	2	5	1	4	**1.8**	**4.6**
	Dirigir	1	5	4	5	1	4	1	5	1	4	**1.6**	**4.6**
	Supervisar	1	5	2	5	0	5	1	5	0	4	**0.8**	**4.8**

Fuente: adaptado de Correa, M., & Parra B. (2012).

La Figura 27 es la representación gráfica de los resultados obtenidos para el sexto principio de la ISO/IEC 38500 y se muestra a continuación:

Nivel de madurez de Gobierno de TI Principio 6. Comportamiento Humano			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	1.8	4.6	5
Dirigir	1.6	4.6	5
Supervisar	0.8	4.8	5

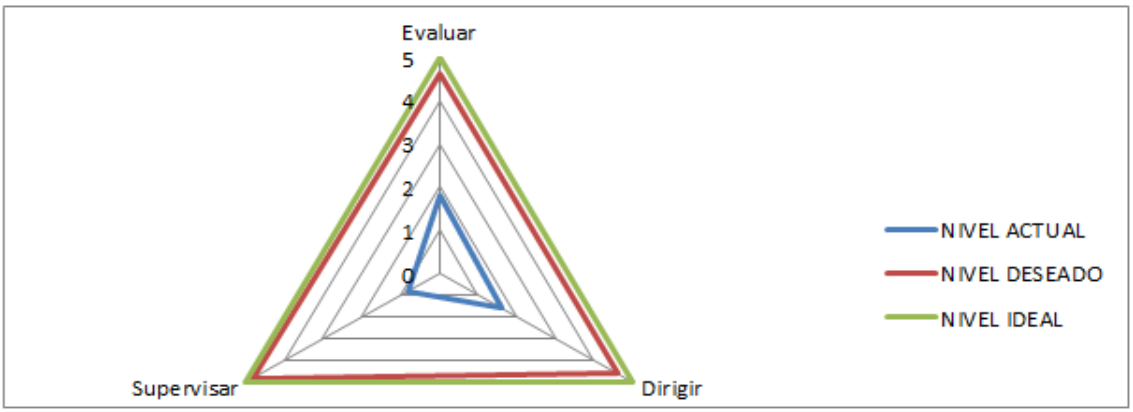


Figura 27. Resultados de nivel de madurez de gobierno TI. Principio 6
Fuente: adaptado de Correa, M., & Parra B. (2012).

Los resultados obtenidos para el Principio 6 indican que los usuarios de la organización tienen un conocimiento básico de las tecnologías que tienen disponibles. El gerente de TI ayuda a que los usuarios entiendan y aprovechen la tecnología que tienen disponible, de modo que estos aumenten su desempeño personal y el de los sistemas de información. El gerente de TI dirige de tal manera que las actividades de TI sean consistentes con el comportamiento humano identificado. El gerente de TI cuenta con mecanismos que permiten que cualquier persona en cualquier momento pueda identificar y reportar riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información.

El nivel al que desea llegar la empresa es que la organización conocerá acerca del comportamiento humano y sabe que esto incluye: cultura, necesidades, y aspiraciones de los usuarios, bien sea como individuos o como grupos. Además, el gerente de TI es consciente (y lo documentará como un riesgo) que estos comportamientos humanos pueden afectar el rendimiento las tecnologías de la información. Las políticas, prácticas y decisiones con respecto a TI demostrarán respeto por el comportamiento humano. La organización contará con políticas y/o procedimientos que permitan escalar los riegos reportados hasta las personas correspondientes a cargo de la toma de decisiones, todos los reportes acerca de los riesgos, oportunidades, problemas y preocupaciones

relacionados con las tecnologías de la información, se encontrarán debidamente documentados. El gerente de TI analizará periódicamente todos los reportes generados en busca de mejoras para la organización, esta supervisará periódicamente el nivel de satisfacción del comportamiento humano. (Por medio de encuestas de clima laboral, por ejemplo). La organización analizará los resultados de la supervisión de los comportamientos humanos y brindará la atención adecuada que se requiera para mejorar nivel de satisfacción. El gerente de TI supervisará periódicamente cómo los comportamientos humanos afectan el rendimiento de las tecnologías de la información. La organización supervisará periódicamente que las políticas, prácticas y decisiones de TI demuestren respeto por el comportamiento humano. El gerente de TI supervisará las prácticas laborales de los usuarios, con el fin de asegurar que sean consistentes del uso adecuado de la tecnología de información.

Se realizó un promedio de las tareas en cada principio de la norma ISO/IEC 38500, tanto para nivel actual como para nivel deseado. El resultado global del nivel de madurez del gobierno TI en la organización lo tenemos en la Figura 28:

Nivel de madurez de Gobierno de TI			
Principios	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
1. Responsabilidad	2.533333333	4.533333333	5
2. Estrategia	1.533333333	4.4	5
3. Adquisición	1.666666667	4.6	5
4. Dsempeño	1.266666667	4.4	5
5. Conformidad	1.266666667	4.4	5
6. Comportamiento Humano	1.4	4.666666667	5

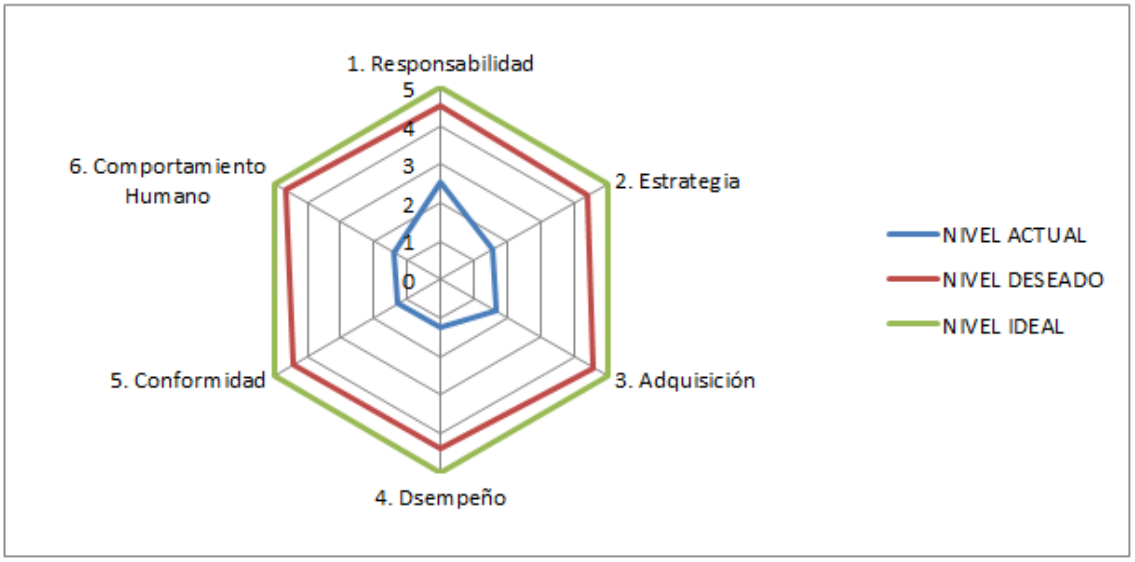


Figura 28. Resultados de nivel de madurez global de gobierno TI
Fuente: adaptado de Correa, M., & Parra B. (2012).

Luego que se obtuvo los resultados para Memorial International of Ecuador se procederá a realizar la definición del marco de gobierno TI en el siguiente apartado.

3.2. Definición del marco de gobernanza TI

Para el desarrollo del marco de gobierno para Memorial International of Ecuador se utilizará como referencia el apéndice E del marco COBIT 5, mismo que establece orientaciones de como los procesos de COBIT 5 posibilitan el desarrollo de los seis principios de la norma ISO/IEC 38500. Este análisis junto con el mapeo que realizó el ITGI (2008) entre COBIT y la ISO 27002 se lo actualizó a las normas y marcos vigentes, y se lo presentará en la figura 29.

Según ISACA (2012a) y su apéndice E, presenta un mapeo de COBIT 5 y la ISO/IEC 38500 para cada uno de sus principios:

- **PRINCIPIO 1 – Responsabilidad**:

  El negocio (el cliente) y las TI (proveedor) deberían colaborar en un modelo cooperativo utilizando canales eficaces de comunicación basados en relaciones positivas y de confianza y demostrando claridad con respecto a la responsabilidad de llevar a cabo las tareas y la verificación de las mismas. Se requiere canales simples de comunicación y tener un enfoque más directo a la hora de supervisar las actividades TI. Así mismo se requieren las estructuras apropiadas de gobierno organizativo, roles y responsabilidades para que todo se ordene desde la estructura de gobierno, proporcionando claridad en cuanto a la propiedad de los activos y la responsabilidad de las decisiones y tareas importantes.

  1. Las matrices RACI abogan fuertemente por la asignación de responsabilidades y proveen roles y responsabilidades.
  2. El proceso EDM05 explica el rol de los directivos en la supervisión y evaluación del gobierno de las TI y del desempeño en las TI con un método genérico para establecer metas y métricas relacionadas. (p.57)

  En el caso de la organización no se tomó en cuenta ningún otro proceso de la parte de Gobierno de COBIT 5 (EDM01, EDM02, EDM03, EDM04) para el principio 1 responsabilidad ya que no existe ningún marco de gobierno establecido por lo tanto no se puede asegurar la optimización de recursos, de riesgos, la entrega de beneficios, ni se puede realizar el mantenimiento del marco de gobierno. Lo que se tomó en cuenta para el desarrollo del marco de gobierno es el proceso EDM05

Asegurar la transparencia hacia las partes interesadas, ya que con este proceso se puede tener una evaluación, orientación y supervisión de los requisitos de elaboración de informes hacia las partes interesadas y conducir a la empresa hacia el nivel de madurez deseado.

- **PRINCIPIO 2 – Estrategia**:

  ISACA (2012a) indica: La planificación estratégica de la TI es una tarea compleja y crítica que requiere una estrecha coordinación entre la unidad de negocio de la empresa y los planes estratégicos de las TI. También es vital priorizar los planes que mejor se adecúan a la consecución de los beneficios deseados y a asignar eficazmente los recursos. Los logros de alto nivel tienen que ser traducidos a planes tácticos realizables, garantizando los mínimos fallos y sorpresas. La meta es conferir valor en el apoyo de los objetivos estratégicos a la vez que se tiene en cuenta el riesgo asociado en relación al umbral de riesgo del consejo. A continuación los procesos que sugiere ISACA:

  1. EDM02 indica cómo las metas corporativas deberían ser apoyadas por los casos de negocio apropiados.
  2. El dominio APO de COBIT 5 explica los procesos necesarios para la planificación y organización eficaces de los recursos TI internos y externos, incluyendo: planificación estratégica, planificación de la tecnología y la arquitectura, planificación organizativa, planificación de la innovación, gestión de la cartera, gestión de la inversión, gestión del riesgo, gestión de las relaciones y gestión de la calidad. (p.57)

  Una vez que se estableció los roles y responsabilidades, se tomó en cuenta en proceso de gobierno EDM02 Asegurar la entrega de beneficios, proceso que evalúa, orienta y supervisa la optimización de valor hacia la empresa. El valor para la empresa son los requerimientos de las partes interesadas, elementos clave de gobierno, efectividad de roles y responsabilidades, tipos de inversión y criterios, etc.

  Varios procesos para la parte de gestión de gobierno del dominio APO se tomaron en cuenta para la definición de este marco, mismos que harán alcanzar con sus prácticas y actividades el nivel de madurez deseado por la organización, como lo sugiere ISACA:

  - APO02 Gestionar la estrategia, tiene prácticas como el comprender la dirección de la empresa; Evaluar el entorno, capacidades y rendimiento

actuales; Definición del objetivo de las capacidades de las TI; Definir el plan estratégico y la hoja de ruta, etc.

- APO03 Gestionar la arquitectura empresarial tiene prácticas como: Definir la arquitectura de referencia, seleccionar las oportunidades y las soluciones, proveer los servicios de arquitectura empresarial, etc.
- APO04 Gestionar la Innovación con prácticas como: Crear un entorno favorable para la innovación; Supervisar y explorar el entorno tecnológico; Recomendar iniciativas apropiadas adicionales, etc.
- APO06 Gestionar el presupuesto y los costes con prácticas como: Gestionar las finanzas y contabilidad; Priorizar asignación de recursos; crear y mantener presupuestos; Gestionar costes; etc.
- APO08 Gestionar las relaciones con prácticas como: Entender las expectativas del negocio; Gestionar las relaciones con el negocio; Proveer datos de entrada para la mejora continua de los servicios, etc.
- APO11 Gestionar la calidad con prácticas como: Establecer un sistema de gestión de la calidad; Definir y gestionar estándares, procesos y prácticas de calidad; Enfocar la gestión de la calidad en los clientes, etc.
- APO12 Gestionar el Riesgo con prácticas como: Analizar el riesgo; Mantener un perfil de riesgo; Definir portafolio de acciones para la gestión de riesgos, etc.
- Para la definición de este marco también se consideró el proceso APO13 Gestionar la seguridad ya que sus prácticas: Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI); Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información y Supervisar y revisar el SGSI, llevan la esencia de lo que es la norma internacional ISO/IEC 27002, misma que se tratará en la definición de este marco de gobierno.

Para el segundo principio se deben aplicar controles de la ISO/IEC 27002 para diferentes prácticas de procesos COBIT 5, según Millet (2015) estos controles son:

- APO03.02. Definir la arquitectura de referencia: la arquitectura de referencia describe cómo está la empresa actualmente para la información, los datos, las aplicaciones, la tecnología y el negocio. (ISACA, 2012c). El uso de los controles mencionados a continuación ayudarán a mejorar las seguridades de esta práctica de COBIT 5:

- 8.1.1. Inventario de activos: ayuda a tener un control más exacto de los activos referentes a las TI. (ISO/IEC 27002, 2013)
- 8.1.3. Uso aceptable de los activos: con el control de activos se maneja apropiadamente los activos, así se tiene en las entregas, retiros, cambios, etc. (ISO/IEC 27002, 2013)
- 8.2.1. Directrices de clasificación: la información se debe clasificar de acuerdo a criterios como: valor, criticidad, requisitos legales, etc. (ISO/IEC 27002, 2013)
- 8.2.2. Etiquetado y Manipulación de la información: para tener un control efectivo de la información es necesario procedimientos de etiquetado de información según criterios de la empresa. (ISO/IEC 27002, 2013)
- 8.2.3. Manipulación de activos: el implementar procedimientos para manipular los activos se debe definir de acuerdo a las directrices de clasificación. (ISO/IEC 27002, 2013)

- APO12.01. Recopilar datos: el recopilar datos relevantes ayuda a realizar análisis de riesgos de las TI. (ISACA, 2012c). El control de esta práctica mejorarán la efectividad de los análisis para posibles riesgos y es:
  - 16.1.2. Notificación de los eventos de seguridad de la información: eventos que comprometan la seguridad de la información de deben comunicar y gestionar de manera adecuada. (ISO/IEC 27002, 2013)
- APO13.01. Establecer y mantener un SGSI: un Sistema de Gestión de Seguridad de la Información (SGSI) según la ISO/IEC (2016): un SGSI consiste en políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas colectivamente por una organización en la búsqueda de la protección de sus activos de información. (p. 16). Más detalle de lo que es un SGSI se lo revisará en la sección 3.2.2.9.
  - 5.1.1. Conjunto de políticas para la seguridad de la información: este control establece que las políticas de seguridad de la información deben ser definidas y comunicadas por la administración a todos los colaboradores tanto internos como externos. (ISO/IEC 27002, 2013)
  - 6.1.1. Roles y responsabilidades de seguridad de la información: para mejorar tener la seguridad de la información correcta es necesario un control que defina y asigne roles y responsabilidades. (ISO/IEC 27002, 2013)

- APO13.02. Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información: el tener un plan de tratamiento del riesgo debe describir cómo se gestiona y alinea los riesgos de la seguridad de la información con la estrategia y arquitectura empresarial. (ISACA, 2012c). Los controles para esta práctica son:
    - 7.2.2. Concienciación, educación y capacitación en seguridad de la información: es importante tener la capacitación adecuada a todos los colaboradores internos y externos sobre las políticas y procedimientos en la organización relevantes para sus funciones. (ISO/IEC 27002, 2013)
    - 12.1.2. Gestión de cambios: todo cambio que se tenga en la organización sean estos procesos de negocio, cambios en instalaciones donde se procese información, sistemas, etc. que afecten a la seguridad de la información deben ser controlados. (ISO/IEC 27002, 2013)
    - 16.1.5. Respuesta a los incidentes de seguridad: todo incidente de seguridad de la información se atenderá de acuerdo con los procedimientos establecidos y documentados. (ISO/IEC 27002, 2013)
- APO13.03. Supervisar y revisar el SGSI: el mejoramiento continuo del SGSI trae consigo beneficios, esto se debe comunicar y mantener. Es importante además mantener una cultura de seguridad y de mejora continua en los colaboradores. (ISACA, 2012c). Los controles de seguridad de la información para esta práctica son:
    - 5.1.2. Revisión de las políticas para la seguridad de la información: las políticas de seguridad de la información deben ser revisados a de forma planificada o si se produjeran cambios significativos. (ISO/IEC 27002, 2013)
    - 18.2.1. Revisión independiente de la seguridad de la información: para la revisión y supervisión del SGSI se debe revisar e forma independiente de forma planificada o cuando ocurre algún cambio significativo. (ISO/IEC 27002, 2013)

- **PRINCIPIO 3 – Adquisición**:

  ISACA (2012a) indica: las soluciones tecnológicas existen para soportar los procesos de negocio por lo que se debe tener cuidado de no considerar las

soluciones TI como algo aislado o solamente como un servicio o proyecto tecnológico. Por otra parte, una elección inadecuada de la arquitectura tecnológica, fallos a la hora de mantener una infraestructura técnica actual y apropiada o una ausencia de recursos humanos cualificados pueden dar como resultado un proyecto fracasado, una incapacidad para soportar las operaciones del negocio o una reducción en el valor del negocio. (p. 58)

La tecnología adquirida también debe soportar y operar con los procesos de negocio e infraestructuras TI existentes y planificados. En la siguiente lista se tienen los procesos que sugiere ISACA (2012a):

1. El proceso APO05 contempla cómo aplicar de manera eficaz la gestión del programa y la cartera de tales inversiones para asegurarse de que se logran los beneficios y de que se optimizan los costes.
2. El dominio APO provee orientaciones para la planificación de la adquisición, incluyendo: planes de inversión, gestión del riesgo, planificación de programas y proyectos y planificación de la calidad.
3. El dominio BAI da orientaciones sobre los procesos necesarios para adquirir e implementar soluciones TI, cubriendo la definición de requerimientos, identificando soluciones viables, preparando documentación y formando y habilitando a los usuarios y las operaciones para hacer funcionar los nuevos sistemas. Además, da orientaciones para asegurar que las soluciones son verificadas y controladas adecuadamente mientras el cambio se aplica al negocio funcional y al entorno tecnológico.
4. El dominio MEA y el proceso EDM05 de COBIT 5 incluyen orientaciones de cómo la dirección puede supervisar y evaluar el proceso de adquisición, y los controles internos para ayudar a garantizar que la adquisición se gestiona y ejecuta de manera adecuada. (p. 58)

Las consideraciones de ISACA para la definición de este principio ayudarán a la consecución del nivel de madurez deseado por la empresa. ISACA tomó en cuenta un proceso de Gobierno EDM05 Asegurar la Transparencia hacia las partes interesadas mismo que facilita la elaboración de informes así como su comprensión y asimilación por parte de quienes los reciben. Además para el desarrollo de este marco se consideró el proceso EDM04 Asegurar la optimización de recursos, este proceso asegura que las necesidades de recursos de la empresa son cubiertas de

un modo óptimo. También se complementan con procesos de otros dominios de COBIT 5 para llegar al nivel deseado.

ISACA (2012c) propone procesos del dominio APO como son:

- APO03 Gestionar la arquitectura empresarial, que representa 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. 63)
- APO05 Gestionar el portafolio, que optimiza el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas. (p. 73)
- APO06 Gestionar el presupuesto y los costes, que 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. (p. 79)
- APO11 Gestionar la calidad, que asegura la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfaga las necesidades de las partes interesadas. (p. 101)
- APO12 Gestionar el riesgo, que integra la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general y equilibra los costes y beneficios de gestionar riesgos empresariales relacionados con TI. (p. 107)

ISACA (2012c) también propone varios procesos del dominio BAI como son:

- BAI03 Gestionar la Identificación y construcción de soluciones, que establece soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales. (p. 133)
- BAI06 Gestionar los cambios, que posibilita una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio. (p. 149)
- BAI09 Gestionar los Activos, que contabiliza todos los activos de TI y optimiza del valor proporcionado por estos activos. (p. 163)

- BA10 Gestionar la configuración, que proporciona la suficiente información sobre los activos del servicio para que el servicio pueda gestionarse con eficacia, evalúa el impacto de los cambios y hacer frente a los incidentes del servicio. (p. 167)

Para el tercer principio se deben aplicar controles de la ISO/IEC 27002 (2013) que aseguren la efectividad y eficacia de seguridad de la información, según Millet (2015) estos controles son:

- APO03.02. Definir la arquitectura de referencia: como ya se revisó en el principio anterior se aplicarán los mismos controles.
- APO12.01. Recopilar datos: mismo control que el principio anterior.
- BAI03.01. Diseñar soluciones de alto nivel: se debe desarrollar y documentar diseños de alto nivel para que se pueda alinear con la estrategia de Ti y la arquitectura de la empresa. (ISACA, 2012c)
    - 14.2.1. Política de desarrollo seguro de software: se debe establecer y aplicar reglas para el desarrollo de software y sistemas. (ISO/IEC 27002, 2013)
- BAI03.02. Diseñar los componentes detallados de la solución: el diseño de los componentes deben documentarse, ser detallados progresivamente, asegurándose que incluyan ANSs y OLAs, tanto internos como externos.
    - 14.2.6. Seguridad en entornos de desarrollo: se debe establecer y proteger de manera adecuada a los entornos de desarrollo e integración de sistemas. (ISO/IEC 27002, 2013)
- BAI03.04. Obtener los componentes de la solución: se requiere que los componentes de la solución que estén basados en el plan de adquisiciones, principios de arquitectura y estándares, procedimientos contractuales generales, requerimientos de calidad, etc. (ISACA, 2012c). Los controles utilizados son:
    - 12.4.1. Registro y gestión de eventos de actividad: se debe registrar sucesos de actividades de usuarios, excepciones, errores y eventos se seguridad de la información que se producen, estos deben ser mantenidos y revisados con regularidad. (ISO/IEC 27002, 2013)
    - 14.2.1. Política de desarrollo seguro de software: control revisado en BAI03.01
    - 14.2.6. Seguridad en entornos de desarrollo: control revisado en BAI03.02

- BAI03.06. Realizar controles de calidad: es importante desarrollar un plan de calidad (QA) para obtener calidad específica de acuerdo a políticas y procedimientos de calidad de la empresa. (ISACA, 2012c)
    - 14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas: la información que requiera servicios de aplicaciones que pasan a través de redes públicas debe protegerse de la actividad fraudulenta, disputa contractual y la divulgación no autorizada y modificación. (ISO/IEC 27002, 2013)
    - 14.1.3. Protección de las transacciones por redes telemáticas: la Información involucrada en las transacciones de servicios de aplicaciones debe ser protegido para evitar la transmisión incompleta, mal enrutamiento, alteración mensaje no autorizado, la divulgación no autorizada, la duplicación no autorizada o bien la repetición de mensajes. (ISO/IEC 27002, 2013)
- BAI03.08. Ejecutar pruebas de la solución: se debe contar con un plan de pruebas y ejecutarlas continuamente durante el desarrollo. (ISACA, 2012c). Los controles de esta práctica a continuación:
    - 14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas: deben cumplir la funcionalidad de la seguridad del sistema desarrollado. (ISO/IEC 27002, 2013)
    - 14.2.9. Pruebas de aceptación: debe también existir programas de pruebas de aceptación de los sistemas desarrollados, actualizaciones o nuevas versiones. (ISO/IEC 27002, 2013)
- BAI03.09. Gestionar cambios a los requerimientos: se debe hacer un seguimiento del estado de requerimientos individuales en todo el ciclo de vida del proyecto gestionando la aprobación de cambios a los requerimientos. (ISACA, 2012c). Los controles a utilizar son:
    - 14.2.2. Procedimientos de control de cambios en los sistemas: todo cambio debe ser controlado por procedimientos formales de control de cambios dentro del ciclo de desarrollo. (ISO/IEC 27002, 2013)
- BAI03.10. Mantener soluciones: es importante desarrollar y ejecutar un plan que asegure el mantenimiento de la solución así como de los componentes de la infraestructura. (ISACA, 2012c). El control utilizado es:
    - 12.6.1. Gestión de las vulnerabilidades técnicas: el control sobre vulnerabilidades técnicas de los sistemas de información debe

mantenerse actualizado, teniendo las medidas frente a riesgos asociados. (ISO/IEC 27002, 2013)

- BAI06.01. Evaluar, priorizar y autorizar peticiones de cambio: se debe evaluar todas las peticiones de cambio y determinar su impacto. (ISACA, 2012c). Los controles utilizados para esta práctica son:
    - 12.1.2. Gestión de cambios: Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados (ISO/IEC 27002, 2013)
    - 14.2.2. Procedimientos de control de cambios en los sistemas. Control ya revisado en BAI03.09.
    - 14.2.4. Restricciones a los cambios en los paquetes de software: cualquier modificación a paquetes de software debe desalentarse, las modificaciones necesarias y todos los cambios deben controlarse estrictamente. (ISO/IEC 27002, 2013)
- BAI09.01. Identificar y registrar activos: se debe mantener un registro actualizado y exacto de todos los activos necesarios para la prestación de servicios, garantizando alineación con la gestión de la configuración y la administración financiera. (ISACA, 2012c). Los controles utilizados para esta práctica son:
    - 8.1.1. Inventario de activos: los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos activos se debe elaborar y mantener. (ISO/IEC 27002, 2013)
    - 8.1.2. Propiedad de los activos: los activos identificados en el inventario deben tener propiedad. (ISO/IEC 27002, 2013)
- BAI09.03. Gestionar el ciclo de vida de los activos: se debe gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente. (ISACA, 2012c). Los controles utilizados para esta práctica son:
    - 8.1.3. Uso aceptable de los activos. control revisado en APO03.02.
    - 8.1.4. Devolución de activos: Todos los empleados y contratistas deben devolver todos los activos de la organización en su posesión a la terminación de su empleo, contrato o acuerdo. (ISO/IEC 27002, 2013)
    - 8.2.2. Etiquetado y manipulado de la información: control revisado en APO03.02

- 8.3.2. Eliminación de soportes: se debe eliminar de forma segura los medios o dispositivos donde se almacene o procese información confidencial, cuando sea necesario utilizando procedimientos formales.. (ISO/IEC 27002, 2013)
- 11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento: todos los elementos del equipo que contiene los medios de almacenamiento deben ser verificados para asegurar que los datos sensibles y software con licencia han sido eliminados o sobrescritos de forma segura antes de su eliminación o reutilización. (ISO/IEC 27002, 2013)

- BAI09.05. Administrar licencias. (ISACA, 2012c)
  - 18.1.2. Derechos de propiedad intelectual: procedimientos apropiados deben ser implementados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario. (ISO/IEC 27002, 2013)

- **PRINCIPIO 4 – Desempeño**:

  Según ISACA (2012a): la medición eficaz del desempeño depende de que se tengan en cuenta dos aspectos clave: una definición clara de las metas de rendimiento y el establecimiento de métricas eficaces para supervisar el logro de las metas. También se requiere un proceso de medición del desempeño para cerciorarse de que dicho desempeño se supervisa de manera consistente y fiable. El gobierno efectivo se alcanza cuando las metas se establecen desde arriba hacia abajo y se alinean con las metas de negocio de alto nivel aprobadas y cuando las métricas se establecen de abajo a arriba y se alinean de manera que permiten que el logro de las metas a todos los niveles pueda ser supervisadas por los niveles de gestión correspondientes. Las TI son un tema técnico y complejo; por eso, es importante lograr transparencia a base de comunicar metas, métricas e informes del desempeño en un lenguaje totalmente comprensible para las partes interesadas de manera que se puedan tomar las acciones apropiadas. (p. 58)

  Los procesos que sugiere ISACA (2012a) son:

  1. El proceso APO02 se centra en el establecimiento de metas.
  2. El proceso APO09 se centra en la definición de servicios y de metas de servicio apropiadas y las documenta en acuerdos de nivel de servicio (SLA).

3. El proceso MEA01 proporciona orientación acerca de las responsabilidades de la gestión ejecutiva para esta actividad. (p.p. 58, 59)

La sugerencia de ISACA (2012c) de tres procesos para la definición del principio 4 y consecución del nivel de madurez deseado son:

- APO02 Gestionar la estrategia, que comunica 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. (p. 57)
- APO09 Gestionar los acuerdos de servicio, que asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa. (p. 93)
- MEA01 Supervisar, Evaluar y Valorar el rendimiento y la conformidad, que proporciona la transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos. (p. 203)

Estos procesos de COBIT 5 junto con sus prácticas y actividades facilitarán que la empresa llegue al nivel deseado de madurez para el gobierno de las TI.

- **PRINCIPIO 5 – Conformidad**:
  ISACA (2012a) indica: en el mercado global de hoy en día, apoyado por Internet y las tecnologías avanzadas, las empresas necesitan cumplir con un número cada vez más grande de requisitos legales y regulatorios. Las partes interesadas exigen mayores garantías de que las empresas cumplen con las leyes y reglamentos y de que se adecúan a las buenas prácticas de gobierno corporativo en su entorno operativo. Además, como las TI han facilitado procesos de negocio cada vez más fluidos entre empresas, hay también una necesidad creciente de cerciorarse de que los contratos incluyen requisitos importantes relativos a las TI en áreas tales como privacidad, confidencialidad, propiedad intelectual y seguridad. La alta gestión debe encontrar el equilibrio apropiado entre desempeño y conformidad, asegurándose de que las metas de desempeño no pongan en peligro la conformidad y, viceversa, que el régimen de conformidad sea apropiado y no penalice en exceso la operativa del negocio. (p.59)

  Los procesos que sugiere ISACA (2012a) para este principio son:

1. El proceso APO02 asegura de que hay un alineamiento entre los planes TI y los objetivos globales de negocio, incluyendo los requisitos de gobierno.
2. El proceso MEA02 facilita a los directivos cómo valorar si los controles son adecuados para satisfacer los requisitos de conformidad.
3. El proceso MEA03 garantiza que se identifican los requisitos de conformidad externos, que los directivos marcan la dirección para la conformidad, y que se supervisa, evalúa y se hacen informes de la conformidad TI en sí misma como una parte de la conformidad global con los requisitos de la empresa. (p. 59)

ISACA (2012c) también sugiere tres procesos para el desarrollo de este principio mismos que ayudarán a que la empresa llegue al nivel deseado de madurez del marco de gobierno de las TI:

- APO02 Gestionar la estrategia, que alinea los planes estratégicos de TI con los objetivos del negocio. (p. 57)
- MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno, que ofrece la 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. (p. 207)
- MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos que asegura que la empresa cumple con todos los requisitos externos que le sean aplicables. (p. 2013)

Para el principio quinto se deben aplicar controles de la ISO/IEC 27002 (2013) que aseguren la efectividad y eficacia de seguridad de la información, según Millet (2015) estos controles son:

- MEA02.01. Supervisar el control interno: se debe realizar de forma continua, la supervisión, estudios comparativos y la mejora en el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos. (ISACA, 2012c). El control para la ISO/IEC27002 seleccionado es:
    - 18.2.2. Cumplimiento de las políticas y normas de seguridad: los gerentes deben comprobar periódicamente el cumplimiento del tratamiento y los procedimientos de información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad. (ISO/IEC 27002, 2013)

- MEA02.02. Revisar la efectividad de los controles sobre los procesos de negocio: revisar la operación de controles para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. (ISACA, 2012c). El control para la ISO/IEC27002 seleccionado es:
    - 18.2.1. Revisión independiente de la seguridad de la información: control revisado en APO13.03
- 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. (ISACA, 2012c). El control para la ISO/IEC27002 seleccionado es:
    - 18.2.3. Comprobación del cumplimiento técnico: Los sistemas de información deben ser revisados regularmente por el cumplimiento de las políticas y estándares de seguridad de la información de la organización. (ISO/IEC 27002, 2013)
- 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. (ISACA, 2012c). El control para la ISO/IEC27002 seleccionado es:
    - 18.2.1. Revisión independiente de la seguridad de la información: control revisado en APO13.03
- 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. (ISACA, 2012c). El control para la ISO/IEC27002 seleccionado es:
    - 18.1.1. Identificación de la legislación aplicable: todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. (ISO/IEC 27002, 2013)
- 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. (ISACA, 2012c). Los controles para la ISO/IEC27002 seleccionados son:

- 18.1.2. Derechos de propiedad intelectual (DPI): control revisado en BAI09.05
- 18.1.3. Protección de los registros de la organización: los registros deben ser protegidos de la pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, de conformidad con los requisitos legislativos reglamentarios, contractuales y comerciales. (ISO/IEC 27002, 2013)

- MEA03.03. Confirmar el cumplimiento de requisitos externos: confirmar el cumplimiento de las políticas, principios, estándares, procedimientos y metodologías con requisitos legales, regulatorios y contractuales. (ISACA, 2012c). Los controles para la ISO/IEC27002 seleccionados son:
  - 18.1.4. Protección de datos y privacidad de la información personal: la privacidad y protección de la información de identificación personal que deben garantizarse como se requiere en la legislación y regulación relevante en su caso. (ISO/IEC 27002, 2013)
  - 18.1.5. Regulación de los controles criptográficos: los controles criptográficos deben ser utilizados en el cumplimiento de todos los acuerdos pertinentes, leyes y reglamentos. (ISO/IEC 27002, 2013)
- MEA03.04. Obtener garantía de cumplimiento de requisitos externos. (ISACA, 2012c). Los controles para la ISO/IEC27002 seleccionados son:
  - 18.1.4. Protección de datos y privacidad de la información personal: control revisado en MEA03.03
  - 18.1.5. Regulación de los controles criptográficos: control revisado en MEA03.03

- **PRINCIPIO 6 – Conducta Humana**:

  Según ISACA (2012a): la implementación de cualquier cambio facilitado por las TI, incluyendo el gobierno de las TI en sí mismo, requiere cambios significativos culturales y de comportamiento tanto dentro de las empresas como con los clientes y con los socios del negocio. La formación y la mejora de las competencias del personal son aspectos clave del cambio especialmente dada la naturaleza rápidamente cambiante de la tecnología. Mientras que los procesos de negocio posibilitados por las TI procuran nuevos beneficios y oportunidades, también conllevan un incremento de los tipos de riesgos. Asuntos tales como privacidad y

fraude son preocupaciones crecientes para los individuos, estos y otros tipos de riesgos tienen que ser gestionados si se quiere que la gente confíe en los sistemas TI que utilizan. (p. 59)

Los cuatro procesos de COBIT 5 que siguiere ISACA (2012a) son:

1. El proceso APO07 explica cómo se debería alinear el desempeño de los individuos con las metas corporativas, cómo se deberían actualizar las competencias de los especialistas en TI y cómo se deberían definir los roles y las responsabilidades.
2. El proceso BAI02 ayuda a asegurar que el diseño de aplicaciones satisface los requisitos de utilización y operación humanos.
3. Los procesos de COBIT 5 BAI05 y BAI08 ayudan a asegurar que los usuarios están capacitados para utilizar los sistemas de manera efectiva. (p. 60)

Finalmente para el principio 6 ISACA (2012c) sugiere cuatro procesos:

- APO07 Gestionar los recursos humanos, que proporciona 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. (p. 83)
- BAI02 Gestionar la definición de requisitos, que identifica soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas, todas estas definiciones se enfocan en la utilización y operación de la parte humana. (p. 129)
- BAI05 Gestionar la facilitación del cambio, que prepara y compromete a los interesados para el cambio de negocio y reducir el riesgo de fracaso. (p. 145)
- BAI08 Gestionar el conocimiento, que proporciona el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad. Estos procesos guiarán a la empresa a alcanzar el nivel deseado de madurez para el marco de gobierno de las TI. (p. 159)

Estos procesos, sub procesos, actividades y prácticas harán que la empresa llegue al nivel deseado de madurez para el marco de gobierno.

Para el sexto principio se deben aplicar controles de la ISO/IEC 27002 (2013) que aseguren la efectividad y eficacia de seguridad de la información, según Millet (2015) estos controles son:

- 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. (ISACA, 2012c). Los controles para la ISO/IEC27002 seleccionados son:
    - 7.1.1. Investigación de antecedentes: los controles de verificación de fondo sobre todos los candidatos para el empleo deben llevarse a cabo de acuerdo con las leyes, regulaciones y ética pertinente y debe ser proporcional a los requerimientos del negocio, la clasificación de la información para acceder y los riesgos percibidos. (ISO/IEC 27002, 2013)
    - 7.1.2. Términos y condiciones de contratación: los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y de la organización para la seguridad de la información. (ISO/IEC 27002, 2013)
- 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.. (ISACA, 2012c). Los controles para la ISO/IEC27002 seleccionados son:
    - 7.3.1. Cese o cambio de puesto de trabajo: las responsabilidades de la seguridad de la información y de los derechos que permanecen válidos después de la terminación o cambio de trabajo deberían ser definidos, comunicando al trabajador y al empresario. (ISO/IEC 27002, 2013)
    - 8.1.4. Devolución de activos: control revisado en BAI09.03
- APO07.04. Evaluar el desempeño laboral de los empleados: llevar 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. (ISACA, 2012c). Los controles para la ISO/IEC27002 seleccionados son:

- 7.2.3. Proceso disciplinario: Debe haber un proceso disciplinario formal y comunicado en su sitio para tomar medidas contra los empleados que han cometido una violación de la seguridad de la información. (ISO/IEC 27002, 2013)
- 8.1.3. Uso aceptable de los activos. control revisado en APO03.02

- BAI08.02. Identificar y clasificar las fuentes de información: identificar oportunidades potenciales para que la TI sea catalizadora de la mejora del rendimiento empresarial. (ISACA, 2012c). El control para seleccionado es:
  - 6.1.4. Contacto con grupos de interés especial: los contactos adecuados con los grupos de intereses especiales u otros foros de seguridad especializada y las asociaciones profesionales deben mantenerse. (ISO/IEC 27002, 2013)

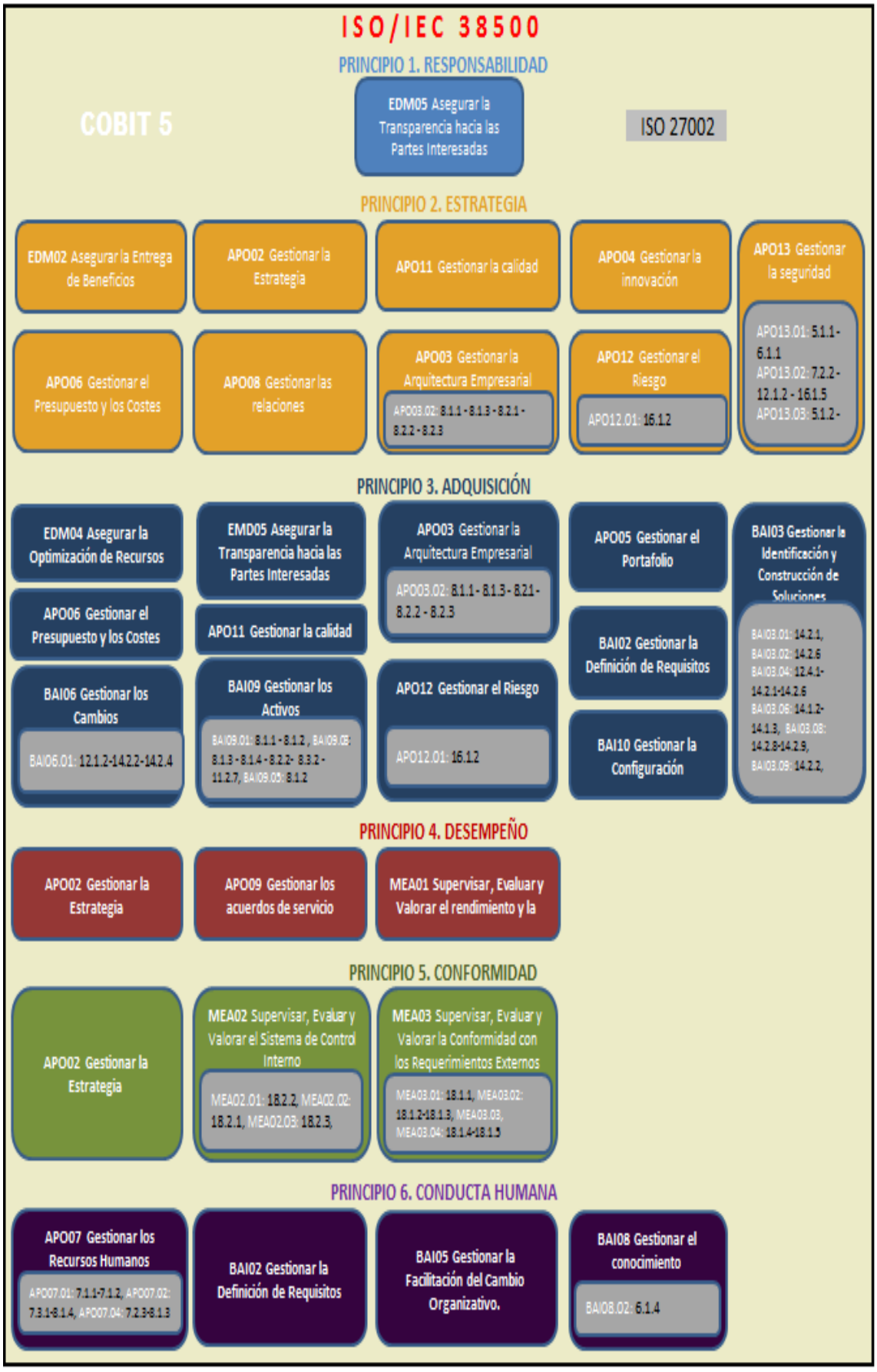


Figura 29. GEIT para Organización Memorial
Fuente: realizado por el autor

A continuación se va a desarrollar los seis principios de la norma ISO/IEC 38500:2015 con cada una de sus tres tareas.

3.2.1. PRINCIPIO 1 RESPONSABILIDAD:

La ISO/IEC (2015) expresa del principio 1 Responsabilidad: “Los individuos y grupos dentro de la organización entienden y aceptan sus responsabilidades en relación con la oferta y la demanda de TI. Los responsables de las acciones también tienen la autoridad para llevar a cabo esas acciones”. (p. 8)

Cada principio de la norma internacional ISO/IEC 38500 tiene tres tareas. Según la ISO/IEC (2015):

- **Evaluar: l**os órganos de gobierno deberían evaluar cuáles son las opciones existentes a la hora de asignar responsabilidades relacionadas con el uso actual y futuro de las TI en la organización. Los administradores deberían buscar el uso eficaz, eficiente y aceptable de la TI, en apoyo de los actuales y futuros objetivos de negocio. Los órganos de gobierno deberían evaluar la competencia de aquellos a quienes dieron la responsabilidad de tomar decisiones sobre la TI.

- **Dirigir: l**os órganos de gobierno deberían dirigir con el objetivo de que los planes se lleven a cabo de acuerdo con las responsabilidades asignadas a TI. Los órganos de gobierno deberían dirigir con el fin de recibir la información que necesitan para cumplir con sus responsabilidades y rendir cuentas.

- **Supervisar:** los órganos de gobierno deberían supervisar que se hayan establecido los mecanismos adecuados de gobernanza de la TI apropiados. Asimismo, deberían monitorizar que aquéllos a los que se les hayan asignado responsabilidades, las entienden y las asumen. (p. 11)

Para el desarrollo del principio 1 de la norma ISO/IEC 38500 se deberá hacerlo con los siguientes procesos de COBIT 5:

- Responsabilidades y matrices RACI para cada proceso de COBIT 5.
- EDM05. Asegurar la Transparencia hacia las Partes Interesadas

3.2.1.1. Responsabilidades y Matrices RACI

El principio 1 debe establecer las responsabilidades de individuos y grupos dentro de la organización en relación a la oferta y demanda de TI.

En la Figura 30 se describe los roles y su definición para individuos y grupos dentro de la organización en relación a la oferta y demanda de TI. Como en la estructura organizacional de TI de la organización no se cuenta con ciertos roles, se asignará roles para el desarrollo del proyecto:

Rol/Estructura	Definición/Descripción	Tipo de Rol
Director General Ejecutivo (CEO)	El ejecutivo de más alto rango a cargo de la gerencia total de la empresa, teniendo el control total de sus recursos.	Roles administrativos
STAFF	El grupo de los ejecutivos de mayor cargo y/o directores ejecutivos de la empresa que son responsables del gobierno de la empresa.	
Director Financiero	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión financiera, incluyendo el riesgo financiero y cuentas confiables y precisas.	
Director de Producción	El ejecutivo de mayor cargo responsable de todos los aspectos de la operación de la empresa.	
Director de Gestión	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión de la empresa.	
Gerente de Talento Humano	El ejecutivo de mayor cargo responsable de todos los aspectos de planificación y políticas relacionadas con todos los recursos humanos de la empresa.	
Gerente Legal	La función en la empresa responsable de dirigir el cumplimiento legal, regulatorio y contractual.	
Ejecutivo de Negocio	Un individuo de la gerencia responsable de la operación de una unidad de negocio específica o de una subsidiaria.	
Propietario del Proceso de Negocio	Un individuo responsable del rendimiento de un proceso en la realización de sus objetivos, realizando mejoras y aprobando cambios al proceso.	
Director de Informática / Sistemas (CIO)	El ejecutivo de mayor cargo responsable de alinear TI con las estrategias del negocio y que también es responsable de que se planifique, se consigan los recursos necesarios y se gestione la entrega de servicios y soluciones de TI para soportar los objetivos de la empresa.	Roles de TI
Jefe de Administración de TI (Asistente Sistemas)	Responsable de los registros relacionados con TI y responsable de soportar las cuestiones administrativas de TI.	
Jefe de Desarrollo (Adm. Base de datos)	Responsable del proceso de desarrollo de soluciones relacionadas con TI	
Gestor de Seguridad de la Información (Soporte Help Desk)	Un individuo que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de la empresa.	

Figura 30. Roles y estructuras organizativas para Memorial International of Ecuador
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012a).

En la Figura 31 se tiene las atribuciones, responsabilidades e interés de los resultados del programa de implementación del GEIT para partes interesadas internas:

Partes Interesadas Internas	Responsabilidades y atribuciones más importantes de alto nivel	Interés en los Resultados del Programa de implementación
Consejo y Gerencia	Establecer la dirección general, el contexto y los objetivos para el programa de mejora y asegurar su alineación con la estrategia, gobierno y gestión del riesgo de la empresa. Proporcionar apoyo y compromiso visible a las iniciativas, incluyendo los roles de promoción y patrocinio de las iniciativas. Aprobar los resultados del programa, y asegurar que los beneficios previstos son alcanzados y se toman medidas correctivas, según corresponda. Asegurarque los recursos necesarios (financieros, humanos y otros)están a disposición de la iniciativa. Establecer la dirección desde la parte superior y predicar con el ejemplo.	El consejo y la gerencia están interesados en obtener el máximo beneficio en el negocio de la implantación del programa. Quieren garantizar que todas las cuestiones relevantes requeridas se consideran, que las tareas requeridas se llevan acabo y que los resultados esperados se entregan correctamente.
Gerentes de negocio y responsables de procesos	Proporcionar recursos de negocio al grupo principal deimplementación. Trabajar conjuntamente con TI paraasegurar que los resultados del programa de mejora estánalineados y son apropiados para el entorno de negociode la empresa, que ese valor es tangible y que el riesgoes gestionado. Apoyar el programa de mejoras de una forma visible y trabajar con TI para resolver cualquier posible incidente. Asegurar que el negocio es considerado adecuadamente durante la implantación y la transición.	A estos grupos de interés le gustaría que el programaresultara en un mejor alineamiento de TI con el negocioen general y sus áreas especificas.
CIO	Proporcionar liderazgo al programa y los recursosde TI necesarios en la implantación. Trabajar con los gestores y ejecutivos del negocio para establecer los objetivos, la dirección y el enfoque adecuados para el programa.	El CIO quiere garantizar que todos los objetivos de implementación de GEIT son alcanzados. Para el CIO, el programa debería resultar un mecanismo que mejore continuamente la relación, el alineamiento, con el negocio (Incluyendo tener una visión compartida del desempeño de IT), conducir a una mejor gestión de las ofertas y demandas de TI y mejorar la gestión de TI relacionada con la gestión del riesgo del negocio.
Gerentes y Responsables de procesos TI	Dotar de liderazgo a los equipos del programa y recursos a los equipos de implementación. Dar información clave para la evaluación del desempeño y para establecer los objetivos de mejoras para los respectivos dominios. Proporcionar información sobre las buenas prácticas pertinentes que deben ser incorporados y proporcionar asesoramiento experto. Asegurar que el caso de negocio y el plan del programa son realistas y alcanzables.	Estos grupos están interesados en garantizar que las iniciativas de mejora resulten en un mejor gobierno de TI sobre todas y cada una de las áreas individuales, y que las opiniones sobre el negocio necesarias para ello son obtenidas de la mejor forma posible.
Empleados	Apoyar el GEIT	Estos grupos de interés están interesados en el/los impacto(s) que tendrán la iniciativa en su día a día en lo que a su trabajo, roles, responsabilidades y actividades se refiere.

Figura 31. Partes interesadas internas en el GEIT
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012b).

No solo las partes interesadas para la implementación del GEIT son internas, también existen partes externas interesadas en la implementación del GEIT, en la Figura 32 se describe estas partes y sus intereses:

Partes Interesadas Externas	Interés en los Resultados del Programa de implementación
Proveedores de servicios TI	La dirección de la empresa debería asegurar que existe una alineación e interfaz entre el GEIT global de la empresa y el gobierno y la gestión de los servicios que ellos prestan.
Reguladores	Los reguladores están interesados en si los resultados del programa de implementación satisfacen y/o proporcionan estructuras y mecanismos para satisfacer todas las regulaciones aplicables y cumplimientos normativos requeridos.
Accionistas	Los accionistas pueden basar en parte las decisiones de inversión en el estado del gobierno de su empresa y su trayectoria en ese ámbito.
Clientes	Los clientes podrían verse afectados por el grado en que se cumplen los objetivos de GEIT. Un ejemplo es la gestión del riesgo empresarial relacionado con TI. Si una empresa está expuesta en el ámbito de la seguridad, por ejemplo, a través de la pérdida de los datos bancarios del cliente, el cliente se verá afectado. El cliente tiene una participación indirecta en los resultados exitosos del programa de implantación.
Auditores Externos	Los auditores externos pueden poner más confianza en los controles relacionados con TI como resultado de un programa de implementación efectiva y estarán interesados en los aspectos de cumplimiento normativo y los informes financieros.
Socios de negocio	Los socios de negocios que utilizan las transacciones electrónicas automatizadas con la empresa podrían tener un interés en los resultados del programa de implantación con respecto a la mejora de la seguridad, integridad y oportunidad de la información. También podrían estar interesado en cumplimiento de las normas y certificaciones de estándares internacionales que podrían ser resultados del programa.

Figura 32. Partes interesadas en el GEIT externas
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012b).

Las matrices RACI se utilizan para establecer responsabilidades de las partes interesadas frente a procesos clave. Cada proceso de COBIT 5 cuenta con su matriz RACI, estás se irán presentando a medida que se continúa con el desarrollo del proyecto. El significado de RACI es:

- **R**esponsable: es la persona que desarrolla el trabajo. **Responsable.**
- **A**ccountable: es la persona responsable del resultado final. **Rinde cuentas.**
- **C**onsulted: cualquiera que deba ser contactado antes de que se tome una decisión. **Consultado.**
- **I**nformed: personas que deben mantenerse informado después que se ha tomado una decisión o una tarea ha sido completada. **Informado.**

3.2.1.2. EDM05. Asegurar la transparencia hacia las partes interesadas

Según ISACA (2012c) el proceso **EDM05 Asegurar la Transparencia hacia las Partes Interesadas** de COBIT 5: “Asegurar que la medición y 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”. (p. 47).

A continuación en la Figura 33 la matriz RACI para el proceso EDM05:

MATRIZ RACI EDM05													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas	R	A	C	C	C		C	C	I	R	I		
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes	R	A	C	C	C		C	C	I	R	I		
EDM05.03 Supervisar la comunicación con las partes interesadas	R	A	C	C	C		C	C	I	R	I		

Figura 33. Matriz RACI EDM05
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2. PRINCIPIO 2 ESTRATEGIA:

La ISO/IEC (2015) indica: “la estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de TI; los planes estratégicos de TI satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.” (p. 8)

Cada principio de la norma internacional ISO/IEC 38500 tiene tres tareas. Según la ISO/IEC (2015):

- **Evaluar**

  Los órganos de gobierno deberían evaluar la evolución de la TI y los procesos de negocio para asegurar que la TI proporcionará apoyo a las futuras necesidades de la organización, además evaluar el uso y las actividades de TI para asegurar que están alineadas con los objetivos de la organización y satisfacen las exigencias de las partes interesadas. También deben tener en cuenta las buenas prácticas y se asegurar que el uso de la TI está sujeto a una adecuada administración del riesgo.

- **Orientar**

  Los órganos de gobierno deberían dirigir la creación y uso de planes y políticas que aseguren que la organización se beneficia del desarrollo en la TI. También deberían alentar la presentación de propuestas de usos innovadores de la TI, que permitan a la organización responder a nuevas oportunidades o desafíos, mejorando los actuales procesos de negocio o emprendiendo otros nuevos.

- **Supervisar**

  Los órganos de gobierno deberían monitorizar el progreso de las propuestas de TI aprobadas, para asegurar que alcanzan los objetivos en los plazos establecidos, utilizando los recursos asignados. Los órganos de gobierno deberían monitorizar el uso de la TI para asegurar que se alcanzan los beneficios esperados. (p. 11)

El principio 2 debe establecer las capacidades actuales y futuras de las TI, asegurando la consecución de los beneficios deseados y asignación eficaz de los recursos.

Para desarrollar el principio 2 de la ISO/IEC 38500 se lo debe realizar con los siguientes procesos de COBIT 5:

- EDM02. Asegurar la entrega de beneficios.
- APO02. Gestionar la estrategia.
- APO03. Gestionar la arquitectura empresarial.
- APO04. Gestionar la innovación.
- APO06. Gestionar el presupuesto y los costes.
- APO08. Gestionar las relaciones.
- APO11. Gestionar la calidad.
- APO12. Gestionar el riesgo.

- APO13. Gestionar la seguridad.

3.2.2.1. EDM02. Asegurar la Entrega de Beneficios

Según ISACA (2012c) el proceso EDM02 Asegurar la Entrega de Beneficios de COBIT 5: “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”. (p. 35)

A continuación en la Figura 34 la matriz RACI para el proceso EDM02:

MATRIZ RACI EDM02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
EDM02.01 Evaluar la optimización del valor.	R	A	R	C	C	C	C	R		R		C	
EDM02.02 Orientar la optimización del valor.	R	A	R	C	C	I	I	R	I	R	I	I	I
EDM02.03 Supervisar la optimización del valor.	R	A	R	C	C	C	C	R		R		C	

Figura 34 Matriz RACI del proceso EDM02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2.2. APO02. Gestionar la Estrategia

Según ISACA (2012c) el proceso APO02 Gestionar la Estrategia de COBIT 5:

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 que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos. (p. 57)

A continuación en la Figura 35 la matriz RACI para el proceso APO02:

MATRIZ RACI APO02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO02.01 Comprender la dirección de la empresa.	C		C	C	C			A	C	R		R	R
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.	C		C	C	C		C	R	C	A	C	R	C
APO02.03 Definir el objetivo de las capacidades de TI.	A		C	C	C		C	C	I	R	C	C	C
APO02.04 Realizar un análisis de diferencias.						C	R	R	R	A	R	R	R
APO02.05 Definir el plan estratégico y la hoja de ruta.	C		I	C	C		C	C		A	C	C	C
APO02.06 Comunicar la estrategia y la dirección de TI.	R	I	I	I	I	I	I	R	I	R	I	I	I

Figura 35 Matriz RACI del proceso APO02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2.3. APO03. Gestionar la Arquitectura Empresarial:

Según ISACA (2012c) el proceso APO03 Gestionar la Arquitectura Empresarial de COBIT 5:

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. 63)

A continuación en la Figura 36 la matriz RACI para el proceso APO03:

MATRIZ RACI APO03													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO03.01 Desarrollar la visión de la arquitectura de la empresa.	A		C	C	C	C	C	R	C	R	C	C	C
APO03.02 Definir la arquitectura de referencia.	C		C	C	C	C	C	R	C	R	C	C	C
APO03.03 Seleccionar oportunidades y las soluciones.	A		C	C	C	C	C	R	C	R	C	C	C
APO03.04 Defnir la implantación de la arquitectura.	A		C	R	R	C	C	C	C	R	C	C	C
APO03.05 Proveer los servicios de arquitectura empresarial.	A		C	R	R	C	C	C	C	R	C	C	C

Figura 36 Matriz RACI del proceso APO03 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso APO03 se tiene controles de la ISO 27002 a continuación en la Figura 37:

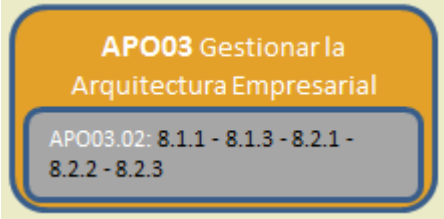


Figura 37 Proceso APO03 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para APO03 a continuación:

APO03.02 Definir la arquitectura de referencia, según la ISO 27002 (2013):

- **Inventario de activos**: "los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos activos se debe elaborar y mantener". (p. 16). Control 8.1.1.
- **Uso aceptable de los activos: "**Las reglas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de la información y la información deben ser identificados, documentados e implementados". (p. 17). Control 8.1.3.
- **Directrices de clasificación:** "La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada". (p. 18). Control 8.2.1.
- **Etiquetado y Manipulación de la información:** "Un conjunto apropiado de procedimientos para el etiquetado de información debe ser desarrollado e implementado de acuerdo con el esquema de clasificación de la información adoptado por la organización". (p. 18). Control 8.2.2.
- **Manipulación de activos:** Procedimientos para la manipulación de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la organización. Control 8.2.3. (p.19)

3.2.2.4. APO04. Gestionar la innovación:

Según ISACA (2012c) el proceso APO04. Gestionar la innovación de COBIT 5:

Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas al 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 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. (p.29)

A continuación en la Figura 38 la matriz RACI para el proceso APO04:

MATRIZ RACI APO04													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO04.01 Crear un entorno favorable para la innovación.	A					R		R	R	R		R	R
APO04.02 Mantener un entendimiento del entorno de la empresa.				A	A			R	R	R		R	
APO04.03 Supervisar y explorar el entorno tecnológico.										A		R	R
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	I			I	I			C	C	A		R	R
APO04.05 Recomendar iniciativas apropiadas adicionales.				I	I			R	R	R		R	R
APO04.06 Supervisar la implementación y el uso de la innovación.								C	C	R		C	C

Figura 38 Matriz RACI del proceso APO04 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2.5. APO06. Gestionar el presupuesto y los costes:

Según ISACA (2012c) el proceso APO06. Gestionar el presupuesto y los costes de COBIT 5:

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. (p. 79)

A continuación en la Figura 39 la matriz RACI para el proceso APO06:

MATRIZ RACI APO06													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO06.01 Gestionar las finanzas y la contabilidad.			A	C	C			C		C	R		
APO06.02 Priorizar la asignación de recursos.	I		R					C	C	A	R	C	C
APO06.03 Crear y mantener presupuestos.	I		A					C	C	R	R	C	C
APO06.04 Modelar y asignar costes.			C					C	C	A	R	C	C
APO06.05 Gestionar costes.			R					C	C	A	R	C	C

Figura 39 Matriz RACI del proceso APO06 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2.6. APO08. Gestionar las relaciones:

Según ISACA (2012c) el proceso APO08. Gestionar las relaciones de COBIT 5:

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. (p. 89)

A continuación en la Figura 40 la matriz RACI para el proceso APO08:

MATRIZ RACI APO08													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO08.01 Entender las expectativas del negocio.	C		C	C	C		C	C	R	A	C	R	R
APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	I			I	I		C	I	R	A		R	
APO08.03 Gestionar las relaciones con el negocio.	C		C	C	C			R	R	A		R	
APO08.04 Coordinar y comunicar.	R		I	R	R			R	R	A		R	
APO08.05 Proveer datos de entrada para la mejora continua de los servicios.	C			C	C		C	C	R	A		R	C

Figura 40 Matriz RACI del proceso APO08 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2.7. APO11. Gestionar la Calidad:

Según ISACA (2012c) el proceso APO11. Gestionar la calidad de COBIT 5:

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. (P. 101)

A continuación en la Figura 41 la matriz RACI para el proceso APO11:

MATRIZ RACI APO11													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO11.01 Establecer un sistema de gestión de la calidad (SGC).	C			A	A		C	C	I	R	R	C	I
APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	C						C	C	R	A	R	R	R
APO11.03 Enfocar la gestión de la calidad en los clientes.							C	A	R	R	I	I	I
APO11.04 Supervisar y hacer controles y revisiones de calidad.							C	C	R	A	C	C	C
APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.								C	C	A		R	
APO11.06 Mantener una mejora continua.							C	C	R	A	R	R	R

Figura 41 Matriz RACI del proceso APO11 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.2.8. APO12. Gestionar el Riesgo:

Según ISACA (2012c) el proceso APO12. Gestionar el riesgo de COBIT 5: “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”. (P. 107)

A continuación en la Figura 42 la matriz RACI para el proceso APO12:

MATRIZ RACI APO12													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO12.01 Recolectar data.	I						C		R	A	R	R	R
APO12.02 Analizar el riesgo.	I						R		R	A	C	C	C
APO12.03 Mantener un perfil de riesgo.	I						R		R	A	C	C	C
APO12.04 Expresar el riesgo.	I						C		R	A	C	C	C
APO12.05 Definir un portafolio de acciones para la gestión de riesgos.	I						C		R	R	C	C	C
APO12.06 Responder al riesgo.	I						C		R	R	R	R	R

Figura 42 Matriz RACI del proceso APO12 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso APO12 se tiene controles de la ISO 27002 a continuación en la Figura 43:

Figura 43 Proceso APO12 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para APO12 a continuación:

APO12.01 Recopilar datos, según la ISO 27002 (2013):

- **Informes eventos de seguridad de la información**: eventos de seguridad de la información deben comunicarse a través de canales de gestión adecuadas tan pronto como sea posible. Control 16.1.2. (p. 65)

3.2.2.9. APO13. Gestionar la seguridad:

Según ISACA (2012c) el proceso APO13: “Definir, operar y supervisar un sistema para la gestión de la seguridad de la información” (p. 113).

A continuación en la Figura 44 la matriz RACI para el proceso APO13:

MATRIZ RACI APO13													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO13.01 Establecer y mantener un SGSI.	C			C	C		C	C	I	R	R	I	R
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	C			C	C		C	C	C	R	R	C	R
APO13.03 Supervisar y revisar el SGSI.							C	C	R	R	R	R	R

Figura 44 Matriz RACI del proceso APO13 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Un Sistema de Gestión de Seguridad de la Información (SGSI) según la ISO/IEC(2016) es :

Un (SGSI) consiste en las políticas, procedimientos, directrices y recursos y actividades asociadas, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en una evaluación del riesgo y los niveles de aceptación del riesgo de la organización diseñada para tratar y gestionar los riesgos de manera efectiva. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI. (p. 16)

Según el análisis que se realizó en el apartado 3.2, para el proceso APO13 se tiene controles de la ISO 27002 a continuación en la Figura 45:

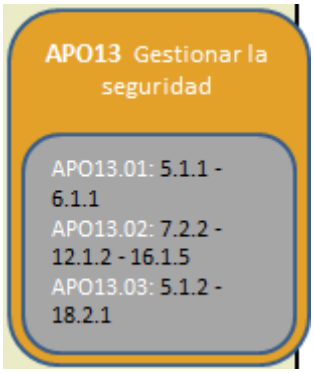


Figura 45 Proceso APO13 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para APO13 a continuación:

APO13.01 Establecer y mantener un SGSI, según la ISO (2013):

- **Conjunto de políticas para la seguridad de la información**: "Un conjunto de políticas de seguridad de la información deben ser definidas, aprobadas por la administración, publicadas y comunicadas a los empleados y colaboradores externos". Control 5.1.1. (p. 6)
- **Roles y responsabilidades de seguridad de la información**: "Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas". Control 6.1.1. (p. 7)

APO13.02 Establecer y mantener un SGSI, según la ISO (2013):

- **Información de concienciación sobre la seguridad, la educación y la formación**: "Todos los empleados de la organización y, en su caso, los contratistas deben recibir la educación adecuada sensibilidad y la formación y actualizaciones regulares en las políticas y procedimientos de la organización, como relevantes para su función de trabajo". Control 7.2.2. (p. 14)
- **Gestión de cambios**: "Los cambios en la organización, los procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados". Control 12.1.2 (p. 39)
- **Respuesta a los incidentes de seguridad**: "Los incidentes de seguridad de la información deben ser atendidos de acuerdo con los procedimientos documentados". Control 16.1.5 (p. 66)

APO13.03 Supervisar y revisar el SGSI, según la ISO (2013):

- **Revisión de las políticas para la seguridad de la información**: "Las políticas de seguridad de la información deben ser revisados a intervalos planificados o si se

produjeran cambios significativos para asegurar su conveniencia, adecuación y eficacia". Control 5.1.2. (p. 7)

- **Revisión independiente de la seguridad de la información**: "El enfoque de la organización para la gestión de seguridad de la información y su aplicación debe ser revisado de forma independiente a intervalos planificados o cuando se producen cambios significativos". Control 18.2.1. (p. 73)

3.2.3. PRINCIPIO 3 ADQUISICIÓN:

La ISO/IEC (2015) expresa: "Las adquisiciones de TI se hacen por razones válidas, basándose en un análisis apropiado y continuo, con las decisiones claras y transparentes. Hay un equilibrio apropiado entre los beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo". (p.8)

Cada principio de la norma internacional ISO/IEC 38500 tiene tres tareas. Según la ISO/IEC (2015):

- **Evaluar**: Los órganos de gobierno deberían evaluar cuáles son las opciones para proveerse de la TI que necesitan para desarrollar las propuestas aprobadas, equilibrando los riesgos y el valor económico de las inversiones propuestas.
- **Orientar**: Los órganos de gobierno deberían dirigir para que los activos de TI (sistemas e infraestructura) se adquieran de manera apropiada, incluyendo la elaboración de documentación adecuada, al tiempo que se asegura que se obtienen las capacidades requeridas. Los órganos de gobierno deberían dirigir para que los acuerdos de provisión soporten las necesidades de negocio de la organización.
- **Supervisar**: Los órganos de gobierno deberían monitorizar las inversiones en TI para asegurar que se provean las capacidades requeridas. Los órganos de gobierno deberían monitorizar hasta qué punto la organización y los proveedores mantienen y comparten el propósito de la organización al realizar una adquisición de TI. (p.p. 12,13)

El principio 3 debe establecer que las adquisiciones de TI se las realiza por razones válidas, con análisis apropiados y continuos, existiendo un equilibrio entre beneficios, oportunidades costes y riesgos.

Para desarrollar el principio 3 de la ISO/IEC 38500 se lo debe realizar con los siguientes procesos de COBIT 5:

- EDM04 Asegurar la optimización de recursos.
- EDM05 Asegurar la transparencia hacia las partes interesadas.

- APO03 Gestionar la arquitectura empresarial.
- APO05 Gestionar el portafolio.
- APO06 Gestionar el presupuesto y los costes.
- APO11 Gestionar la calidad.
- APO12 Gestionar el riesgo.
- BAI02 Gestionar la definición de requisitos.
- BAI03 Gestionar la identificación y construcción de soluciones.
- BAI06 Gestionar los cambios.
- BAI09 Gestionar los activos.
- BAI10 Gestionar la configuración.

3.2.3.1. EDM04 Asegurar la optimización de recursos:

Según ISACA (2012c): el proceso EDM04 Asegurar la optimización de recursos de COBIT 5: “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.” (p. 43)

A continuación en la Figura 46 la matriz RACI para el proceso EDM04:

MATRIZ RACI EDM04													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
EDM04.01 Evaluar la gestión de recursos.	R	A	C	C	C	C	C	R		R		C	
EDM04.02 Orientar la gestión de recursos.	R	A	C	C	C	I	I	R	I	R	I	I	I
EDM04.03 Supervisar la gestión de recursos.	R	A	C	C	C	C	C	R	I	R	I	C	I

Figura 46 Matriz RACI del proceso EDM04 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.2. EDM05 Asegurar la transparencia hacia las partes interesadas.

Según ISACA (2012c) el proceso EDM05 Asegurar la transparencia hacia las partes interesadas de COBIT 5: “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”. (p. 47)

A continuación en la Figura 47 la matriz RACI para el proceso EDM05:

MATRIZ RACI EDM05													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.	R	A	C	C	C		C	C	I	R	I		
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.	R	A	C	C	C		C	C	I	R	I		
EDM05.03 Supervisar la comunicación con las partes interesadas.	R	A	C	C	C		C	C	I	R	I		

Figura 47 Matriz RACI del proceso EDM05 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.3. APO03 Gestionar la arquitectura empresarial.

Según ISACA (2012c) el proceso APO03 Gestionar la Arquitectura Empresarial de COBIT 5:

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 arquitectura objeto. 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.63)

A continuación en la Figura 48 la matriz RACI para el proceso APO03:

MATRIZ RACI APO03													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO03.01 Desarrollar la visión de la arquitectura de la empresa.	A		C	C	C	C	C	R	C	R	C	C	C
APO03.02 Definir la arquitectura de referencia.	C		C	C	C	C	C	R	C	R	C	C	C
APO03.03 Seleccionar oportunidades y las soluciones.	A		C	C	C	C	C	R	C	R	C	C	C
APO03.04 Defnir la implantación de la arquitectura.	A		C	R	R	C	C	C	C	R	C	C	C
APO03.05 Proveer los servicios de arquitectura empresarial.	A		C	R	R	C	C	C	C	R	C	C	C

Figura 48 Matriz RACI del proceso APO03 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.4. APO05 Gestionar el portafolio.

Según ISACA (2012c) el proceso APO05 Gestionar el portafolio de COBIT 5:

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 fondo, basados en su alineamiento con los objetivos estratégicos así 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. (p.73)

A continuación en la Figura 49 la matriz RACI para el proceso APO05:

MATRIZ RACI APO05													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO05.01 Establecer la mezcla del objetivo de inversión.	R	A	R				C	C		C			
APO05.02 Determinar la disponibilidad y las fuentes de fondos.		C	A					R		R			
APO05.03 Evaluar y seleccionar los programas a financiar.	A	C	R					R		R			
APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	C	I	C	C	C		C	C	C	C			C
APO05.05 Mantener los portafolios.			I	R	R			R	R	R		C	C
APO05.06 Gestionar la consecución de beneficios.	C		C	A	A		C	A	A	R			C

Figura 49 Matriz RACI del proceso APO05 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.5. APO06 Gestionar el presupuesto y los costes.

Según ISACA (2012c) el proceso APO06 Gestionar el presupuesto y los costes de COBIT 5:

Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuestos, 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. Consulta 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. (p. 79)

A continuación en la Figura 50 la matriz RACI para el proceso APO06:

MATRIZ RACI APO06													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO06.01 Gestionar las finanzas y la contabilidad.			A	C	C			C		C	R		
APO06.02 Priorizar la asignación de recursos.	I		R					C	C	A	R	C	C
APO06.03 Crear y mantener presupuestos.	I		A					C	C	R	R	C	C
APO06.04 Modelar y asignar costes.			C					C	C	A	R	C	C
APO06.05 Gestionar costes.			R					C	C	A	R	C	C

Figura 50 Matriz RACI del proceso APO06 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.6. APO11 Gestionar la calidad.

Según ISACA (2012c) el proceso APO11 de COBIT 5: “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.” (p. 101)

A continuación en la Figura 51 la matriz RACI para el proceso APO11:

MATRIZ RACI APO11													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.								C	C	A		R	

Figura 51 Matriz RACI del proceso APO11 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.7. APO12 Gestionar el riesgo.

Según ISACA (2012c) el proceso APO12. Gestionar el riesgo de COBIT 5: “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”. (p. 107)

A continuación en la Figura 52 la matriz RACI para el proceso APO12:

MATRIZ RACI APO12													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO12.01 Recolectar datos	I						C		R	A	R	R	R

Figura 52 Matriz RACI del proceso APO12 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso APO12 se tiene controles de la ISO 27002 a continuación:

APO12.01 Recopilar datos, según la ISO 27002 (2013):

- **Informes eventos de seguridad de la información**: eventos de seguridad de la información deben comunicarse a través de canales de gestión adecuadas tan pronto como sea posible. Control 16.1.2. (p. 65)

3.2.3.8. BAI02 Gestionar la definición de requisitos.

Según ISACA (2012c) el proceso BAI02 de COBIT 5:

Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas. (p. 129)

A continuación en la Figura 53 la matriz RACI para el proceso BAI02:

MATRIZ RACI BAI02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.							C	I	R	C		R	C
BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.							C	R	R	C		R	C
BAI02.03 Gestionar los riesgos de los requerimientos.							C	R	R	R		R	C
BAI02.04 Obtener la aporbación de los requerimientos y soluciones.							C	R	R	C		C	C

Figura 53 Matriz RACI del proceso BAI02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.3.9. BAI03 Gestionar la identificación y construcción de soluciones.

Según ISACA (2012c) el proceso BAI03 de COBIT 5:

Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios. (p. 133)

A continuación en la Figura 54 la matriz RACI para el proceso BAI03:

MATRIZ RACI BAI03													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI03.01 Diseñar soluciones de alto nivel.							C		R	I		A	C
BAI03.02 Diseñar los componentes detallados de la solución.							C		R	I		A	C
BAI03.03 Desarrollar los componetes de la solución.							C		R	I		A	C
BAI03.04 Obtener los componetes de la solución.							C	I	R	A	R	R	C
BAI03.05 Construir soluciones.							C		R	I		A	C
BAI03.06 Realizar controles de calidad.							C	I	R	I		R	C
BAI03.07 Preparar pruebas de la solución.							C		R	I		R	R
BAI03.08 Ejecutar las pruebas de solución.							I		R	I		R	I
BAI03.09 Gestionar cambios a los requerimientos.							I	I	R	C		R	C
BAI03.10 Mantener soluciones.							C		R	I		A	C
BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.							I	I	I	R	C	C	I

Figura 54 Matriz RACI del proceso BAI03 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso BAI03 se tiene controles de la ISO 27002 a continuación en la Figura 55:

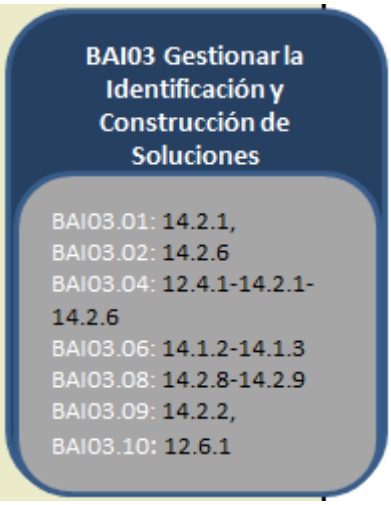


Figura 55 Proceso BAI03 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para BAI03 a continuación:

BAI03.01. Diseñar soluciones de alto nivel, según la ISO (2013):

- **Política de desarrollo seguro de software: "**Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a la evolución de la organización". (p. 55). Control 14.2.1.

BAI03.02. Diseñar los componentes detallados de la solución., según la ISO (2013):

- **Seguridad en entornos de desarrollo:** "Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguras para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema". (p. 58). Control 14.2.6

BAI03.04. Obtener los componentes de la solución, según la ISO (2013):

- **Registro y gestión de eventos de actividad:** "La grabación de registros de sucesos actividades del usuario, excepciones, errores y eventos de seguridad de información se deben producir, mantenidos y revisados con regularidad". (p. 58). Control 12.4.1.
- **Política de desarrollo seguro de software: "**Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a la evolución de la organización". (p. 55). Control 14.2.1.
- **Seguridad en entornos de desarrollo;** "Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguras para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema". (p. 58). Control 14.2.6

BAI03.06. Realizar controles de calidad, según la ISO (2013):

- **Seguridad de las comunicaciones en servicios accesibles por redes públicas: "**La información que requiera servicios de aplicaciones que pasan a través de redes públicas debe protegerse de la actividad fraudulenta, disputa contractual y la divulgación no autorizada y la modificación." (p. 53). Control 14.1.2
- **Protección de las transacciones por redes telemáticas**: "La Información involucrada en las transacciones de servicios de aplicaciones debe ser protegido para evitar la transmisión incompleta, mal enrutamiento, alteración mensaje no autorizado, la divulgación no autorizada, la duplicación no autorizada o bien la repetición de mensajes". (p. 53). Control 14.1.3.

BAI03.08. Ejecutar pruebas de la solución, según la ISO (2013):

- **Pruebas de funcionalidad durante el desarrollo de los sistemas:** “Pruebas de la funcionalidad de seguridad debe ser llevada a cabo durante el desarrollo.” (p. 59). Control 14.2.8.
- **Pruebas de aceptación**: Control 14.2.9.

BAI03.09. Gestionar cambios a los requerimientos, según la ISO (2013):

- **Procedimientos de control de cambios en los sistemas:** “Los programas de pruebas de aceptación y criterios relacionados deben ser establecidos para los nuevos sistemas de información, actualizaciones y nuevas versiones”. (p. 56). Control 14.2.2.

BAI03.10. Mantener soluciones, según la ISO (2013):

- **Gestión de las vulnerabilidades técnicas:** “La información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan deben obtenerse de manera oportuna, evaluarse la exposición de la organización a tales vulnerabilidades y tomarse medidas adecuadas para hacer frente a los riesgos asociados". (p. 46). Control 12.6.1.

3.2.3.10. BAI06 Gestionar los cambios.

Según ISACA (2012c) el proceso BAI06 de COBIT 5:

Gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación. (p. 148).

A continuación en la Figura 56 la matriz RACI para el proceso BAI06:

MATRIZ RACI BAI06													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.							C	A	R	R	C	R	C
BAI06.02 Gestionar cambios de emergencia.							C	A	I	R		R	C
BAI06.03 Hacer seguimiento e informar de cambios de estado.								C	R	A		R	
BAI06.04 Cerrar y documentar los cambios.							C	R	R	R	I	R	

Figura 56 Matriz RACI del proceso BAI06 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso BAI06 se tiene controles para la ISO 27002 a continuación en la Figura 57:

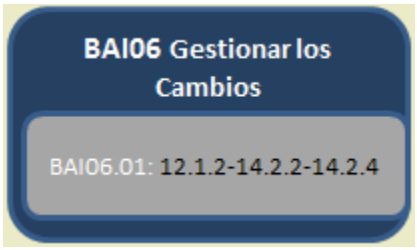


Figura 57 Proceso BAI06 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para BAI06 a continuación:

BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio, según la ISO (2013):

- **Gestión de cambios.**: "Los cambios en la organización, los procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados". Control 12.1.2 (p. 39)
- **Procedimientos de control de cambios en los sistemas**: "Los programas de pruebas de aceptación y criterios relacionados deben ser establecidos para los nuevos sistemas de información, actualizaciones y nuevas versiones". (p. 56). Control 14.2.2.

- **Restricciones a los cambios en los paquetes de software**: “Las modificaciones a los paquetes de software deben desalentarse, otros, las modificaciones necesarias y todos los cambios deben ser estrictamente controlados”. (p. 57). Control 14.2.4.

3.2.3.11. BAI09 Gestionar los activos.

Según ISACA (2012c) el proceso BAI09 Gestionar los activos de COBIT 5:

Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia. (p. 163).

A continuación en la Figura 58 la matriz RACI para el proceso BAI09:

MATRIZ RACI BAI09													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI09.01 Identificar y registrar activos actuales.							R	A	R	R	R	R	R
BAI09.02 Gestionar activos críticos						C	C	A	R	R		R	
BAI09.03 Gestionar el ciclo de vida de los activos.						C	I		C	A	R	R	
BAI09.04 Optimizar el coste de los activos.							R		A	R	R	C	C
BAI09.05 Administrar licencias.							C		A	R	R	C	R

Figura 58 Matriz RACI del proceso BAI09 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso BAI09 se tiene controles de la ISO 27002 a continuación en la Figura 59:

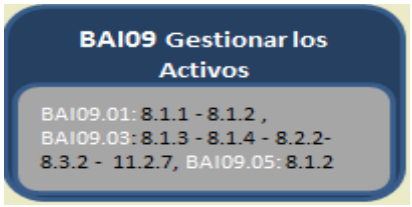


Figura 59 Proceso BAI09 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para BAI09 a continuación:

BAI09.01 Identificar y registrar activos, según la ISO (2013):

- **Inventario de activos**: "Los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos activos se debe elaborar y mantener". (p. 16). Control 8.1.1.
- **Propiedad de los activos:** "Los activos mantenidos en el inventario deben tener propiedad. " (p. 16). Control 8.1.2.

BAI09.03 Gestionar el ciclo de vida de los activos., según la ISO (2013):

- **Uso aceptable de los activos.**: "Las reglas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de la información y la información deben ser identificados, documentados e implementados". (p. 17). Control 8.1.3.
- **Devolución de activos**: "Todos los empleados y contratistas deben devolver todos los activos de la organización en su posesión a la terminación de su empleo, contrato o acuerdo". (p. 17). Control 8.1.4.
- **Etiquetado y manipulado de la información**: "Un conjunto apropiado de procedimientos para el etiquetado de información debe ser desarrollado e implementado de acuerdo con el esquema de clasificación de la información adoptado por la organización". (p. 18). Control 8.2.2.
- **Eliminación de soportes**: "Los medios de comunicación deberán eliminarse de forma segura cuando ya no sea necesario, utilizando procedimientos formales". (p. 19). Control 8.3.2.
- **Reutilización o retirada segura de dispositivos de almacenamiento**: "Todos los elementos del equipo que contiene los medios de almacenamiento deben ser verificados para asegurar que los datos sensibles y software con licencia ha sido eliminado o sobrescrito de forma segura antes de su eliminación o reutilización". (p. 37). Control 11.2.7.

BAI09.05 Administrar licencias, según la ISO (2013):

- **Derechos de propiedad intelectual (DPI):** “Los procedimientos apropiados deben ser implementados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario”. (p. 70). Control 18.1.2.

3.2.3.12. BAI10 Gestionar la configuración.

Según ISACA (2012c) el proceso BAI10 Gestionar la configuración de COBIT 5:

Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración. (p. 167)

A continuación en la Figura 60 la matriz RACI para el proceso BAI10:

MATRIZ RACI BAI10													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI10.01 Establecer y mantener un modelo de configuración.									C	C	R	I	
BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.											R	R	
BAI10.03 Mantener y controlar los elementos de configuración.										A	R	R	
BAI10.04 Generar informes de estado y configuración.									I	I	R	C	
BAI10.05 Verificar y revisar la integridad del repositorio de configuración.									I			R	

Figura 60 Matriz RACI del proceso BAI10 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.4. PRINCIPIO 4 DESEMPEÑO:

Según la ISO/IEC (2015): “La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras”. (p. 8)

Cada principio de la norma internacional ISO/IEC 38500 tiene tres tareas. Según la ISO/IEC (2015):

- **Evaluar:** los órganos de gobierno deberían evaluar los planes propuestos por la dirección para asegurar que la TI sustentará los procesos de negocio con las capacidades y aptitudes requeridas. Estas propuestas deberían incluir la continuidad de la operación normal de la organización y la gestión de los riesgos asociados al uso de la TI. Los órganos de gobierno deberían evaluar los riesgos para la continuidad del negocio derivados de las actividades de TI, deberían evaluar los riesgos para la integridad de la información y la protección de los activos de TI, incluyendo la propiedad intelectual y la memoria colectiva de la organización. Los órganos de gobierno deberían evaluar opciones para asegurar la eficaz y oportuna toma de decisiones relativas al uso de la TI para alcanzar los objetivos del negocio y evaluar periódicamente la eficacia y el desempeño del gobierno de la TI de la organización.
- **Orientar:** los órganos de gobierno deberían asegurar la asignación de recursos suficientes para que la TI satisfaga las necesidades de la organización, de acuerdo con las prioridades acordadas y las restricciones presupuestarias, además deberían dirigir a los responsables para asegurar que, cuando sea necesario por razones de negocio, la TI proporciona soporte al negocio con información actualizada, correcta y protegida ante pérdidas o usos inadecuados
- **Supervisar:** los órganos de gobierno deberían monitorizar el grado con el que la TI sustenta la organización. Los administradores deberían monitorizar el grado con el cual los recursos y presupuestos asignados son priorizados de acuerdo con los objetivos de negocio de la organización. Los órganos de gobierno deberían monitorizar cómo está de extendido el seguimiento de políticas tales como las de precisión de los datos y uso eficiente de la TI. (p.p. 12-13)

Para desarrollar el principio 4 de la ISO/IEC 38500 se lo debe desarrollar con los siguientes procesos de COBIT 5:

- APO02 Gestionar la Estrategia.
- APO09 Gestionar los acuerdos de servicio

- MEA01 Supervisar, Evaluar y Valorar el rendimiento y la conformidad.

3.2.4.1. APO02 Gestionar la Estrategia

Según ISACA (2012c) el proceso APO02 Gestionar la Estrategia de COBIT 5:

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 que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos. (p. 57)

A continuación en la Figura 61 la matriz RACI para el proceso APO02:

MATRIZ RACI APO02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO02.01 Comprender la dirección de la empresa.	C		C	C	C			A	C	R		R	R
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.	C		C	C	C		C	R	C	A	C	R	C
APO02.03 Definir el objetivo de las capacidades de TI.	A		C	C	C		C	C	I	R	C	C	C
APO02.04 Realizar un análisis de diferencias.						C	R	R	R	A	R	R	R
APO02.05 Definir el plan estratégico y la hoja de ruta.	C		I	C	C		C	C		A	C	C	C
APO02.06 Comunicar la estrategia y la dirección de TI.	R	I	I	I	I	I	I	R	I	R	I	I	I

Figura 61 Matriz RACI del proceso APO02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.4.2. APO09 Gestionar los acuerdos de servicio

Según ISACA (2012c) el proceso APO09 Gestionar el presupuesto y los costes de COBIT 5: “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”. (p. 93)

A continuación en la Figura 62 la matriz RACI para el proceso APO09:

MATRIZ RACI APO09													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO09.01 Identificar servicios TI.	C			R	R		I	R	R	R	C	C	I
APO09.02 Catalogar servicios basados en TI.							I	I	I	R	C	C	I
APO09.03 Definir y preparar acuerdos de servicio.							C	R	C	R	R	C	C
APO09.04 Supervisar e informar de los niveles de servicio.	I			I	I			I	R	I	I	I	
APO09.05 Revisar acuerdos de servicio y contratos.							C	A	C	R	R	C	C

Figura 62 Matriz RACI del proceso APO09 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.4.3. MEA01 Supervisar, Evaluar y Valorar el rendimiento y la conformidad.

Según ISACA (2012c) el proceso MEA01 de COBIT 5:

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. (p.203)

A continuación en la Figura 63 la matriz RACI para el proceso MEA01:

MATRIZ RACI MEA01													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
MEA01.01 Establecer un enfoque de la supervisión.	A		R	R	R	C	C	R	I	R	I	C	I
MEA01.02 Estabelcer los objetivos de cumplimiento y rendimiento.	I		I	I	I	C		A	R	C	I	R	I
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.						C		C	R	A	I	R	I
MEA01.04 Analizar e informar sobre el rendimiento.						C	C	A	R	C	C	R	C
MEA01.05 Asegurar la implantación de medidas correctivas.	I	I	I	I	I	C	C	C	R	A	C	R	C

Figura 63 Matriz RACI del proceso MEA01 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.5. PRINCIPIO 5 CONFORMIDAD:

Según la ISO/IEC (2015): “La función de TI cumple con todas las leyes y normas aplicables. Las políticas y prácticas están claramente definidas, implementadas y exigidas”. (p. 8)

Cada principio de la norma internacional ISO/IEC 38500 tiene tres tareas. Según la ISO/IEC (2015):

- **Evaluar:** los órganos de gobierno deberían evaluar periódicamente el grado con el que la TI cumplen con las obligaciones relevantes, políticas internas, normas y directrices profesionales, además evalúan periódicamente el cumplimiento interno de la organización con su sistema de gobernanza de la TI.
- **Orientar:** los órganos de gobierno deberían dirigir a los responsables para establecer mecanismos periódicos y rutinarios para asegurar que el uso de la TI cumple con las obligaciones relevantes, políticas internas, normas y directrices profesionales, además dirigen para que estén establecidas y se hagan cumplir las políticas que permitan a la organización satisfacer sus obligaciones internas en el uso de la TI. Los órganos de gobierno deberían dirigir para que el

personal de TI cumpla las directrices relevantes en materia de desarrollo y conducta profesional y dirigen para que la ética rija todas las acciones relacionadas con la TI.

- **Supervisar:** los órganos de gobierno deberían supervisar el cumplimiento y conformidad de la TI mediante prácticas adecuadas de auditoría y emisión de informes, asegurando que las revisiones sean oportunas, completas y adecuadas para la evaluación del grado de satisfacción de la organización. También deberían monitorizar las actividades de la TI, incluyendo la pérdida de información y de activos, para asegurar que se cumplen las obligaciones ambientales, de privacidad, de gestión del conocimiento estratégico, conservación de la memoria colectiva de la organización y otras obligaciones. (p.p. 14-15)

El principio 5 define claramente las políticas, prácticas, leyes, normas, y son implementadas y exigidas.

Para desarrollar el principio 5 de la ISO/IEC 38500 se lo debe desarrollar con los siguientes procesos de COBIT 5:

- APO02 Gestionar la Estrategia.
- MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.
- MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

3.2.5.1. APO02 Gestionar la estrategia

El concepto de APO02 se las desarrolló en el literal 3.2.4.1. Ya que APO02 está incluido en los principios Estrategia, Desempeño y Conformidad, en cada uno de ellos se interpreta de diferente manera.

A continuación en la Figura 64 la matriz RACI para el proceso APO02:

MATRIZ RACI APO02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO02.03 Definir el objetivo de las capacidades de TI.	A		C	C	C		C	C	I	R	C	C	C
APO02.05 Definir el plan estratégico y la hoja de ruta.	C		I	C	C		C	C		A	C	C	C
APO02.06 Comunicar la estrategia y la dirección de TI.	R	I	I	I	I	I	I	R	I	R	I	I	I

Figura 64 Matriz RACI del proceso APO02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.5.2. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno:

Según ISACA (2012c) el proceso MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno de COBIT 5:

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. (p. 207)

A continuación en la Figura 65 la matriz RACI para el proceso MEA02:

MATRIZ RACI MEA02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
MEA02.01 Supervisar el control interno.	I		C	I	I		R	C	R	A	R	R	R
MEA02.02 Revisar la efectividad de los controles sobre procesos de negocio.	I	I	R	I	I		R	A	R	C			C
MEA02.03 Realizar autoevaluaciones de control.	I		C	I	I		R	C	R	A	R	R	R
MEA02.04 Indentificar y comunicar las diferencias de control.	I		C	I	I		R	C	R	A	R	R	R
MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.							A		R	R			
MEA02.06 Planificar iniciativas de aseguramiento.	A						C	C	R	R	C	C	C
MEA02.07 Estudiar las iniciativas de aseguramiento.				R	R		C	R	R	R	C	C	C
MEA02.08 Ejecutar las iniciativas de aseguramiento.	I	I					C	C	R	R	C	C	C

Figura 65 Matriz RACI del proceso MEA02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso MEA02 se tiene controles de la ISO 27002 a continuación en la Figura 66:

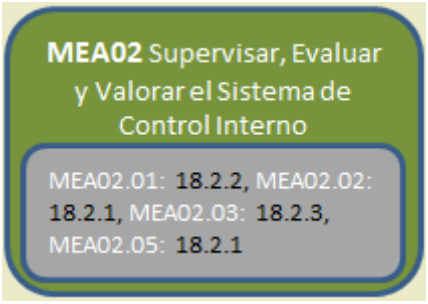


Figura 66 Proceso MEA02 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para MEA02 a continuación:

MEA02.01 Supervisar el control interno, según la ISO (2013):

- **Cumplimiento de las políticas y normas de seguridad**: “Los gerentes deben comprobar periódicamente el cumplimiento del tratamiento y los procedimientos de información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.” (p. 73) Control 18.2.2.

MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio, según la ISO (2013):

- **Revisión independiente de la seguridad de la información**: “El enfoque de la organización para la gestión de seguridad de la información y su aplicación debe ser revisado de forma independiente a intervalos planificados o cuando se producen cambios significativos” (p. 73) Control 18.2.1.

MEA02.03 Realizar autoevaluaciones de control, según la ISO (2013):

- **Comprobación del cumplimiento técnico**: “Los sistemas de información deben ser revisados regularmente por el cumplimiento de las políticas y estándares de seguridad de la información de la organización” (p. 22) Control 18.2.3.

MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados: se realizará con el Control 18.2.2 qué se revisó en MEA02.01

3.2.5.3. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

Según ISACA (2012c) el proceso MEA03 de COBIT 5:

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. (p. 213)

A continuación en la Figura 67 la matriz RACI para el proceso MEA03:

MATRIZ RACI MEA03													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
MEA03.01 Identificar requisitos externos de cumplimiento.							R	A	R	R			
MEA03.02 Optimizar la respuesta a requisitos externos.	R		R	R	R		R	A	R	R	R	R	R
MEA03.03 Confirmar el cumplimiento de requisitos externos.	R	I	R	R	R		A	R	R	R	C	C	C
MEA03.04 Obtener garantía de cumplimiento de requisitos externos.	I	I	I	I	I		C	C	C	R	C	C	C

Figura 67 Matriz RACI del proceso MEA02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso MEA03 se tiene controles de la ISO 27002 a continuación en la Figura 68:

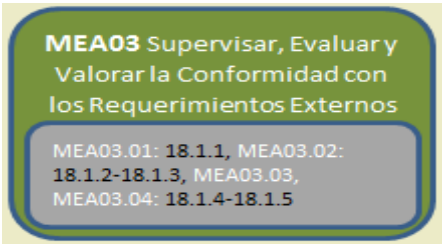


Figura 68 Proceso MEA03 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para MEA03 a continuación:

MEA03.01 Identificar requisitos externos de cumplimiento, según la ISO (2013):

- **Identificación de la legislación aplicable**: "Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización". (p. 70) Control 18.1.1.

MEA03.02 Optimizar la respuesta a requisitos externos, según la ISO (2013):

- **Derechos de propiedad intelectual (DPI)**: "Los procedimientos apropiados deben ser implementados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario". (p. 70) Control 18.1.2.

- **Protección de los registros de la organización**: “Los registros deben ser protegidos de la pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, de conformidad con los requisitos legislativos reglamentarios, contractuales y comerciales”. (p. 71) Control 18.1.3.

MEA03.03 Confirmar el cumplimiento de requisitos externos y MEA03.04 Obtener garantía de cumplimiento de requisitos externos, según la ISO (2013):

- **Protección de datos y privacidad de la información personal**: “Privacidad y protección de la información de identificación personal que deben garantizarse como se requiere en la legislación y regulación relevante en su caso”. (p. 72) Control 18.1.4.
- **Regulación de los controles criptográficos**: “Los controles criptográficos deben ser utilizados en el cumplimiento de todos los acuerdos pertinentes, leyes y reglamentos”. (p. 72) Control 18.1.5.

3.2.6. PRINCIPIO 6 CONDUCTA HUMANA:

Según la ISO/IEC (2015:)“Las políticas de TI, prácticas y decisiones demuestran respeto por el comportamiento humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada**”** (p. 9)

Cada principio de la norma internacional ISO/IEC 38500 tiene tres tareas. Según la ISO/IEC (2015):

- **Evaluar:** los órganos de gobierno deberían evaluar las actividades de las TI para asegurar que las conductas humanas se identifican y se consideran adecuadamente.
- **Orientar:** los órganos de gobierno deberían dirigir para que las actividades de TI sean consistentes con la conducta humana identificada además deberían dirigir para que los riesgos, oportunidades, problemas y preocupaciones relacionados con el negocio puedan identificarse y sean notificados por cualquier individuo en cualquier momento.
- **Supervisar:** los órganos de gobierno deberían monitorizar las actividades de TI para asegurar que las conductas humanas identificadas siguen siendo pertinentes y que se les presta una atención adecuada, también deberían monitorizar las prácticas de trabajo para asegurar que sean consistentes con el uso apropiado de las TI. (p.p. 15, 16)

El principio 5 debe establecer que las políticas y prácticas de TI, respetan y velan por las personas involucradas.

Para desarrollar el principio 2 de la ISO/IEC 38500 se lo debe hacer con los siguientes procesos de COBIT 5:

- APO07 Gestionar los Recursos Humanos
- BAI02 Gestionar la Definición de Requisitos
- BAI05 Gestionar la Facilitación del Cambio Organizativo.
- BAI08 Gestionar el conocimiento

3.2.6.1. APO07 Gestionar los Recursos Humanos

Según ISACA (2012c) el proceso APO07 Gestionar el presupuesto y los costes de COBIT 5:

> 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. (p. 83)

A continuación en la Figura 69 la matriz RACI para el proceso APO07:

MATRIZ RACI APO07													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
APO07.01 Mantener la dotación de personal suficiente y adecuada.						R				A	R	R	R
APO07.02 Identificar personal clave de TI.						R				A	R	R	R
APO07.03 Mantener las habilidades y competencias del personal.						R				A	R	R	R
APO07.04 Evaluar el desempeño laboral de los empleados.						R				A	R	R	R
APO07.05 Planificar y realizar un seguimiento del uso de recursos				R	R	I		R	R	R	R	R	R
APO07.06 Gestionar el personal contratado.						R				A	R	R	R

Figura 69 Matriz RACI del proceso APO07 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso APO07 se tiene controles de la ISO 27002 a continuación en la Figura 70:

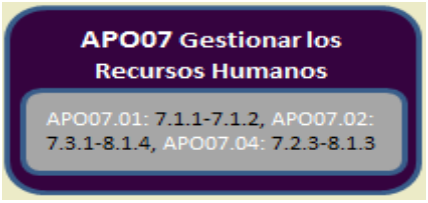


Figura 70 Proceso APO07 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para APO07 a continuación:

APO07.01 Mantener la dotación de personal suficiente y adecuado, según la ISO (2013):

- **Investigación de antecedentes:** Los controles de verificación de fondo sobre todos los candidatos para el empleo deben llevarse a cabo de acuerdo con las leyes, regulaciones y ética pertinente y debe ser proporcional a los requerimientos del negocio, clasificación de la información para acceder y riesgos percibidos (p. 12) Control 7.1.1.
- **Términos y condiciones de contratación:** "Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y de la organización para la seguridad de la información." (p. 13) Control 7.1.2.

APO07.02 Identificar personal clave de TI, según la ISO (2013):

- **Cese o cambio de puesto de trabajo:** "Las responsabilidades de seguridad de la información y de los derechos que permanecen válidas después de la terminación o cambio de trabajo deberían ser definidos, comunicado al trabajador o del empresario y forzada." (p. 15) Control 7.3.1.
- **Devolución de activos:** "Todos los empleados y contratistas deben devolver todos los activos de la organización en su posesión a la terminación de su empleo, contrato o acuerdo." (p. 17) Control 8.1.4.

APO07.04 Evaluar el desempeño laboral de los empleados, según la ISO (2013):

- **Proceso disciplinario** "Debe haber un proceso disciplinario formal y comunicado en su sitio para tomar medidas contra los empleados que han cometido una violación de la seguridad de la información" (p. 15) Control 7.2.3.
- **Uso aceptable de los activos:** "Reglas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de la información y la información deben ser identificados, documentados e implementados" (p. 17) Control 8.1.3.

3.2.6.2. BAI02 Gestionar la Definición de Requisitos

El proceso BAI02 Gestionar la Definición de Requisitos de COBIT 5, la definición, metas y definición de actividades se revisó en el apartado 3.2.3.8.

A continuación en la Figura 71 la matriz RACI para el proceso BAI02:

MATRIZ RACI BAI02													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.							C	I	R	C		R	C

Figura 71 Matriz RACI del proceso BAI02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.6.3. BAI05 Gestionar la Facilitación del Cambio Organizativo.

Según ISACA (2012c) el proceso BAI05 de COBIT 5: “Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI”. (p. 145)

A continuación en la Figura 72 la matriz RACI para el proceso BAI05:

MATRIZ RACI BAI05													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI05.01 Establecer el deseo de cambiar.	A	R	C	C	C	R	C	R	C	R	C	C	C
BAI05.02 Formar un equipo de implementación efectivo.	I		I	C	C	C	C	A	C	R	C	R	C
BAI05.03 Comunicar la visión deseada.	A		C	C	C	I	I	R	I	R	I	I	I
BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.				R	R	R	C	A	C	R		C	C
BAI05.05 Facilitar la operación y el uso.				C	C			A	R	R		R	R
BAI05.06 Integrar nuevos enfoques.	R		R	R	R			A	R	R		R	R
BAI05.07 Mantener los cambios.	R	R	R	R	R			A	R	R		R	R

Figura 72 Matriz RACI del proceso BAI02 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

3.2.6.4. BAI08 Gestionar el conocimiento

Según ISACA (2012c) el proceso BAI08 Gestionar el conocimiento de COBIT 5: “Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.” (p.159)

A continuación en la Figura 73 la matriz RACI para el proceso BAI08:

MATRIZ RACI BAI08													
Práctica clave de gobierno	Director General Ejecutivo (CEO)	STAFF	Director Financiero	Director de Producción	Director de Gestión	Gerente de Talento Humano	Gerente Legal	Ejecutivos de Negocio	Propietario del Proceso de Negocio	Director de Informática / Sistemas (CIO)	Jefe de Administración de TI	Jefe de Desarrollo	Gestor de Seguridad de la Información
BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos.							R	A	R	R	R	R	R
BAI08.02 Identificar y clasificar las fuentes de información.						C	C	A	R	R		R	
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.						C	I		C	A	R	R	
BAI08.04 Utilizar y compartir conocmiento.							R		A	R	R	C	C
BAI08.05 Evaluar y retirar la información.							C		A	R	R	C	R

Figura 73 Matriz RACI del proceso BAI08 de COBIT 5
Fuente: adaptado de Information Systems Audit and Control Association (ISACA, 2012c).

Según el análisis que se realizó en el apartado 3.2, para el proceso BAI08 se tiene controles de la ISO 27002 a continuación en la Figura 74:

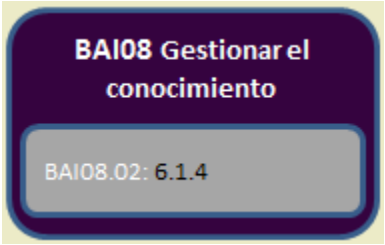


Figura 74 Proceso BAI08 de COBIT 5 y controles ISO 27002
Fuente: adaptado de (Millet, 2015).

Los controles ISO 27002 para BAI08 a continuación:

BAI08.02 Identificar y clasificar las fuentes de información, según la ISO (2013):

- **Contacto con grupos de interés especial:** “Los contactos adecuados con los grupos de intereses especiales u otros foros de seguridad especializada y las asociaciones profesionales deben mantenerse”. (p. 9) Control 6.1.4.

CAPITULO 4 NIVEL ACTUAL Y NIVEL DESEADO

Luego de realizado el análisis del estado actual de la empresa en el apartado 3.1, se puede observar que se tiene grandes brechas casi todas de 3 puntos entre el estado actual de la empresa y el estado al que se desea llegar tal como se muestra en la Figura 75:

Nivel de madurez de Gobierno de TI				BRECHA
Principios	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL	
1. Responsabilidad	2.533333333	4.533333333	5	2.00
2. Estrategia	1.533333333	4.4	5	2.87
3. Adquisición	1.666666667	4.6	5	2.93
4. Desempeño	1.266666667	4.4	5	3.13
5. Conformidad	1.266666667	4.4	5	3.13
6. Comportamiento Humano	1.4	4.666666667	5	3.27

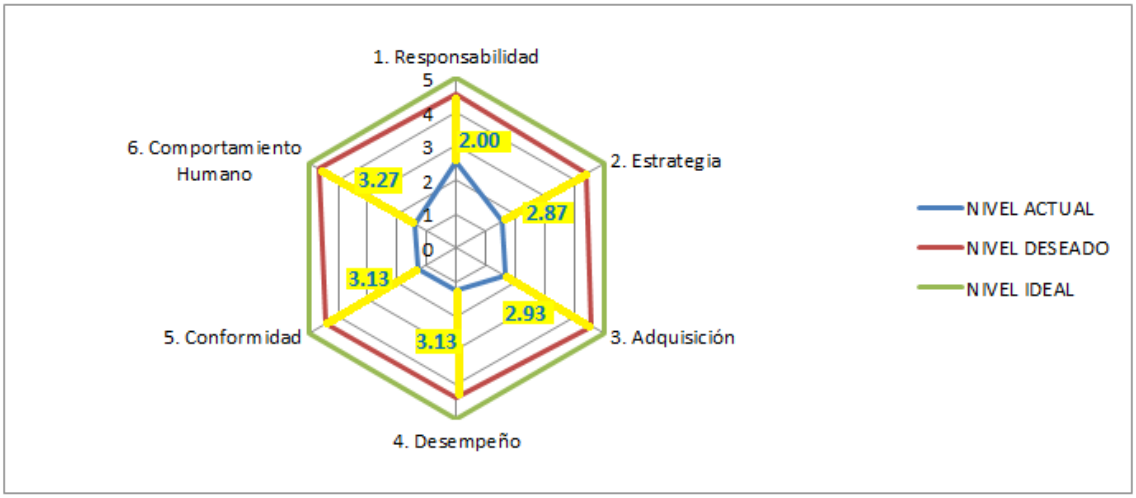


Figura 75 Nivel de madurez actual, deseado y brecha de Gobierno TI.
Fuente el autor

Estas brechas son fuentes potenciales de riesgos, mala administración, ineficiencia en la prestación de servicios, falta de establecimiento de procesos y controles, gastos innecesarios en equipamiento y contrataciones de tecnología, dependencia de personas clave en los procesos, desmotivación del personal, etc.

La implementación del marco de gobierno desarrollado en la Figura 29 ayudará a la empresa a pasar del estado actual hacia el estado deseado y eliminar las brechas que se tienen en la Figura 75.

4.1. Principio 1 Responsabilidad

La elaboración de matrices RACI para cada proceso de COBIT 5 permitirá la definición de roles y responsabilidades de las personas involucradas en la implementación del marco de gobierno o GEIT (Governance of Enterprise Information Technology). El realizar los subprocesos y actividades que aseguren 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 es imprescindible para completar el principio 1 de la ISO/IEC 38500.

Para alcanzar el nivel deseado: “El gerente de TI tendrá alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encontrará documentado. El gerente de TI verificará que todos los proyectos de tecnología, estén alineadas con las responsabilidades asignadas al área de TI y exigirá que se le entregue la información que necesita para cumplir su responsabilidad, incluidas las relativas a acciones y toma de decisiones. El gerente de TI supervisará y/o auditará periódicamente el desempeño de aquellos a quienes se ha asignado responsabilidad en el gobierno de TI”, por medio del desarrollo de las matrices RACI se asigna roles y responsabilidades a las personas involucradas en la implementación del marco de gobierno para cada práctica de los procesos COBIT 5.

Para el desarrollo del principio 1 se seleccionó únicamente el proceso EDM05 Asegurar la transparencia hacia las partes interesadas que tiene actividades como: “*Determinar si se están cumpliendo los requisitos de los diferentes interesados, Principios de elaboración de informes y comunicación; Evaluación de los requisitos corporativos de elaboración de informes; Directrices de escalado, etc.”* se podrá llegar al nivel de madurez deseado para el GEIT.

Más detalle de las prácticas y actividades para el principio 1 Responsabilidad se lo encuentra en el Anexo 4.

4.2. Principio 2 Estrategia

Según ISACA (2012c) para el principio 2: el 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 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 las soluciones y servicios; el crear mejores resultados,

mayor confianza en la tecnología y conseguir un uso efectivo de los recursos; el 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 y el 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, harán alcanzar el estado de madurez deseado por la empresa para el marco de gobierno TI. (p. p. 57, 79, 89, 101, 113)

Para alcanzar el nivel de madurez deseado: “El gerente de TI cuente con un plan estratégico de TI, el cual tendrá en cuenta los planes y las políticas de la organización. Los directores de TI evalúan periódicamente que las actividades de TI se mantengan alineadas con los objetivos de la organización. Los directores de TI tienen establecidos procedimientos y/o formatos para la presentación y recepción de propuestas de innovación en TI. Los directores de TI no solo supervisan el progreso del avance de los proyectos de TI, sino que se asegura que se estén cumpliendo los objetivos y beneficios planteados.”, se deberán realizar actividades de los procesos de COBIT 5 detallados en la Figura 29 tales como: *Desarrollar y mantener* estrategias y objetivos del negocio, *Definir los objetivos/metas de TI a alto nivel y cómo contribuirán a los objetivos de negocio empresariales, Definición de iniciativas estratégicas, Hoja de ruta estratégica*, *Modelo de la arquitectura de la información, Modelo de la arquitectura de procesos*, *Priorización y clasificación de las iniciativas de TI*, *Plan de Innovación*, etc. Más actividades y prácticas se las puede encontrar con detalle en el Anexo 4.

4.3. Principio 3 Adquisición

Según ISACA (2012c) para el principio 3: el 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 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, el 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 crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo; el establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales; el posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se

mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio; el proporcionar suficiente información sobre los activos del servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes del servicio harán que la organización llegue al nivel de madurez deseado para el marco de gobierno de las TI. (p.p. 43, 79, 101, 133, 149, 167)

Para alcanzar el nivel de madurez deseado: "Garantizar el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo, contar con procedimientos documentados y/o formatos que evidencien el cumplimiento del equilibrio mencionado. Los directores de TI gestionan los acuerdos de nivel de servicio (tanto internos como externos) de modo que aseguran que estos soportan las necesidades del negocio. (Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento de los acuerdos de nivel de servicio). Los directores de TI tienen contacto y/o alianzas estratégicas con los todos los proveedores de tecnología", se deberán desarrollar varias actividades tales como: *Desarrollar* p*rincipios rectores para la asignación de recursos y capacidades, 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. 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, etc*. El realizar las actividades mencionadas y las actividades detalladas del Anexo 4 harán que la organización elimine las brechas entre el nivel actual y el nivel deseado de madurez.

4.4. Principio 4 Desempeño

Según ISACA (2012c) el principio 4: el proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos; el alinear los planes estratégicos de TI con los objetivos del negocio, el 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 asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa, harán que la empresa alcance el nivel de madurez deseado para el GEIT. (p.p. 57, 93, 203)

Eliminar las brechas y llegar al nivel de madurez deseado:" El gerente de TI garantizará que la tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, los acuerdos de niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio, soportando las metas del negocio. El gerente de TI garantizará que los recursos que le son asignados, satisfacen las necesidades de la organización. La información que soporta al negocio, se encontrará disponible cuando se requiere, con datos correctos y actualizados y están protegidos contra pérdida o mal uso. Se tendrá establecido un cronograma, el cual se encuentra supervisado, con renovación de la tecnología de la información, de igual forma se tendrá asegurado los recursos para dicha renovación. El gerente de TI poseerá, controlará y supervisará el presupuesto asignado por la organización para la inversión de TI", se logrará con el desarrollo de actividades como: desarrollar *requisitos de supervisión; desarrollar métricas y objetivos de supervisión aprobado; realizar informes de desempeño, Catálogos de servicio, Acuerdos de nivel de servicio (ANSs), Acuerdos de nivel operativos (OLAs),etc*.

Para completar el principio 4 Desempeño se deberá desarrollar las actividades del Anexo 4, con esto se logrará alcanzar el nivel de madurez deseado por la organización.

4.5. Principio 5 Conformidad

Según ISACA (2012c) para el principio 5: el 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 asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables; el 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 harán que la organización alcance el nivel deseado. (p.p. 57, 207, 213)

Para llegar al nivel deseado por la empresa: "Cuenta con políticas y prácticas claras, las cuales se encuentren documentadas y detallen los requerimientos legales de TI que rigen a la Organización. El gerente de TI supervisará periódicamente que se cumplen dichas prácticas y políticas expresadas por la organización. El gerente de TI supervisará periódicamente que se cumpla con las obligaciones internas y externas en el uso de la tecnología de la información, los resultados de estas supervisiones se encontrarán

documentadas y son analizadas periódicamente en busca de la mejora continua. El gerente de TI supervisará la conformidad y el cumplimiento a través de prácticas de auditoría, dichas auditorias se encontrarán debidamente programadas, serán oportunas, exhaustivas y adecuadas y evaluarán el grado de satisfacción de las tecnologías de la información con los objetivos, políticas y/o directrices de la organización. Las auditorias incluirán la supervisión de los activos de TI y los datos (información) de la organización. También se incluirá la verificación del cumplimiento de todas las obligaciones legales pertinentes y las suscritas con clientes y proveedores.", se deberá desarrollar actividades tales como: *las políticas, principios, procedimientos y estándares deben estar actualizados*; o*btener 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*; *gestionar las deficiencias de cumplimiento en las políticas, estándares y procedimientos dentro de plazos razonables*, *etc*.

Como en todos los principios revisados se debe realizar las actividades detalladas en el Anexo 4 para poder eliminar las brechas entre el nivel actual y nivel deseado por la organización.

4.6. Principio 6 Conducta Humana

Según ISACA (2012c) para el principio 6: el optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa: el crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo; el establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales; el preparar y comprometer a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso; el proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad, harán que la empresa llegue al nivel de madurez deseado. (p.p. 83, 129, 133, 144, 159)

Eliminar las brechas del principio 6 y llegar al nivel deseado por la empresa: "El nivel al que desea llegar la empresa es que la organización conocerá acerca del comportamiento humano y sabe que esto incluye: cultura, necesidades, y aspiraciones de los usuarios, bien sea como individuos o como grupos. Además, el gerente de TI es consciente (y lo documentará como un riesgo) que estos comportamientos humanos pueden afectar el rendimiento las tecnologías de la información. Las políticas, prácticas y decisiones con respecto a TI demostrarán respeto por el comportamiento humano. La

organización contará con políticas y/o procedimientos que permitan escalar los riegos reportados hasta las personas correspondientes a cargo de la toma de decisiones, todos los reportes acerca de los riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información, se encontrarán debidamente documentados. El gerente de TI analizará periódicamente todos los reportes generados en busca de mejoras para la organización, esta supervisará periódicamente el nivel de satisfacción del comportamiento humano. (Por medio de encuestas de clima laboral, por ejemplo). La organización analizará los resultados de la supervisión de los comportamientos humanos y brindará la atención adecuada que se requiera para mejorar nivel de satisfacción. El gerente de TI supervisará periódicamente cómo los comportamientos humanos afectan el rendimiento de las tecnologías de la información. La organización supervisará periódicamente que las políticas, prácticas y decisiones de TI demuestren respeto por el comportamiento humano. El gerente de TI supervisará las prácticas laborales de los usuarios, con el fin de asegurar que sean consistentes del uso adecuado de la tecnología de información", se deberá desarrollar actividades tales como: *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*; *implementar un proceso de reconocimiento que premie el compromiso adecuado, el desarrollo de competencias y el logro exitoso de los objetivos de desempeño; realizar evaluaciones de desempeño, desarrollar planes de mejora, etc.*

El desarrollo de las actividades mencionas más el desarrollo de las actividades del Anexo 4 harán que la empresa alcance el nivel de madurez deseado para el GEIT.

4.7. Controles ISO/IEC 27002:2013

Finalmente se tienen los controles de seguridad de la ISO/IEC 27002:2013 que se deberán desarrollar para prácticas de varios procesos de COBIT 5 según sea el caso, completándose así la definición del marco de gobierno TI con la ISO/IEC 38500, COBIT 5 y la ISO/IEC 27002 y se lo tiene en la tabla 30 a continuación:

Tabla 8. Controles de las mejores prácticas de seguridad de la ISO 27002.

ID Proceso	Nombre Proceso	Práctica	Control ISO 27002:2013
APO03		APO03.02. Definir la arquitectura de referencia.	8.1.1. Inventario de activos
			8.1.3. Uso aceptable de los activos

	Gestionar la Arquitectura Empresarial		8.2.1. Directrices de clasificación
			8.2.2. Etiquetado y Manipulación de la información
			8.2.3. Manipulación de activos
APO12	Gestionar el Riesgo	APO12.01. Recopilar datos	16.1.2. Notificación de los eventos de seguridad de la información.
APO13	Gestionar la seguridad	APO13.01. Establecer y mantener un SGSI.	5.1.1. Conjunto de políticas para la seguridad de la información.
			6.1.1. Política de uso de dispositivos para movilidad.
		APO13.02. Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	7.2.2. Concienciación, educación y capacitación en seguridad de la información.
			12.1.2. Gestión de cambios.
			16.1.5. Respuesta a los incidentes de seguridad.
		APO13.03. Supervisar y revisar el SGSI.	5.1.2. Revisión de las políticas para la seguridad de la información.
			18.2.1. Revisión independiente de la seguridad de la información.
APO03	Gestionar la Arquitectura Empresarial	APO03.02. Definir la arquitectura de referencia.	8.1.1. Inventario de activos
			8.1.3. Uso aceptable de los activos
			8.2.1. Directrices de clasificación
			8.2.2. Etiquetado y Manipulación de la información
			8.2.3. Manipulación de activos
APO12	Gestionar el Riesgo	APO12.01. Recopilar datos	16.1.2. Notificación de los eventos de seguridad de la información.
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.01. Diseñar soluciones de alto nivel.	14.2.1. Política de desarrollo seguro de software.
		BAI03.02. Diseñar los componentes detallados de la solución.	14.2.6. Seguridad en entornos de desarrollo.
		BAI03.04. Obtener los componentes de la solución.	12.4.1. Registro y gestión de eventos de actividad.
			14.2.1. Política de desarrollo seguro de software.
			14.2.6. Seguridad en entornos de desarrollo.
		BAI03.06. Realizar controles de calidad.	14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas.
			14.1.3. Protección de las transacciones por redes telemáticas
		BAI03.08. Ejecutar pruebas de la solución.	14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas.
			14.2.9. Pruebas de aceptación.
		BAI03.09. Gestionar cambios a los requerimientos.	14.2.2. Procedimientos de control de cambios en los sistemas.
		BAI03.10. Mantener soluciones.	12.6.1. Gestión de las vulnerabilidades técnicas.
BAI06			12.1.2. Gestión de cambios.

	Gestionar los Cambios	BAI06.01. Evaluar, priorizar y autorizar peticiones de cambio.	14.2.2. Procedimientos de control de cambios en los sistemas.
			14.2.4. Restricciones a los cambios en los paquetes de software.
BAI09	Gestionar los Activos	BAI09.01. Identificar y registrar activos	8.1.1. Inventario de activos.
			8.1.2. Propiedad de los activos.
		BAI09.03. Gestionar el ciclo de vida de los activos.	8.1.3. Uso aceptable de los activos.
			8.1.4. Devolución de activos.
			8.2.2. Etiquetado y manipulado de la información.
			8.3.2. Eliminación de soportes.
			11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento.
		BAI09.05. Administrar licencias.	18.1.2. Derechos de propiedad intelectual (DPI).
MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	MEA02.01. Supervisar el control interno.	18.2.2. Cumplimiento de las políticas y normas de seguridad.
		MEA02.02. Revisar la efectividad de los controles sobre los procesos de negocio.	18.2.1. Revisión independiente de la seguridad de la información.
		MEA02.03. Realizar autoevaluaciones de control.	18.2.3. Comprobación del cumplimiento.
		MEA02.05. Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	18.2.1. Revisión independiente de la seguridad de la información.
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA03.01. Identificar requisitos externos de cumplimiento.	18.1.1. Identificación de la legislación aplicable.
		MEA03.02. Optimizar la respuesta a requisitos externos.	18.1.2. Derechos de propiedad intelectual (DPI).
			18.1.3. Protección de los registros de la organización.
		MEA03.03. Confirmar el cumplimiento de requisitos externos.	18.1.4. Protección de datos y privacidad de la información personal.
			18.1.5. Regulación de los controles criptográficos.
		MEA03.04. Obtener garantía de cumplimiento de requisitos externos.	18.1.4. Protección de datos y privacidad de la información personal.
			18.1.5. Regulación de los controles criptográficos.
APO07	Gestionar los Recursos Humanos	APO07.01. Mantener la dotación de personal suficiente y adecuado.	7.1.1. Investigación de antecedentes.
			7.1.2. Términos y condiciones de contratación.
		APO07.02. Identificar personal clave de TI.	7.3.1. Cese o cambio de puesto de trabajo.
			8.1.4. Devolución de activos.
			7.2.3. Proceso disciplinario.

		APO07.04. Evaluar el desempeño laboral de los empleados.	8.1.3. Uso aceptable de los activos.
BAI08	Gestionar el conocimiento	BAI08.02. Identificar y clasificar las fuentes de información.	6.1.4. Contacto con grupos de interés especial.

Fuente: adaptado de (Millet, 2015).

CONCLUSIONES

La organización está en un nivel muy bajo de Gobernanza de las TI, es importante tomar en consideración el marco definido de referencia para gobernanza de TI utilizando las mejores prácticas de los marcos y estándares ISO/IEC 38500, COBIT 5 e ISO/IEC 27002 para Memorial International of Ecuador mismo que mejorará la dirección y control de las TI actuales y futuras. El establecimiento del GEIT encaminará a la empresa hacia un manejo eficiente y eficaz de las TI, además permitirá tener un control más exacto de todos los componentes tecnológicos, se podrá mantener documentación de todos los procesos, políticas, prácticas y actividades que conciernan a las TI, se tendrá ahorros en la adquisición y renovación de equipos tecnológicos, se mejorará las seguridades de las TI, etc.

El análisis realizado en la empresa, indica que el nivel actual de la organización está situado para la mayoría de principios de la ISO/IEC 38500 en los dos puntos de un total de cinco puntos que es un nivel ideal. Además este análisis reveló que el nivel deseado de la empresa está por los cuatro puntos y medio para todos los principios.

Se realizó el análisis del marco de gobierno COBIT 5 y de los estándares internacionales ISO/IEC 38500 y 27002 para que estos sean efectivos, realizables y acorde para la organización. La falta de procesos, políticas y controles, hacen que las TI no sean eficientes ni eficaces, es por eso que la definición del marco de referencia para Gobernanza de TI debe ser tomado en cuenta en la gestión estratégica de la empresa.

Los controles de seguridad de la información de la organización son mínimos esto puede generar pérdida o robo de información, siniestros a nivel de arquitectura, daño de equipos, niveles de riesgos altos y no controlados, la implementación de controles de seguridad como los que se desarrolló para el marco de gobernanza ayudarán a la reducción de riesgos y un mejor control de estos.

La organización realiza actividades mínimas para la gestión de las TI, es importante que se tome en cuenta el marco de gobierno definido con sus procesos, actividades y controles para que la Gobernanza de las TI llegue al nivel deseado por la organización. El detalle de las actividades necesarias para implementación del marco de gobierno se encuentran definidas en el Anexo 4.

RECOMENDACIONES

Se recomienda la implementación del marco de gobierno definido en este trabajo para la Gobernanza de las TI utilizando las mejores prácticas y estándares como son la ISO 38500, COBIT 5 e ISO/IEC 27002:2013 para mejorar la gestión de las TI en la organización.

Se recomienda realizar para cada práctica de los procesos de COBIT 5 las actividades descritas en el Anexo 4, mismas que asegurarán el establecimiento del marco de gobierno y la correcta dirección y control de las TI de la organización.

Se recomienda de igual manera desarrollar los controles de seguridad de la ISO/IEC27002:2013 para las prácticas de COBIT 5 mapeadas para el GEIT de la organización definido es este trabajo.

Se recomienda el uso de roles y responsabilidades para implementar el marco de Gobierno de acuerdo a cada proceso COBIT 5 mapeado con la ISO 38500. Los roles y responsabilidades brindarán el alcance que involucra al personal que estará implementando el GEIT en la organización.

El estar alineado con normas internacionales y un marco de gobierno muy conocido como COBIT 5 hace que la empresa sea mejor vista tanto a nivel de país como internacionalmente, se solidifica su credibilidad y aumenta sus expectativas en la calidad de servicios ofrecidos tanto a los clientes internos como externos de la organización.

Se recomienda realizar un análisis profundo de los procesos y actividades que involucran las TI para tener una línea de partida y se pueda ver la diferencia entre el estado actual de las TI y un estado luego de implementado el GEIT.

BIBLIOGRAFÍA

Correa, M., & Parra B. (2012). *Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia*. (Proyecto de grado) Recuperado de: https://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/70666/5/modelo_gobierno_bancarias.pdf

Garbarino, Helena (2014). *Marco de Gobernanza de TI* para empresas. PyMEs - SMEsITGF. (Tesis doctoral) Recuperado de: http://oa.upm.es/31002/

Gasca, G., & Vega, V., & Echeverry, A. (2012). Análisis Comparativo de Modelos de Calidad. *Identificación de Mejores Prácticas para la Gestión de Calidad en Pequeños Entornos.* Recuperado de: www.infonorchile2012.uta.cl/download.php?file=infonor2012_1.pdf

Hernández, R., & Fernández, C., & Baptista, P. (1991). *Metodología de la Investigación.* Naucalpan de Juárez: McGraw-Hill

Information Systems Audit and Control Association (ISACA, 2012a). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Recuperado de: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Information Systems Audit and Control Association (ISACA, 2012b). *COBIT 5 Implementación*. Recuperado de: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Information Systems Audit and Control Association (ISACA, 2012c). *COBIT 5 Procesos Catalizadores*. Recuperado de: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2015). *ISO/IEC38500.* Information technology — Governance of IT for the organization. . Recuperado de https://inen.isolutions.iso.org/obp/ui/#iso:pub:PUB200013:en

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2013). *ISO/IEC 27002.* Information technology — Governance of IT for the organization. . Recuperado de https://inen.isolutions.iso.org/obp/ui/#iso:pub:PUB200013:en

ISO27000.ES. (2016). Guía de Controles ISO 27002:2013. Madrid. Recuperado de: http://iso27000.es/download/ControlesISO27002-2013.pdf

IT Governance Institute (ITGI, 2003). Board Briefing on IT Governance, 2nd Edition.

Recuperado de:
http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf

Millet, Eloy (2015). Estudio de una metodología de trabajo para la realización de auditorías integradas de sistemas de información. (Trabajo de fin de grado) Recuperado de:
https://riunet.upv.es/bitstream/handle/10251/54040/MILLET%20-%20Estudio%20de%20una%20metodolog%C3%ADa%20de%20trabajo%20para%20la%20realizaci%C3%B3n%20de%20auditor%C3%ADas%20integradas%20de%20si....pdf?sequence=1

Tamayo, M. (2003). *El proceso de la Investigación Científica.* México D.F.: Limusa

The Bank for International Settlements (BIS, 1999), *Enhancing Corporate Governance in Banking Organisation.* Recuperado de: http://www.bis.org/publ/bcbs56.pdf

The Committee on the Financial Aspects of Corporate Governance. (Cadbury Report, 1992) *The Report of the Committee on the Financial Aspects of Corporate Governance.* Recuperado de: http://www.icaew.com/~/media/corporate/files/library/subjects/corporate%20governance/financial%20aspects%20of%20corporate%20governance.ashx

Weill, P. & J. Ross, (2004). *IT Governance. How top performers manage IT decision rights for superior results*. Harvard Business School Press: Boston, Massachusetts. Recuperado de https://books.google.com.ec/books?id=0Gfraz7FyrYC&printsec=frontcover&dq=IT+Governance.+How+top+performers+manage+IT+decision+rights+for++superior+results+2015.&hl=es&sa=X&ved=0ahUKEwjpjdC9-snJAhULlx4KHe4lAuIQ6AEIHjAA#v=onepage&q&f=false

ANEXOS

ANEXO 1. Autoevaluación de nivel de madurez del Gobierno TI

Principio	Tarea	Nivel de Madurez					Nivel actual	Nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
1. Responsabilidad	Evaluar	En general, los individuos o grupos dentro de la organización no tienen claras sus responsabilidades con respecto al suministro y a la demanda de la información.	Los directores de TI establecen reglas y responsabilidades con relación al uso actual y futuro de las tecnologías de la información de la organización.	Con respecto al suministro y a la demanda de la información, los usuarios dentro de la organización, entienden y aceptan las reglas y responsabilidades asignadas por TI.	Los directores de TI tienen alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encuentran documentados.	Los directores de TI, evalúan la competencia (capacidad, autoridad, experiencia, etc.) de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a TI. (Los resultados de estas evaluaciones se encuentran documentados)		
	Dirigir	En la organización no se cuenta con proyectos de tecnología.	Los directores de TI, conocen pero no dirigen los proyectos de tecnología que se establecen en la alta gerencia de la organización (u otras áreas)	Los directores de TI dirigen todos los proyectos de tecnología de la organización. Los Directores de TI, cuentan con una autoridad parcial para solicitar información de otras dependencias.	Los directores de TI cuentan con un procedimiento documentado para ayudar a evaluar el cumplimiento de las metas de los proyectos de tecnología que dirigen.	Los directores de TI verifican que todos los proyectos de tecnología, estén alineadas con las responsabilidades asignadas al área de TI. Los directores de TI exigen que se les entregue la información que necesitan para cumplir sus responsabilidades, incluidas las relativas a acciones y toma de decisiones.		
	Supervisar	Los directores de TI tienen algún conocimiento acerca de gobierno de TI.	Los directores de TI conocen y supervisan que se hayan establecido los mecanismos adecuados para el gobierno de TI. Así mismo, cuenta con procedimientos y/o formatos que garanticen el mantenimiento de un modelo de gobierno de TI	Los directores de TI supervisan y/o auditan periódicamente el funcionamiento de los mecanismos implementados para el cumplimiento de gobierno de TI. (Dichas supervisiones se encuentran documentadas)	Los directores de TI supervisan y/o auditan periódicamente el desempeño de aquellos a quienes se ha asignado responsabilidad en el gobierno de TI (por ejemplo, aquellas personas miembros de los comités, jefes, coordinadores, etc.)	También supervisan y/o auditan periódicamente que los individuos o grupos dentro de la organización entiendan y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de tecnología de la información.		

Principio		Nivel de Madurez					Nivel actual	Nivel desead
	Tarea	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
2. Estrategia	Evaluar	Los directores de TI, evalúan y brindan soporte a las necesidades actuales del negocio.	Los directores de TI estudian los avances de la tecnología de la información y los procesos del negocio con el fin de asegurarse de que TI brinda soporte a las necesidades futuras del negocio. (Los resultados de dicha evaluación se encuentran documentadas)	Los directores de TI evalúan y monitorean las actividades de TI, pero no aseguran que estas se mantengan (con el paso del tiempo) alineadas con los objetivos de la organización.	Los directores de TI cuentan con un plan estratégico de TI, el cual tiene en cuenta los planes y las políticas de la organización. Los directores de TI evalúan periódicamente que las actividades de TI se mantengan alineadas con los objetivos de la organización. (Los resultados de dicha evaluación y alineación con los objetivos de la organización se encuentran documentados)	Los directores de TI garantizan que sus procesos podrían ser (en cualquier momento), verificados, auditados y/o evaluados tal como se describe en normas nacionales e internacionales pertinentes.		
	Dirigir	Los usuarios conocen los procesos de TI de la Organización.	Los usuarios de la Organización están autorizados para presentar propuestas de innovación para TI	La Organización fomenta y estimula la presentación de propuestas de innovación de TI. (Se tiene establecido un procedimiento, formato lineamiento, etc., que evidencie la forma como se fomenta dicha actividad)	Los directores de TI tienen establecidos procedimientos y/o formatos para la presentación y recepción de propuestas de innovación en TI.	Los directores de TI fomentan y evalúan que estas propuestas permitan a la organización responder a oportunidades, nuevos retos, mejorar los procesos de la organización y/o estén alineadas con los objetivos del negocio.		
	Supervisar	La Organización cuenta con una metodología para la ejecución de proyectos	Todos los proyectos de la organización (incluidos los de TI) son monitoreados para supervisar el progreso de los mismas	Los directores de TI conocen y supervisan el progreso de los proyectos de TI. (Dicha supervisión se encuentra debidamente documentada)	Los directores de TI no solo supervisan el progreso del avance de los proyectos de TI, sino que se asegura que se estén cumpliendo los objetivos y beneficios planteados.	Los directores de TI, supervisan el uso de TI para asegurar que de ésta, se obtienen los beneficios previstos y que continúen alineados con los objetivos de la organización.		

Principio		Nivel de Madurez					Nivel actual	Nivel desead
	Tarea	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3. Adquisición	Evaluar	Cualquier proceso dentro de la Organización puede solicitar un requerimiento para la adquisición tecnología.	Los directores de TI evalúan diferentes opciones al momento de adquirir tecnología, pero no son los únicos encargados de aprobar la propuesta.	Los directores de TI son los encargados y responsables de adquirir tecnología para la organización	Los directores de TI aprueban la mejor propuesta que de cumplimiento a los requerimientos planteados, además que garantice el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.	Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento del equilibrio mencionado		
	Dirigir	Los directores de TI gestionan y mantienen los activos de TI (sistemas e infraestructura)	Los directores de TI adquieren tecnología de forma correcta, clara y transparente, teniendo en cuenta los requerimientos planteados	Los directores de TI verifican que se incluya la respectiva documentación (instructivos, manuales, etc.) de la tecnología adquirida, a la vez que aseguran que el las tecnologías adquiridas cumplen con las capacidades requeridas.	Los directores de TI verifican el cumplimiento de los acuerdos de nivel de servicio (tanto internos como externos)	Los directores de TI gestionan los acuerdos de nivel de servicio (tanto internos como externos) de modo que aseguran que estos soportan las necesidades del negocio. (Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento de los acuerdos de nivel de servicio)		
	Supervisar	La organización cuenta con mecanismos para supervisar que las inversiones, en términos generales, están acordes con las requeridas.	Los directores de TI supervisan (auditan) que las inversiones en TI, proporcionan las capacidades requeridas para las cuales fueron adquiridas.	Se tienen algún tipo de procedimiento y/o formato que permita evidenciar el resultado de la supervisión realizada en las inversiones de TI	Los directores de TI tienen contacto con los proveedores de tecnología solo en ocasiones puntuales	Los directores de TI tienen contacto y/o alianzas estratégicas con los todos los proveedores de tecnología.		

Principio		Nivel de Madurez					Nivel actual	Nivel desead
	Tarea	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
4. Desempeño	Evaluar	Los directores de TI evalúan que la tecnología de la información apoya los procesos de negocio con la habilidad y capacidad requeridas.	Los directores de TI tienen políticas dirigidas hacia la continuidad de la operación normal del negocio y del tratamiento de los riesgos asociados con el uso de la tecnología de la información.	Los directores de TI evalúan periódicamente los riesgos que se originan en las actividades de la tecnología de la información para la continuidad de la operación de los negocios. Además evalúan los riesgos para la integridad de la información y protección de los activos de tecnología de la información, incluyendo la propiedad intelectual y memoria organizacional asociadas.	Los directores de TI garantizan que la tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, los acuerdos de niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio, soportando las metas del negocio.	Los directores de TI evalúan con regularidad la eficacia y el desempeño del sistema organización para el gobierno TI (Se cuenta con un procedimiento documentado y/o formatos que evidencia el cumplimiento de esta evaluación)		
	Dirigir	La Organización cuenta con un mecanismo de asignación de recursos para sus diferentes procesos.	Los directores de TI tienen asegurada la asignación de los recursos suficientes para el ejercicio de sus funciones	Los directores de TI garantizan que los recursos que le son asignados, satisfacen las necesidades de la organización.	La información que soporta al negocio, se encuentra disponible cuando se requiere, con datos correctos y actualizados y están protegidos contra pérdida o mal uso.	Los directores de Ti cuentan con mecanismos y/o procedimientos que garantizan la calidad y disponibilidad de la información		
	Supervisar	Los directores de TI supervisan la "vida útil" de la tecnología de la información da soporte al negocio.	Los directores de TI cuentan con mecanismos documentados que permiten prever cuando la tecnología de la información, se acerca al final de su "vida útil"	Se tiene establecido un cronograma, el cual se encuentra supervisado, de renovación de la tecnología de la información, de igual forma se tiene asegurado los recursos para dicha renovación.	Los directores de TI poseen, controlan y supervisan el presupuesto asignado por la Organización para la inversión de TI	Los directores de TI dan prioridad a las inversiones que impacten directamente los objetivos del negocio.		

Principio	Tarea	Nivel de Madurez					Nivel actual	Nivel desead
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
5. Conformidad	Evaluar	Los directores de TI garantizan que le tecnología de la Información cumple con todos lineamientos establecidos por la Organización	De igual manera, los directores de TI garantizan que la tecnología de la Información de la Organización cumple con todas las leyes y los reglamentos obligatorios.	La Organización cuenta con políticas y prácticas claras, las cuales se encuentran documentadas y detallan los requerimientos legales de TI que rigen a la Organización.	Los directores de TI supervisan periódicamente que se cumplen dichas prácticas y políticas expresadas por la Organización.	Los directores de TI evalúan periódicamente que las tecnologías de la información satisfacen las obligaciones reglamentarias, legislativas, de ley, contractuales, las políticas internas, las normas y las directrices profesionales.		
	Dirigir	La Organización garantiza que se cumple con las obligaciones legales pertinentes.	Los directores de TI colaboran con la Alta Gerencia a establecer mecanismos regulares y rutinarios para garantizar que el uso de la tecnología de la información cumple con las obligaciones pertinentes (reglamentarias, legislativas, de ley, contractuales), las normas y las directrices.	Los directores de TI supervisan periódicamente que se cumpla con las obligaciones internas y externas en el uso de la tecnología de la información.	Los resultados de estas supervisiones se encuentran documentadas y son analizadas periódicamente en busca de la mejora continua.	La organización cuenta con directrices claras que regulan el comportamiento de los usuarios con relación a las TI de la Organización.		
	Supervisar	Los directores de TI supervisan la conformidad y el cumplimiento de las obligaciones de TI a través de prácticas adecuadas de auditoría.	Dichas auditorias se encuentran debidamente programadas, son oportunas, exhaustivas y adecuadas y evalúan el grado de satisfacción de las tecnologías de la información con los objetivos, políticas y/o directrices de la Organización.	Las auditorias incluyen la supervisión de los activos de TI y los datos (información) de la Organización.	También se incluye la verificación del cumplimiento de todas las obligaciones legales pertinentes y las suscritas con clientes y proveedores	Las auditorias también supervisan las actividades tendientes a la preservación de la información privada de la Organización		

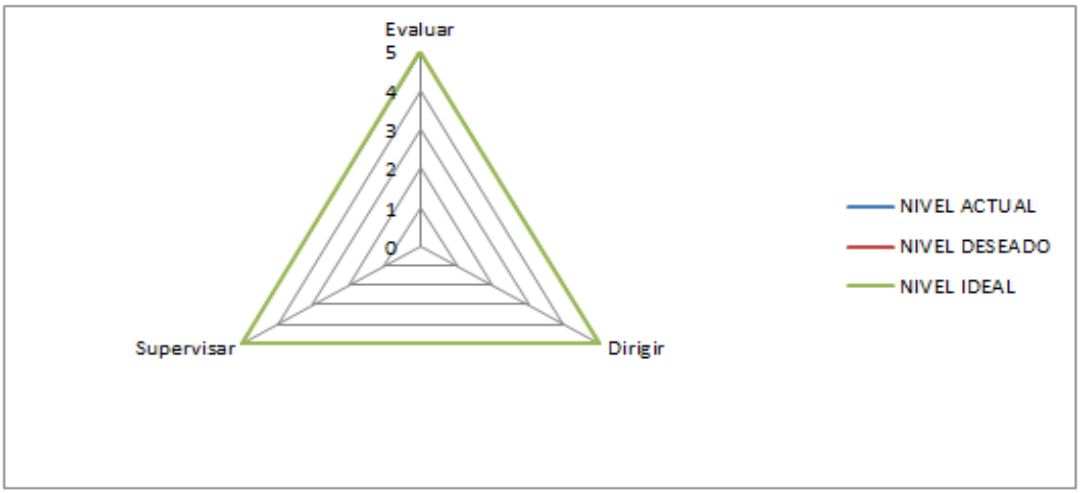
Principio		Nivel de Madurez					Nivel actual	Nivel desead
	Tarea	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
6. Comportamiento Humano	Evaluar	Los usuarios de la Organización tienen un conocimiento básico de las tecnologías que tienen disponibles	Los directores de TI ayudan a que los usuarios entiendan y aprovechen la tecnología que tienen disponible, de modo que estos aumenten su desempeño personal y el de los sistemas de información.	Los directores de TI tienen documentadas las interacciones (relaciones) existentes entre los usuarios y las tecnologías de la información disponibles en la Organización.	La Organización conoce acerca del comportamiento humano y sabe que esto incluye: La cultura, las necesidades, y las aspiraciones de los usuarios, bien sea como individuos o como grupos. Además, los directores de TI son conscientes (y lo documentan como un riesgo) que estos comportamientos humanos pueden afectar el rendimiento las tecnologías de la información.	Las políticas, prácticas y decisiones con respecto a TI demuestran respeto por el comportamiento humano.		
	Dirigir	Los directores de TI dirigen de tal manera que las actividades de TI sean consistentes con el comportamiento humano identificado.	Los directores de TI cuentan con mecanismos que permiten que cualquier persona en cualquier momento pueda identificar y reportar riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información	La Organización cuenta con políticas y/o procedimientos que permiten escalar los riegos reportados hasta las personas correspondientes a cargo de la toma de decisiones.	Todos los reportes acerca de los riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información, se encuentran debidamente documentados	Los directores de TI analizan periódicamente todos los reportes generados en busca de mejoras para la Organización		
	Supervisar	La Organización supervisa periódicamente el nivel de satisfacción del comportamiento humano. (Por medio de encuestas de clima laboral, por ejemplo).	La Organización analiza los resultados de la supervisión de los comportamientos humanos y brinda la atención adecuada que se requiera para mejorar nivel de satisfacción.	Los directores de TI supervisan periódicamente cómo los comportamientos humanos afectan el rendimiento de las tecnologías de la información.	La Organización supervisa periódicamente que las políticas, prácticas y decisiones de TI demuestren respeto por el comportamiento humano	Los directores de TI supervisan las prácticas laborales de los usuarios, con el fin de asegurar que sean consistentes del uso adecuado de la tecnología de información.		

ANEXO 2. Formato para toma de resultados de Autoevaluación del nivel de madurez de Gobierno TI

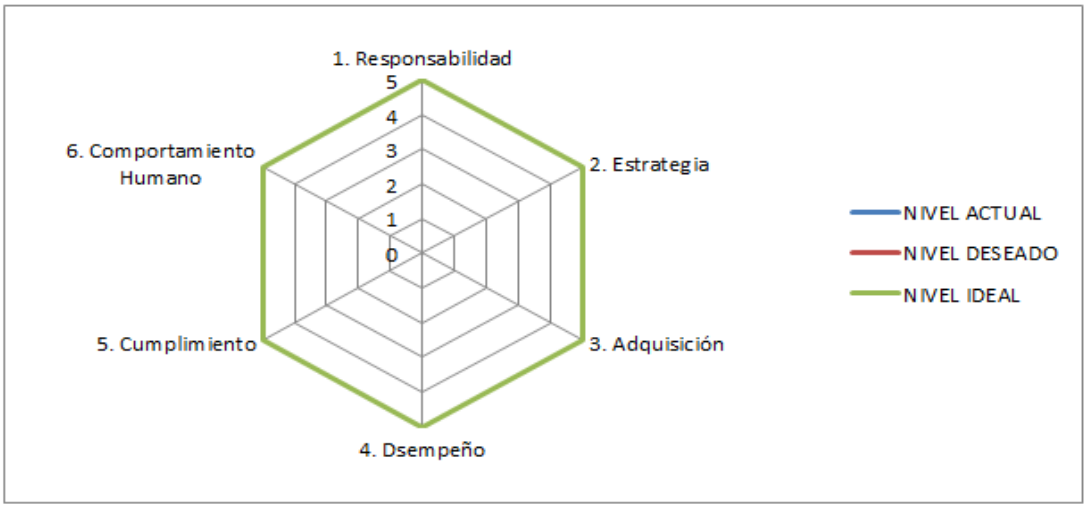
Principio		Encuestado 1		Encuestado 2		Encuestado 3		Encuestado 4		Encuestado 5		RESULTADO	
	Tarea	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado	Nivel actual	Nivel deseado
1. Responsabilidad	Evaluar												
	Dirigir												
	Supervisar												
2. Estrategia	Evaluar												
	Dirigir												
	Supervisar												
3. Adquisición	Evaluar												
	Dirigir												
	Supervisar												
4. Desempeño	Evaluar												
	Dirigir												
	Supervisar												
5. Conformidad	Evaluar												
	Dirigir												
	Supervisar												
6. Comp. Humano	Evaluar												
	Dirigir												
	Supervisar												

ANEXO 3. Formato de análisis de resultados de la Autoevaluación del nivel de madurez de Gobierno TI individual y global

Nivel de madurez de Gobierno de TI Principio 1. Responsabilidad			
TAREAS	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
Evaluar	0	0	5
Dirigir	0	0	5
Supervisar	0	0	5



Nivel de madurez de Gobierno de TI			
Principios	NIVEL ACTUAL	NIVEL DESEADO	NIVEL IDEAL
1. Responsabilidad	0	0	5
2. Estrategia	0	0	5
3. Adquisición	0	0	5
4. Dsempeño	0	0	5
5. Cumplimiento	0	0	5
6. Comportamiento Humano	0	0	5



ANEXO 4. Actividades para el marco de Gobierno TI de procesos COBIT 5

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
EDM02	Asegurar la Entrega de Beneficios	EDM02.01	Evaluar la optimización de valor	1 Comprender los requerimientos de las partes interesadas, y la tecnología con capacidades para la estrategia de la empresa. 2 Comprender elementos clave de gobierno 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. 3 Evaluar la efectividad de integración y alineamiento de las estratégias de TI que aporten valor. 4 Comprender y considerar la efectividad de los roles, responsabilidades, asignaciones actuales, asegurando la creación de valor de las inversiones, servicios y activos de TI.	1 Evaluación de la alineación estratégica. 2 Evaluación de inversiones y portafolio de servicios.
		EDM02.02	Orientar la optimización de valor	1 Definir y comunicar la cartera,los tipos de inversión, categorías, criterios y ponderaciones relativas a los criterios. 2 Definir los requerimientos para los cambios de fase (state gate) y otras revisiones por la importancia de la inversión para la empresa y el riesgo asociado. 3 Orientar a la dirección a considerar usos potenciales de TI innovadores. 4 Definir y comunicar a nivel de empresa los objetivos de entrega de valor y las medidas de resultados que permitan un control eficaz. 5 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. 6 Recomendar innovaciones potenciales, cambios organizativos o mejoras operativas que desde las iniciativas TI pudieran impulsar un crecimiento de valor para la empresa.	1 Tipos de inversión y criterios 2 Requerimientos para las revisiones de cambio de fase (state gate)
		EDM02.03	Supervisar la optimización de valor	1 Definir un conjunto equilibrado de objetivos de desempeño, métricas, metas y puntos de referencia. 2 Recoger datos pertinentes, oportunos, completos, fiables y precisos para informar sobre avances en la entrega de valor. 3 Conseguir informes habituales y relevantes de la cartera, programa y desempeño de TI. 4 Tras la revisión de los informes, tomar las medidas de gestión apropiadas para asegurar que el valor sea optimizado. 5 Tras la revisión de los informes,asegúrese de que las medidas correctivas apropiadas son iniciadas y controladas.	1 Acciones para mejorar la entrega de valor. 2 Comentarios sobre el rendimiento de la cartera y del programa.
EDM04	Asegurar la Optimización de Recursos	EDM04.01	Evaluar la gestión de recursos	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. 2 Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI puedan satisfacer las necesidades de la empresa, con la habilidad y capacidad requerida de acuerdo a las prioridades acordadas y las limitaciones presupuestarias. 3 Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la empresa para la entrega de valor y la mitigación de riesgos con los recursos asignados. 4 Comprender los requisitos para alinear la gestión de recursos con la planificación de recursos empresariales financieros y humanos. 5 Definir los principios para la gestión y el control de la arquitectura de la empresa.	1 Principios rectores para la asignación de recursos y capacidades. 2 Principios rectores de la arquitectura de la empresa 3 Plan de recursos aprobado
		EDM04.02	Dirigir la gestión de recursos	1 Comunicar e impulsar la adopción de estrategias de gestión de recursos, principios y el plan de recursos y las estrategias de arquitectura de empresa acordados. 2 Asignar responsabilidades para la ejecución de la gestión de recursos. 3 Definir los objetivos, medidas y métricas clave para la gestión de los recursos. 4 Establecer los principios relacionados con la protección de recursos. 5 Alinear la gestión de recursos con la planificación de RRHH y financiera de la empresa.	1 Comunicación de las estrategias de reasignación de 2 Principios para la protección de recursos 3 Responsabilidades asignadas para la gestión de los recursos.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
		EDM04.03	Supervisar la gestión de recursos.	1 Supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la empresa mediante objetivos y métricas acordados. 2 Supervisar las estrategias de aprovisionamiento 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 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.	1 Comentarios sobre la asignación y la eficacia de los recursos y capacidades. 2 Acciones correctivas para hacer frente a las desviaciones de gestión de recursos.
EDM05	Asegurar la transparencia hacia las partes interesadas	EDM05.01	Evaluar los requisitos de elaboración de informes de las partes	1 Examinar y juzgar los requisitos actuales y futuros de elaboración de informes respecto al uso de las TI dentro de la empresa. 2 Examinar y juzgar los requisitos actuales y futuros de elaboración de informes para otros interesados respecto al uso de las TI dentro de la empresa. 3 Mantener los principios de comunicación con los grupos de interés externos e internos.	1 Principios de elaboración de informes y comunicación 2 Evaluación de los requisitos corporativos de elaboración de informes
		EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes	1 Orientar el establecimiento de la estrategia de comunicación interesados externos e internos. 2 Orientar la implementación de mecanismos para garantizar que la información cumple con todos los criterios corporativos obligatorios de elaboración de informes de TI. 3 Establecer mecanismos de validación y aprobación de la elaboración obligatoria de informes. 4 Establecer mecanismos de escalado en la elaboración de informes.	1 Directrices de escalado 2 Reglas de validación y aprobación de informes
		EDM05.03	Supervisar la comunicación con las partes interesadas	1 Evaluar periódicamente la eficacia de los mecanismos para asegurar la precisión y fiabilidad de la elaboración obligatoria de informes. 2 Evaluar periódicamente la eficacia de los mecanismos y las salidas de la comunicación con interesados externos e internos. 3 Determinar si se están cumpliendo los requisitos de los diferentes interesados.	1 Evaluación de la eficacia de la elaboración de informes
APO02	Gestionar la estratégia	APO02.01	Comprender la dirección de la empresa.	1 Desarrollar y mantener estrategias y objetivos del negocio. 2 Determinar prioridades para el cambio estratégico. 3 Identificar las partes interesadas más importantes y obtener comprensión de sus requerimientos. 4 Identificar y analizar las fuentes de los cambios en la empresa y en el entorno externo. 5 Entender la arquitectura actual de empresa y determinar brechas potenciales en la arquitectura.	1 Fuentes y prioridades para cambios.
		APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	1 Desarrollar un punto de referencia del negocio, entorno de TI, capacidades y servicios actuales. 2 Identificar los problemas, fortalezas, oportunidades y amenazas en el entorno actual, las capacidades y servicios. 3 Identificar los actuales y potenciales riesgos y tecnologías en declive. 4 Identificar diferencias entre el negocio actual y las capacidades de TI, entre servicios y estándares y mejores prácticas de referencia. 5 Identificar los problemas, fortalezas, oportunidades y amenazas en el entorno actual, las capacidades y servicios.	1 Análisis DAFO de capacidades. 2 Línea de referencia de capacidades actuales. 3 Diferencias y riesgos relacionados con las capacidades actuales.
		APO02.03	Definir el objetivo de las capacidades de TI.	1 Definir los objetivos/metas de TI a alto nivel y cómo contribuirán a los objetivos de negocio empresariales. 2 Definir el proceso de negocio requerido y deseado, las capacidades y los servicios de TI. 3 Identificar las amanazas por el rechazo a las actuales y nuevas tecnologías adquiridas. 4 Considerar la aprobación de tecnologías emergentes e ideas innovadoras.	1 Propuesta de cambio en la arquitectura del negocio. 2 Requerimientos del negocio y capacidades de TI. 3 Objetivos de TI a alto nivel

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO02	Gestionar la estratégia	APO02.04	Realizar un análisis de diferencias.	1 Identificar todas las diferencias y cambios necesarios para realizar en el entorno deseado. 2 Considerar las implicaciones a alto nivel de todas las diferencias. 3 Evaluar el impacto de posibles cambios en el negocio y en los modelos operativos de TI, y en los programas de inversión de TI. 4 Mejorar la definición del entorno deseado y preparar una declaración de valor con los beneficios a percibir de ese entorno.	1 Diferencias y cambios requeridos para alcanzar la meta de capacidad. 2 Declaración del valor beneficio para el entorno deseado.
		APO02.05	Definir el plan estratégico y la hoja de ruta.	1 Identificar los requerimientos de recursos, planificación y presupuestos de inversión/operacional de cada iniciativa. 2 Identificar y abordar adecuadamente los riesgos, costes e implicaciones de los cambios organizativos en el proceso de planificación. 3 Crear una hoja de ruta indicando la planificación y las interdependencias de las iniciativas. 4 Definir las iniciativas necesarias para cerrrar las diferencias y migrar del entorno actual al deseado. 5 Traducir los objetivos en medidas de resultado representativas por métricas (qué) y objetivos (cuánto) que puedan ser relacionados con los beneficios empresariales. 6 Obtener formalmente soporte de las partes interesadas y obtener aprobación del plan.	1 Definición de iniciativas estratégicas. 2 Evaluación del riesgo. 3 Hoja de ruta estratégica.
		APO02.06	Comunicar la estratégia y la dirección de TI.	1 Desarrollar y mantener una red de aprobación e impulso de la estrategia de TI. 2 Desarrollar un plan de comunicación que cubra los mensajes necesarios, audiencias objetivo, mecanismos/canales de comunicación y horarios. 3 Preparar un paquete de comunicaciones que entegue el plan de manera eficaz utilizando los medios de comunicacipón y tecnologías disponibles. 4 Obtener retroalimentación y actulizar el plan de comunicaciones y de entrega según sea necesario.	1 Plan de comunicación 2 Paquete de comunicación
APO03	Gestionar la Arquitectura Empresarial	APO03.01	Desarrollar la visión de la arquitectura de empresa.	1 Identificar a las partes interesadas clave de la empresa y sus objetivos/preocupaciones y definir los requisitos clave a ser considerados. 2 Alinear los objetivos de la arquitectora con la prioridades estratégicas del plan empresarial. 3 Definir qué está dentro y qué está fuera del alcance de la arquitectura de partida y los esfuerzos de arquitectura objetivo. 4 Crear la visión de la arquitectura atendiendo a las preocupaciones de las partes interesades. 5 Definir la proposiciones de valor, los objetivos y métricas de la arquitectura objetivo. 6 Identificar los riesgos empresariales asociados con el cambio de la nueva visión de la arquitectura, evaluar el nivel de riesto inicial y desarrollar una estrategia de mitigación. 7 Desarrollar el caso de negocio del concepto de arquitectura empresarial.	1 Alcance de la arquitectura definido 2 Principios de arquitectura 3 Caso de negocio y propuesta de valor del concepto arquitectura.
		APO03.02	Definir la arquitectura de referencia.	1 Mantener un repositorio de la arquitectura que contenga los estándares, los componentes reutilizables, el modelado, las relaciones, las dependencias y las vistas. 2 Seleccionar los puntos de vista de referencia del repositorio de la arquitectura. 3 Desarrollar descripciones de dominio de arquitectura de partida. 4 Mantener un modelo de arquitectura de procesos como parte de las descripciones de dominio de referencia y objetivo. 5 Mantener un diccionario de datos de la empresa que promueva la interpretación común. 6 Crear un documento de definición de la arquitectura.	1 Descripciones de dominio de partida y definición de la arquitectura. 2 Modelo de arquitectura de procesos. 3 Modelo de la arquitecrura de la información.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO03	Gestionar la Arquitectura Empresarial	APO03.03	Seleccionar las oportunidades y las soluciones.	1 Determinar y confirmar los atributos clave del cambio. 2 Revisar y consolidar los resultados del análisis de diferencias entre las arquitecturas de partida y 3 Evaluar las necesidades, las carencias, las soluciones y los fatores para identificar un conjunto mínimo de requisitos funcionales. 4 Afinar las dependencias iniciales. 5 Confirmar el grado de preparación de la empresa y el riesgo asociado a la transformación 6 Formular una implementación de alto nivel y una estrategia de migración. 7 Desarrollar una serie de arquitecturas de transición cuando sea necesario un enfoque incremental. 8 Conciliar los requisitos ya consolidados con las posibles soluciones. 9 Identificar y agrupar los principales paquetes de trabajo en un conjunto de programas y proyectos	1 Estrategia de implementación a alto nivel y estrategia de migración. 2 Arquitecturas de transición.
		APO03.04	Definir la implantación de la arquitectura.	1 Establecer lo que el plan de implementacion y migración debería incluir como parte del programa y plan de proyectos. 2 Confirmar las fases y progresos de la arquitectura de transición y actualizarlos en el documento de definición de la arquitectura. 3 Definir los requisitos de gobiernos de implementación de la arquitectura.	1 Requisitos de gobierno de la arquitectura. 2 Descripciones de las fases de implementación. 3 Necesidades de recursos
		APO03.05	Proveer los servicios de arquitectura empresarial.	1 Confirmar alcance, prioridades y proporcionar orientación para desarrollor y desplegar soluciones. 2 Gestionar la cartera de servicios de arquitectura para asegurar el alineamiento con los objetivos estratégicos y el desarrollo de soluciones. 3 Gestionar los requisitos de la arquitectura empresarial y dar solporte con los principios de dicha arquitectura, modelos y componentes básicos 4 Identificar y alinear las prioridades de la arquitectura empresarial a los motivadores del valor. 5 Medir el cumplimiento de estos estándares y guías de referencia.	1 Orientación para el desarrollo de soluciones.
APO05	Gestionar el Portafolio	APO05.01	Establecer la mezcla del objetivo de inversión.	1 Validar que las inversiones TI y los servicios TI actuales están alineados con la visión y principios corporativos, metas,objetivos estratégicos. 2 Conseguir un entendimiento común entre TI y otras funciones de negocio sobre potenciales oportunidades de TI. 3 Crear una mezcla de inversión que logre el balance adecuado entre distintas dimensiones. 4 Identificar las categorias generales de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura, activos de TI, recursos, habilidades, prácticas, controles y relaciones que sustenten la estrategia corporativa. 5 Acordar una estrategia TI y metas. Identificar y facilitar sinergias que puedan ser alcanzadas.	1 Mezcla de inversión definida. 2 Identificar recursos y capacidades necesarias para soportar la estrategia. 3 Observaciones a la estrategia y a las metas.
		APO05.02	Determinar la disponibilidad y las fuentes de fondos.	1 Entender la disponibilidad y el compromiso de los fondos actuales, el gasto actual aprobado y la cantidad real gastada hacia la fecha. 2 Identificar las opciones para obtener financiación adicional para las inversiones TI. 3 Determinar las implicaciones de la fuente de financiacipon en las expectativas del retorno de	1 Opciones de financiación. 2 Expectativas de retorno de inversión.
		APO05.03	Evaluar y seleccionar los programas a financiar.	1 Reconocer las oportunidades de inversión y clasificarlas en línea con las categorías del portafolio de inversiones. 3 Evaluar el impacto en el portafolio general de inversiones por añadir los programas candidatos. 4 Decidir qué programas candidatos deberían ser trasladados al portafolio de inversiones activas. 5 Determinar los hitos necesarios para el ciclo de vida económico de cada programa seleccionado. 6 Establecer procedimientos para comunicar coste, beneficios y aspectos relativos al riesgo de los	1 Casos de negocio de programa. 2 Programas seleccionados con hitos del retorno de

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO05	Gestionar el Portafolio	APO05.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	1 Revisar regularmente el portafolio para identificar y explotar sinergias, eliminar programas duplicados e identificar y mitigar el riesgo. 2 Cuando sucedan cambios, volver a evaluar y a priorizar el portafolio. 3 Ajustar los objetivos, provisiones, presupuestos. 4 Identificar desviaciones para control presupuestario y gestión del beneficio. 5 Desarrollar métricas para medir la contribución de TI a la empresa.	1 Informes de rendimiento del portafolio de inversiones.
		APO05.05	Mantener los portafolios.	1 Crear y mantener portafolios de programas de inversiones TI, servicios TI y activos TI. 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.	1 Portafolios de programas, servicios y activos actualizados.
		APO05.06	Gestionar la consecución de beneficios.	1 Utilizar las métricas acordadas y realizar seguimiento. 2 Implementar acciones correctivas cuando los beneficios alcanzados se desvían de los esperados. 3 Considerar obtener orientación de expertos esternos, líderes de la industria y datos de análisis comparativos para probar y mejorar las métricas y los objetivos.	1 Resultados de los beneficios y comunicaciones relacionadas. 2 Acciones correctivas para mejorar la producción de
APO06	Gestionar el Presupuesto y los Costes	APO06.01	Gestionar las finanzas y la contabilidad.	1 Definir procesos, entradas, salidas y responsabilidades de manera alineada con las políticas y el enfoque empresarial de presupuesto y contabilización de costes. 2 Definir un esquema de clasificación para identificar los elementos de coste relacionados con las TI. 3 Definir la forma de analizar, informar y utilizar el control del presupuestario. 4 Establecer y mantener prácticas para la planificiación financiera para entregar el máximo valor a la empresa con el menor gasto posible.	1 Procesos de Contabilidad 2 Esquema de clasificación de costes de TI. 3 Prácticas de planificación financiera.
		APO06.02	Priorizar la asignación de recursos.	1 Establecer un órgano de toma de decisiones para priorizar recursos de TI. 2 Establecer un procedimiento para comunicar las decisiones presupuestarias. 3 Identificar, comunicar y resolver los impactos más significativos de las decisiones presupuestarias.	1 Priorización y clasificación de las iniciativas de TI. 2 Asignaciones presupuestarias.
		APO06.03	Crear y mantener presupuestos.	1 Implememtentar un presupuesto formal de TI. 2 Indicar la necesidad de planificar presupuestos a los dueños de procesos, servicios o programas. 3 Revisar los planes de presupuesto y tomar decisiones sobre las asignaciones presupuestarias. 4 Registrar, mantener y comunicar el presupuesto actual de TI.	1 Presupuestos y plan de TI.
		APO06.04	Modelar y asignar costes.	1 Clasificar todos los costes de TI adecuadamente. 2 Definir y acordar un modelo. 3 Comunicar a los dueños de los procesos empresariales los cambios en el modelo de costes. 4 Diseñar el modelo de costes. 5 Definir y acordar un modelo.	1 Costes de TI categorizados. 2 Comunicaciones de asignación de costes. 3 Modelo de asignación de costes. 4 Procedimientos operativos.
		APO06.05	Gestionar costes.	1 Asegurar la debida autorización y la dependencia entre los responsables de los presupuestos de TI y los individuos que capturan, analizan y repostan información financiera. 2 Definir cómo se consolidan los costes para los niveles adecuados en la empresa y la forma en que se presentará a las partes interesadas. 3 Identificar a los responsables de gestión de costes que capturen, recojan y consoliden los datos, y presenten y comuniquen los datos a los pertinenetes propietarios del presupuesto. 4 Alinear los presupuestos y servicios de TI a la infraestructura de TI, procesos empresariales, y a los propietarios que los utiliza. 5 Identificar formas de optimizar los costes e introducir eficiencia sin poner en peligro los servicios.	1 Método de recolección de datos de coste. 2 Método de consolidación de costes. 3 Oportunidades de optimización de costes.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO07	Gestionar los Recursos Humanos	APO07.01	Mantener la dotación de personal suficiente y adecuada.	1 Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar que la función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos empresariales, procesos de negocio y los controles e iniciativas TI. 2 Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa. 3 Incluir controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores. 4 Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio. 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.	1 Evaluaciones de requisitos de personal 2 Planes de desarrollo de carrera y de competencias. 3 Planes de aprovisionamiento de personal
		APO07.02	Identificar personal clave de TI.	1 Minimizar la dependencia en una sola persona en la realización de una función crítica de trabajo. 2 Como medida de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que deben tomar los individuos clave. 3 Tomar acciones expeditivas con respecto a cambios laborales, especialmente despidos. 4 Probar regularmente los planes de respaldo (backup) del personal.	
		APO07.03	Mantener las habilidades y competencias del personal.	1 Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos. 2 Proporcionar una planificación formal de la carrera y desarrollo profesional fomentando el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave. 3 Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y 4 Identificar las diferencias entre las habilidades necesarias y las disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva. 5 Desarrollar y ejecutar programas de formación basados en los requisitos organizativos y de procesos, incluidos los requisitos sobre conocimiento empresarial, control interno, conducta ética y seguridad. 6 Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. 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	1 Matriz de habilidades y competencias 2 Planes de desarrollo de habilidades 3 Revisión de informes
		APO07.04	Evaluar el desempeño laboral de los empleados.	1 Considerar los objetivos funcionales de empresa como el contexto para establecer las metas 2 Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes. 3 Recopilar los resultados de la evaluación de desempeño de 360 grados. 4 Implementar y comunicar un proceso disciplinario. 5 Proporcionar retroalimentación oportuna sobre el desempeño frente a las metas del individuo. 6 Implementar un proceso de reconocimiento que premie el compromiso adecuado, el desarrollo de competencias y el logro exitoso de los objetivos de desempeño. 7 Desarrollar planes de mejora del desempeño.	1 Metas personales 2 Evaluaciones de desempeño 3 Planes de mejora
		APO07.05	Planificar y realizar un seguimiento del uso de recursos	1 Crear y mantener un inventario de recursos humanos de negocio y TI. 2 Entender la demanda actual y futura de recursos humanos para apoyar el logro de los objetivos de TI y ofrecer servicios y soluciones. 3 Identificar las carencias y proporcionar datos de entrada a planes de aprovisionamiento, así como a los procesos de contratación de TI.	

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO07	Gestionar los Recursos Humanos	APO07.06	Gestionar el personal contratado.	1 Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización y el marco de control de TI. 2 Obtener un acuerdo formal por parte de los contratistas en el inicio del contrato en cuanto a que están obligados a cumplir con el marco de control de TI de la empresa. 3 Advertir a los contratistas de que la gerencia se reserva el derecho de supervisar e inspeccionar todo uso de los recursos de TI. 4 Definir todo el trabajo a realizar por terceras partes en contratos formales y sin ambigüedades. 5 Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios. 6 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.	1 Inventario de recursos humanos del negocio y de TI. 2 Análisis de deficiencias en la obtención de recursos. 3 Registros de utilización de recursos.
APO08	Gestionar las relaciones	APO08.01	Entender las expectativas del negocio.	1 Identificar a las partes interesadas del negocio, sus intereses y sus áreas de responsabilidad. 2 Revisar la orientación de la empresa, asuntos, objetivos estratégicos actuales y alineamiento con la arquitectura empresarial. 3 Mantener atención sobre procesos de negocio y actividades asociadas, entender patrones de demanda de volumen y uso de servicios. 4 Esclarecer las expectativas del negocio para los servicios y soluciones basados en TI. 5 Confirmar el acuerdo sobre las expectativas del negocio, criterios de aceptación y métricas para las partes relevantes de la infraestructura TI. 6 Gestionar las expectativas asegurando que las unidades de negocio entienden las prioridades, dependencias, restricciones financieras y la necesidad de planificar peticiones.	1 Expectativas de negocio aclaradas y acordadas
		APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	1 Entender las tendencias tecnológicas y cómo pueden aplicarse de modo innovador para mejorar el rendimiento de los procesos de negocio. 2 Tomar un papel proactivo en identificar y comunicar a las partes interesadas clave las oportunidades, riesgos y limitaciones. 3 Asegurar que el negocio y la TI entienden y aprecian los objetivos estratégicos y la visión de la arquitectura empresarial. 4 Coordinar en la planificación de nuevas iniciativas TI para asegurar la integración y el alineamiento con la arquitectura empresarial.	1 Acuerdo en los siguientes pasos y planes de acción.
		APO08.03	Gestionar las relaciones con el negocio.	1 Asignar un responsable de la relación como punto único de contacto por cada unidad de negocio 2 Gestionar la relación de un modo formal y transparente que asegure conseguir un objetivo común. 3 Definir y comunicar un proceso de reclamaciones y escalado de las mismas para resolver cualquier incidencia en la relación. 4 Planificar interacciones específicas y calendarios basados en objetivos acordados mutuamente y en un lenguaje común. 5 Asegurar que las decisiones claves son acordadas y aprobadas por las partes interesadas responsables y relevantes.	1 Decisiones claves acordadas. 2 Estado de las quejas y del escalado.
		APO08.04	Coordinar y comunicar.	1 Coordinar y comunicar cambios y actividades de transición, actividades operativas, roles y 2 Tomar en consideración de la reacción del negocio ante eventos que puedan influenciar en la relación con el mismo. 3 Mantener un plan de comunicación extremo a extremo.	1 Paquetes de comunicación 2 Respuestas de los clientes 3 Plan de comunicación

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO09	Gestionar los acuerdos de servicio	APO09.01	Identificar servicios TI.	1 Valorar los servicios TI actuales y los niveles de servicio para identificar lagunas entre los servicios exixtentes y los procesos de negocio de los que son base. 2 Analizar, estudiar y estimar la futura demanda y confirmar la capacidad de los servicios TI existentes. 3 Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios TI nuevos o rediseñados. 4 Comparar los requisitos idenficados con los componentes del servicio existentes en el catálogo. 5 Siempre que sea posible, relacionar demanda con paquetes de servicio y crear servicios estandarizados para obtener una eficiencia global. 6 Revisar el catálogo de servicios TI para identificar servicios obsoletos.	1 Carencias identificadas de los servicios TI de cara al negocio. 2 Definición de servicios
		APO09.02	Catalogar servicios basados en TI.	1 Publicar los servicios TI, paquetes de servicio y opciones de nivel de servicio activos en la cartera de servicios en los catálogos relevantes. 2 Asegurar de forma continua que los componentes de servicio en el portafolio y en los catálogos de servicio están completos y actualizados. 3 Informar al gestor de relaciones de negocio de las actualizaciones en lo catálogos de servicios.	1 Catálogos de servicio.
		APO09.03	Definir y preparar acuerdos de servicio.	1 Analizar los requisitos para acuerdos de servicio nuevos o modificados recibidos desde la gestión de las relaciones de negocio. 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. 3 Determinar, acordar y documentar los acuerdos operativos internos para cimentar los acuerdos de servicio con clientes.	1 Acuerdos de nivel de servicio (ANSs) 2 Acuerdos de nivel operativos (OLAs)
		APO09.04	Supervisar e informar de los niveles de servicio.	1 Establecer y mantener medidas para supervisar y recolectar datos del nivel de servicio. 2 Evaluar el rendimiento y proporcionar informes regular y formalmente sobre el rendimiento del acuerdo de servicio. 3 Hacer revisiones regulares para anticipar e identificar tendencias en el rendimiento del nivel de servicio. 4 Acordar planes de acción y remedio para los incidentes del rendimiento o tendencias negativas del mismo.	1 Informes de rendimiento del nivel de servicio. 2 Planes de acción de mejora y rendimiento.
		APO09.05	Revisar acuerdos de servicio y contratos.	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 de TI, paquetes de servicio u opciones de nivel de servicio se tienen en cuenta cuando sea apropiado.	1 ANS actualizados.
APO11	Gestionar la Calidad	APO11.01	Establecer un sistema de gestión de la calidad (SGC).	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 calidad. 2 Definir roles, tareas, capacidades de decisión y responsabilidades para la gestión de la calidad, dentro de la estructura organizativa. 3 Definir planes de gestión de calidad para los procesos, proyectos u objetivos importantes. 4 Supervisar y medir la eficiencia y la aceptación de la gestión de la calidad y mejorarla cuando sea 5 Obtener los inputs necesarios de las partes interesadas internas y externas para definir requisitos y criterios de aceptación de la calidad. 6 Comunicar de manera eficaz el enfoque. 7 Revisar periódicamente la relevancia, eficiencia y eficacia de los procesos específicos de gestión de	1 Roles, responsabilidades y capacidades de decisión del SGC. 2 Planes de gestión de la 3 Resultados de las revisiones de eficacia del SGC.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO11	Gestionar la Calidad	APO11.02	Definir y gestionar estándares, proceso y prácticas de calidad.	1 Definir las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI. 2 Considerar los costes y los beneficios de las certificaciones de calidad.	1 Estándares de gestión de la calidad.
		APO11.03	Enfocar la gestión de la calidad en los clientes.	1 Enfocar la gestión de la calidad en los clientes, mediante la determinación de requisitos de los clientes internos y externos. 2 Gestionar las necesidades y las expectativas del negocio para cada proceso de negocio, servicio operativo y nuevas soluciones de TI. 3 Comunicar los requisitos y expectativas del cliente por toda la organización de negocio y de TI. 4 Supervisar y revisar regularmente que el SGC está de acuerdo a los criterios de aceptación de la 5 Capturar criterios de aceptación de calidad para su inclusión en los ANS.	1 Criterios de aceptación. 2 Revisión de los resultados de la calidad de los servicios. 3 Requisitos de los clientes para la gestión de la calidad.
		APO11.04	Supervisar y hacer controles y revisiones de calidad.	1 Supervisar la calidad de los procesos y servicios de forma permanente y sistemática. 2 Prepara y llevar a cabo revisiones de calidad. 3 Informar de los resultados de las revisiones y poner en marcha las mejoras necesarias. 4 Supevisar la calidad de procesos y el valor proporcionado por la calidad.	1 Resultados de las revisionees y auditorias de calidad. 2 Metas y métricas del proceso de calidad de los servicios.
		APO11.05	Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	1 Integrar las prácticas de gestión de calidad en los procesos y prácticas de desarrollo de soluciones. 2 Supervisar continuamente los niveles de servicio e incorporar prácticas de gestión de calidad en todos los procesos y prácticas de prestación de servicios. 3 Identificar y documentar las causas raíz de las no conformidades y comunicar los resultados a la dirección de TI y otras partes interesadas.	1 Resultados de la supervisión de la calidad de los servicios y las soluciones entregadas. 2 Causas raíz de los fallos en la entrega de calidad.
		APO11.06	Mantener una mejora continua.	1 Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua. 2 Establecer una plataforma para compartir las mejores prácticas e información sobre los defectos y errores que permita aprender de ellos. 3 Identificar ejemplos recurrentes de los defectos de calidad. 4 Identificar ejemplos de procesos excelentes de prestación de calidad que pueden beneficiar a otros servicios o proyectos. 5 Promover una cultura de calidad y mejora continua. 6 Establecer un circuito de retroalimentación entre la gestión de la calidad y la gestión de problemas.	1 Comunicaciones sobre las mejores prácticas y la mejora continua. 2 Ejemplos de las mejores prácticas para ser compartidas. 3 Resultados de revisiones de análisis comparativos de la
APO12	Gestionar el Riesgo	APO12.01	Recopilar datos	1 Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI. 2 Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas. 3 Registrar datos de eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI. Destacar factores contribuyentes. 4 Determinar las condiciones específicas que existían o faltaban cuando cuando ocurrieron los eventos de riesgo. 5 Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo.	1 Datos en el entorno de operación relacionados con el riesgo. 2 Datos en eventos de riesgo y en factores contribuyentes. 3 Elementos y factores de riesgo emergentes.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO12	Gestionar el Riesgo	APO12.02	Analizar el riesgo.	1 Definir la amplitud y profundidad para los esfuerzos en análisis de riesgos. 2 Construir y actualizar regularmente escenarios de riesgo de TI. 3 Estimular la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. 4 Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial. Proponer la respuesta al riesgo óptima. 5 Especificar requerimientos de alto nivel para proyectos o programas que implementarán las respuestas de riesgo seleccionadas. 6 Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones.	1 Alcance de los esfuerzos de análisis de riesgos. 2 Escenarios de riesgo de TI 3 Resultados de análisis de riesgos.
		APO12.03	Mantener un perfil de riesgo	1 Inventariar procesos de negocio y documentar la dependencia de procesos de gestión de servicio TI y de recursos de infraestructuras TI. 2 Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. 3 Agregar escenarios de riesgo actuales. 4 Definir un conjunto de indicadores de riesgo que permitan la identificación rápida y supervisión del riesgo actual.	1 Escenarios de riesgo documentados por línea de negocio y función 2 Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo
		APO12.04	Expresar el riesgo.	1 Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas. 2 Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable. 3 Informar el perfil de riesgo actual a todas las partes interesadas. 4 Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisisones del aseguramiento de calidad y mapearlos con el perfil de riesgo. 5 Para áreas con un riesgo relativo, identificar oportunidades relaciondas con TI, que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.	1 Análisis de riesgos e informes del perfil de riesgos para las partes interesadas. 2 Revisión de resultados de evaluaciones de riesgos de terceras partes. 3 Oportunidades para la aceptación de un riesgo mayor.
		APO12.05	Definir portafolio de acciones para la gestión de riesgos.	1 Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo. 2 Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos.	1 Propuestas de proyecto para reducir el riesgo.
		APO12.06	Responder al riesgo.	1 Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo. 2 Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. 3 Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.	1 Planes de respuesta para incidentes de riesgo. 2 Comunicaciones del impacto del riesgo. 3 Causas raíz relacionadas con el riesgo.
APO13	Gestionar la Seguridad	APO13.01	Establecer y mantener un SGSI.	1 Definir el alcance y los límites del SGSI. 2 Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología. 3 Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa. 4 Obtener autorización de la dirección para implementar y operar o cambiar el SGSI. 5 Prepara y mantener una declaración de aplicabilidad que describa el alcance del SGSI. 6 Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información. 7 Comunicar el enfoque del SGSI.	1 Política de SGSI 2 Declaración de alcance del SGSI.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
APO13	Gestionar la Seguridad	APO13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	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. 2 Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa. 3 Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la 4 Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información. 5 Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas. 6 Recomendar programas de formación y concienciación en seguridad de la información. 7 Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles.	1 Plan de tratamiento de riesgos de seguridad de la 2 Casos de negocio de seguridad de información.
		APO13.03	Supervisar y revisar el SGSI.	1 Realizar revisiones periódicas del SGSI. 2 Realizar auditoria internas al SGSI a intervalos planificados. 3 Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI. 4 Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica. 5 Registrar las acciones y los eventos que podrían tener un impacto en la efectiviade o el desempeño	1 Informes de auditoría del SGSI. 2 Recomendaciones para mejorar el SGSI.
BAI02	Gestionar la Definición de Requisitos	BAI02.01	Definir y mantener los requerimientos técnicos y funcionales del negocio.	1 Definir e implementar la definición de requerimientos y el procedimiento de mantenimiento y un repositorio de requisitos. 2 Expresar los requerimientos de la empresa en términos de cómo la diferencia entre las capacidades de negocio exixtentes y deseadas son tratadas y como cada rol interactuará con la solición y la utilizará. 4 Especificar y priorizar la información, los requerimientyos técnicos y funcionales basados en los requerimientos de las partes interesadas. 5 Validar todos los requerimientos mediante aproximaciones tales como revisón por iguales, validación del modelo o prototipo operativo. 6 Confirmar la aceptación de aspectos clave de los requerimientos. 7 Hacer seguimiento y controlar el alcance, los requerimientos y los cambios a lo largo del ciclo de vida de la solución. 8 Considerar los requerimientos relativos a políticas y estándares empresariales, arquitectura empresarial, planes TI estratégicos y tácticos, procesos de TI internos y externalizados, requerimientos de seguridad, requerimientos regulatorios, competencias del personal, estructura organizativa, caso de negocio y tecnologias catalizadoras.	1 Repositorio de definición de requerimientos. 2 Confirmación de los criterios de aceptación de las partes interesadas. 3 Registro de las peticiones de cambios de los requerimientos.
		BAI02.02	Realizar un estudio de viabilidad y proponer soluciones alternativas.	1 Definir y ejecutar un estudio de viabilidad, piloto que clara y concisamente describa las soluciones laternativas que satisfagan los requerimientos funcionales y de negocio. 2 Identificar las acciones requeridas para la adquisición o desarrollo de la solución, basada en la arquitectura de la empresa. 3 Revisar las soluciones alternativas con todas las partes interesadas y seleccionar la más apropiada basada en criterios de viabilidad incluyendo costes y riesgos. 4 Traducir la línea de acción preferida a un plan de alto nivel de adquisición/desarrollo identificando recursos a utilizar y fases que requieran decisiones de continuar/no continuar.	1 Informe de estudio de viabilidad. 2 Plan de alto nivel de adquisiciones/desarrollo.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI02	Gestionar la Definición de Requisitos	BAI02.03	Gestionar los riesgos de los requerimientos.	1 Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información. 2 Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto. 3 Identificar modos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de	1 Registro de riesgos de los requerimientos. 2 Acciones de mitigación de
		BAI02.04	Obtener la aprobación de los requerimientos y soluciones.	1 Asegurar que el patrocinador de negocio o propietario del producto toman la decisión final con respecto a la elección de la solución, enfoque de adquisición y diseño acorde al caso de negocio. 2 Obtener revisiones de calidad completas y de cada fase clave de proyecto, iteración o versión comparando los resultados obtenidos contra los criterios originales de acpetación.	1 Aprobaciones del patrocinador de requerimientos y soluciones propuestas. 2 Aprobación de las revisiones de calidad.
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.01	Diseñar soluciones de alto nivel.	1 Establecer especfiicaciones de diseño a alto nivel. 2 Involucrar a usuarios experimentados y apropiadamente cualificados así como especialistas TI en el proceos de diseño. 3 Crear un diseño acorde a los estándares de diseño de la organización. 4 Remitir el diseño final a alto nivel del proyecto a las partes interesadas y al patrocinador/dueño del proceso de negocio para su aprobación.	1 Aprobación de las especificaciones del diseño de alto nivel.
		BAI03.02	Diseñar los componentes detallados de la solución.	1 Diseñar las actividades del proceso de negocio y los flujos de trabajo necesarios. 2 Diseñar las etapas de procesamiento de la aplicación. 3 Clasificar las entradas y salidas de datos acorde a los estándares de arquitectura empresarial. 4 Diseñar el interfaz del sistema/solución. 5 Diseñar el almacenamiento de los datos, localización y capacidad de recuperación. 6 Diseñar la redundacnia, recuperación y copia de seguridad apropiadas. 7 Diseñar el interfaz entre el usuario y la apliación del sistema para que sea fácil de usar y sea auto 8 Considerar el impacto de las necesidades de la solución en el rendimiento de la infraestructura. 9 Evaluar proactivamente las debilidades del diseño a través de todo el ciclo de vida, identificando mejorar cuando se requiera. 10 Proporcionar métodos para auditar las transacciones e identificar la causa raíz de los problemas en el procesamiento.	1 Especificaciones de diseño detalladas y aprobadas. 2 ANSs y OLAs
		BAI03.03	Desarrollar los componentes de la solución.	1 Desarrollar los procesos de negocio, servicios de soporte, aplicaciones e infraestructura y repositorios de información. 2 Cuando proveedores terceros desarrollen la solución, asegurar que el mantenimiento, soporte, estándares y licenciamiento están contempladas en las obligaciones contractuales. 3 Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas. 4 Evaluar el impacto de la personalización de la solución y la configuración en el rendimiento y eficiencia de las soluciones adquiridas.	1 Documentar los componentes de la solución.
		BAI03.04	Obtener los componentes de la solución.	1 Crear y mantener un plan de adquisiciones de los componentes de la solución. 2 Revisar y aprobar todos los planes de adqusiciones. 3 Evaluar y documentar en qué grado las soluciones adquiridas requieren adaptación a los procesos de negocio para aprovechar sus beneficios. 4 Registrar los recibos de todas las adquisiciones realizadas de software e infraestructura en el inventario de activos.	1 Plan de adquisiciones aprobado. 2 Actualizaciones del inventario de activos.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.05	Construir soluciones.	1 Integrar y configurar los componentes de la solución TI y de negocio. 2 Implementar pistas de auditoría durante la configuración e integración del hardware e infraestructura del software. 3 Asegurar la interoperabilidad de los componentes de la solución econ las pruebas de soporte preferiblemente automatizadas. 4 Configurar que el software de aplicación adquirido cumple con los requerimientos de proceso de 5 Definir el catálogo de servicios para los objetivos basados en los requerimientos de negocio.	1 Componentes de la solución integrados y configurados.
		BAI03.06	Realizar controles de calidad.	1 Definir un plan de calidad (QA) y prácticas. 2 Supervisar frecuentemente la solución de calidad. 3 Utilizar apropiadamente inspección de código, pruebas conducidas sobre el desarrollo, pruebas automatizadas, integración continua, revisiones y pruebas sobre aplicaciones. 4 Supervisar todas las excepciones de calidad y tratar todas las acciones correctivas.	1 Plan de aseguramiento de la calidad (QA). 2 Resultados de la revisión de calidad, excepciones y correcciones.
		BAI03.07	Preparar pruebas de la solución.	1 Crear un plan de pruebas integradas y prácticas acordes al entorno de la empresa y planes estratégicos de tecnología. 2 Crear un entorno de pruebas que soporte el alcance completo de la solución. 3 Crear procedimientos de prueba alineados con el plan y las prácticas y que permitan la evaluación operativa de la solución en condiciones reales.	1 Plan de pruebas 2 Procedimientos de pruebas.
		BAI03.08	Ejecutar pruebas de la solución.	1 Realizar las pruebas de las soluciones y sus componentes. 2 Utilizar instrucciones de pruebas claramente definidas. 3 Realizar todas las pruebas conforme el plan y prácticas de pruebas. 4 Identificar, registrar y clasificar los errores durante las pruebas. 5 Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas.	1 Registros de resultados de pruebas y pistas de auditoría. 2 Comunicaciones del resultado de las pruebas.
		BAI03.09	Gestionar cambios a los requerimientos.	1 Evaluar el impacto de todas las peticiones de cambio de la solución en su desarrollo, en el caso de negocio original y en el presupuesto, y categorizar y priorizar las peticiones convenientemente. 2 Hacer seguimiento de los requerimientos. 3 Aplicar las peticiones de cambio, manteniendo la integridad de la integración y configuración de los componentes de la solución.	1 Registro de todas las peticiones de cambio aprobadas y aplicadas.
		BAI03.10	Mantener soluciones.	1 Desarrollar y ejecutar un plan de mantenimiento de los componentes de la solución. 2 Evaluar la significatividad de las actividades de mantenimiento propuestas sobre el diseño de la solución, funcionalidad y/o procesos de negocio actuales. 4 Asegurar que el patrón y volumen de las actividades son analizadas periódicamente para buscar tendencias anormales. 5 Para actualizaciones de mantenimiento, utilizar el proceso de gestión de cambio paa controlar todas las peticiones de mantenimiento.	1 Plan de mantenimiento 2 Componentes de la solución actualizados y documentación relacionada.
		BAI03.11	Definir los servicios TI y mantener el catálogo de servicios.	1 Proponer definiciones de los nuevos o modificados servicios TI que aseguren que los servicios cumplen con el propósito. 2 Proponer cambios o nuevas opciones de niveles de servicios para asegurar que los servicios TI son adecuados para su uso. 3 Intermediar con le gestor de relaciones de negocio y el gestor del portafolio para acordar las definiciones y opciones de niveles de servicio.	1 Definiciones de servicio 2 Catálogo de servicios actualizado.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.01	Establecer el deseo de cambiar.	1 Evaluar el alcance y el impacto del cambio divisado, las diferentes partes interesadas que se verán afectadas, la naturaleza del impacto y la involucración necesaria. 2 Identificar, impulsar y comunicar puntos de conflicto, eventos negativos, riesgos, insatisfacción de clientes y problemas del negocio, así como beneficios iniciales, oportunidades y ventajas 3 Emitir las comunicaciones clave del Comité Ejecutivo o el Director General Ejecutivo para demostrar el compromiso con el cambio.	1 Comunicaciones de los motivadores del cambio. 2 Comunicaciones de la dirección ejecutiva comprometiendo se con el cambio.
		BAI05.02	Formar un equipo de implementación efectivo.	1 Identificar y montar un equipo de implementación principal efectivo que incluya miembros adecuados de TI y del negocio. 2 Crear confianza dentro del equipo de implementación principal mediante eventos planificados cuidadosamente con comunicación y actividades conjuntas efectivas. 3 Desarrollar una visión y metas comunes que soporten los objetivos empresariales.	1 Equipo de implementación y roles 2 Visión y objetivos comunes
		BAI05.03	Comunicar la visión deseada.	1 Desarrollar un plan de comunicación de la visión para abordar a los grupos de audiencia principales. 2 Realizar la comunicación a niveles adecuados de la empresa. 3 Reforzar la comunicación mediante repetición y múltiples foros. 4 Verificar la comprensión de la visión deseada y dar respuesta a cualquier cuestión del personal. 5 Hacer responsables a todos los niveles de liderazgo para demostrar la visión.	1 Plan de comunicación de la visión. 2 Comunicaciones de la visión.
		BAI05.04	Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.	1 Identificar estructuras organizativas compatibles con la visión; si fuera necesario, realizar cambios para asegurar el alineamiento. 2 Planificar las necesidades de formación del personal para desarrollar las habilidades y actitudes adecuadas para que se sientan facultados. 3 Alinear los procesos de RRHH y sistemas de mediciónpara dar soporte a la visión. 4 Identificar y gestionar líderes que continúen resistiéndose a la necesidad de cambio. 5 Identificar, priorizar y proveer oportunidades de victorias rápidas (quick-wins). 6 Aprovechar las victorias rápidas para mostrar que la visión en el buen camino.	1 Metas de desempeño de RRHH alineadas 2 Beneficios en el corto plazo (quick-wins) identificados 3 Comunicación de los beneficios
		BAI05.05	Facilitar la operación y el uso.	1 Desarrollar un plan de operación y uso del cambio que comunique y se base en las mejoras inmediatas que se hayan percibido. 2 Implementar el plan de operación y uso. Definir y registrar métricas de éxito.	1 Resultados y métricas de éxito. 2 Plan de operación y uso.
		BAI05.06	Integrar nuevos enfoques.	1 Reconocer los éxitos e implementar programas de recompensa y reconocimiento para reforzar el proceso de cambio. 2 Usar sistemas de medida del desempeño para identificar las causas raíz de una baja adopción de los cambios y aplicar medidas correctoras. 3 Hacer responsables a los propietarios de proceso de que se hagan todas las operaciones propias del día a día. 4 Llevar a cabo auditorías de cumplimiento para identificar las causas raíz de una baja adopción de los cambios y recomendar acciones correctivas.	1 Resultados de auditorías de cumplimiento 2 Comunicaciones de concienciación. 3 Resultados de la revisión. de rendimiento de RRHH
		BAI05.07	Mantener los cambios.	1 Proporcionar tutoría, formación, entrenamiento y transferencia de conocimiento al personal nuevo para mantener los cambios. 2 Mantener y reforzar los cambios mediante comunicaciones regulares . 3 Realizar revisiones periódicas de la operación y uso de los cambios e identificar mejoras. 4 Captar lecciones aprendidas sobre la implementación de los cambios y divulgar este conocimiento.	1 Planes de transferencia del conocimiento. 2 Comunicación del compromiso de la Dirección. 3 Revisión del uso operativo.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI06	Gestionar los Cambios	BAI06.01	Evaluar, priorizar y autorizar peticiones de cambio.	1 Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones.	1 Evaluaciones de impacto 2 Peticiones de cambio aprobadas. 3 Plan de cambio y cronograma.
				2 Categorizar las peticiones de cambio y relacionarlas con los elementos de configuración afectados.	
				3 Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el	
				4 Planificar y evaluar todas las peticiones de una manera estructurada.	
				5 Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado.	
				6 Planificar y programar todos los cambios aprobados.	
				7 Considerar el impacto en los proveedores de servicios en el proceso de gestión del cambio.	
		BAI06.02	Gestionar cambios de emergencia.	1 Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.	1 Revisión de cambios de emergencia tras su implementación.
				2 Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.	
				3 Supervisar todos los cambios de emergencia y realizar revisiones post-implantación involucrando a todas las partes interesadas.	
				4 Definir qué constituye un cambio de emergencia.	
		BAI06.03	Hacer seguimiento e informar de cambios de estado.	1 Categorizar las peticiones de cambio en el proceso de seguimiento.	1 Reporte del estado de cambio de una petición.
				2 Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global.	
				3 Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.	
				4 Mantener un sistema de seguimiento e informe para todas las peticiones de cambio.	
		BAI06.04	Cerrar y documentar los cambios.	1 Incluir los cambios en la documentación en el procedimiento de gestión del cambio.	1 Documentación del cambio.
				2 Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación de usuario.	
				3 Someter a la documentación a la misma revisión que al cambio en sí mismo.	
BAI08	Gestionar el conocimiento	BAI08.01	Cultivar y facilitar una cultura de intercambio de conocimientos.	1 Comunicar proactivamente el valor del conocimiento para impulsar la creación, uso, reutilización y compartición de conocimiento.	1 Comunicaciones sobre el valor del conocimiento.
				2 Impulsar la compartición y transferencia de conocimiento mediante la identificación de factores que fluyan en la motivación.	
				3 Crear un entorno, herramientas y elementos que den soporte a la compartición y transferencia de conocimientos.	
				4 Integrar prácticas de gestión del conocimiento en otros procesos de TI.	
				5 Establecer expectativas de la Dirección y demostrar la actitud adecuada acerca de la utilidad del conocimiento y la necesidad de compartir el conocimiento corporativo.	
		BAI08.02	Identificar y clasificar las fuentes de información.	1 Identificar usuarios potenciales de conocimiento, incluyendo propietarios de información que pueden necesitar contribuir y aprobar conocimiento.	1 Clasificación de fuentes de información.
				2 Considerar tipos de contenidos, elementos e información estructurada y no estructurada.	
				3 Clasificar las fuentes de información basándose en un esquema de clasificación de contenido.	
				4 Recoger, poner en orden y validar las fuentes de información.	

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI08	Gestionar el conocimiento	BAI08.03	Organizar y contextualizar la información, transformándola en conocimiento.	1 Identificar atributos compartidos y casar fuentes de información, creando relaciones entre conjunto de información.	1 Repositorios de información publicada.
				2 Crear vistas para conjuntos de datos relacionados, considerando reqsuisitos oprganizativos y de las partes interesadas.	
				3 Concebir e implantar un esquema para gestionar la información no estructurada que no esté disponible a partir de fuentes de información.	
				4 Publicar y hacer acceso el conocimiento a las partes interesadas relevantes, basándose en roles y mecanismos de acceso.	
		BAI08.04	Utilizar y compartir el conocimiento.	1 Identificar usuarios potenciales de conocimiento mediante la clasificación de la información.	1 Base de datos de usuarios de conocimiento
				2 Transferir el conocimiento a los usuarios de conocimientos basándose en un análisis de necesidades, técnicas de aprendizaje efectivas y herramientas de acceso.	
				3 Educar y entrenar a los usuarios en el conocimiento dispoble, en el acceso al conocimiento y en el uso de herramientas de acceso al conocimiento.	2 Esquemas de concienciación y formación de conocimiento.
		BAI08.05	Evaluar y retirar la información.	1 Medir el uso y evaluar la utilidad, relevancia y valor de los elementos de conocimiento.	1 Resultados de la evaluación de uso y retirada del conocimiento.
				2 Definir las reglas para la retirada de conocimiento y retirar el mismo de forma acorde.	2 Reglas para la retirada de conocimiento.
BAI09	Gestionar los Activos	BAI09.01	Identificar y registrar activos	1 Identificar todos los activos en un registro que indique el estado actual.	1 Registro de activos
				2 Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.	2 Resultados de comprobaciones físicas de inventario.
				3 Verificar la existencia de todos los activos mediante la realización periódica de controles de inventario físicos y lógicos y su conciliación.	
				4 Comprobar que los activos se adecuan a sus objetivos.	3 Resultados de revisiones de adecuación al objetivo.
				5 Determinar de forma regular si cada activo continúa proporcionando valor.	
				6 Asegurar la contabilización de todos los activos.	
		BAI09.02	Gestionar activos críticos	1 Identificar los activos que son críticos en la provisión de la capacidad del servicio refiriéndose a los requisitos en las definiciones de servicio, ANSs y el sistema de gestión de la configuración.	1 Comunicación de tiempo de inactividad planificado para mantenimiento.
				2 Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes.	2 Contratos de mantenimiento.
				3 Considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico.	
				4 Mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, supervisión del rendimiento.	
				5 Establecer un plan de mantenimiento preventivo para todo el hardware.	
				6 Comunicar a los clientes y los usuarios afectados el impacto esperado de las actividades de	
				7 Asegurar que los servicios de acceso remoto y perfiles de usuario están activos sólo cuando sea necesario.	
				8 Incorporar el tiempo de inactividad previsto en general en el calendario de producción, y programar las actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio.	

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI09	Gestionar los Activos	BAI09.03	Gestionar el ciclo de vida de los activos.	1 Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa. 2 Identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico. 3 Aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por 4 Desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación. 5 Asignar activos a los usuarios, con aceptación y firma de responsabilidades, según corresponda. 6 Eliminar los activos cuando no sirvan a ningún propósito útil. 7 Planificar, autorizar y realizar las actividades relacionadas con la finalización de uso, manteniendo los registros apropiados para satisfacer las necesidades regulatorias y cambiantes del negocio.	1 Solicitudes de adquisición de activos aprobadas. 2 Registro de activos actualizado. 3 Retirada autorizada de activos.
		BAI09.04	Optimizar el coste de los activos.	1 Revisar la base general de activos de forma regular, teniendo en cuenta si está alineada con los requerimientos del negocio. 2 Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor 3 Revisar las garantías y considerar la relación calidad-precio y estrategias de reemplazo para determinar opciones de menor coste. 4 Revisar la base general para identificar oportunidades de normalización, abastecimiento único y otras estrategias que pueden disminuir los costes de adquisición, soporte y mantenimiento. 5 Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes. 6 Revisar el estado general para identificar las oportunidades para aprovechar tecnologías emergentes o estrategias de aprovisionamiento alternativas para reducir los costes o incrementar el valor del	1 Resultados de las revisiones de optimización de costes. 2 Oportunidades para reducir el coste de activos o aumentar su valor.
		BAI09.05	Administrar licencias.	1 Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia 2 De forma regular, llevar a cabo una auditoría para identificar a todos las copias de software instalado con licencia. 3 Comparar el número de copias de software instalado con el número de licencias en propiedad. 4 Cuando las copias sean inferiores al número en propiedad, decidir si existe una necesidad de mantener o cancelar licencias. 5 Cuando las copias sean superiores al número en propiedad, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas. 6 De forma regular, considerar si se puede obtenerse un mejor valor mediante la actualización de productos y licencias asociadas.	1 Registro de licencias de 2 Resultado de auditorías de licencias instaladas. 3 Plan de acción para ajustar el número de licencias y su asignación.
BAI10	Gestionar la Configuración	BAI10.01	Establecer y mantener un modelo de configuración.	1 Definir y acordar el alcance y nivel de detalle para la gestión de la configuración. 2 Establecer y mantener un modelo lógico para la gestión de la configuración.	1 Ámbito de aplicación del modelo de gestión de la 2 Modelo de configuración lógica.
		BAI10.02	Establecer y mantener un repositorio de configuración y una base de referencia.	1 Identificar y clasificar los elementos de configuración y rellenar el repositorio. 2 Crear, revisar y formalizar un acuerdo sobre las bases de referencia de configuración de un servicio, aplicación o infraestructura.	1 Repositorio de Configuración. 2 Base de Referencia de configuración.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
BAI10	Gestionar la Configuración	BAI10.03	Mantener y controlar los elementos de configuración.	1 Identificar regularmente todos los cambios en los elementos de configuración.	1 Repositorio actualizado con los elementos de configuración.
				2 Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.	
				3 Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.	2 Cambios aprobados a la base de referencia.
				4 Crear, revisar y formalizar acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.	
		BAI10.04	Generar informes de estado y configuración.	1 Identificar cambios en el estado de los elementos de configuración y contrastarlo con la base de referencia.	1 Informes de estado de configuración
				2 Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado.	
				3 Identificar requisitos de información de todas las partes interesadas, incluyendo contenido, frecuencia y medios.	
		BAI10.05	Verificar y revisar la integridad del repositorio de configuración.	1 Verificar periódicamente los elementos de configuración en activo.	1 Resultados de la verificación física de elementos de configuración.
				2 Informar y revisar todas las desviaciones de las correcciones o acciones aprobadas para eliminar los activos no autorizados.	
				3 Verificar periódicamente que todos los elementos físicos de configuración, tal como se definen en el repositorio, existen físicamente. Informar de cualquier desviación a la Dirección.	2 Desviaciones de licencias.
				4 Establecer y revisar periódicamente el objetivo de completitud del repositorio de configuración basado en las necesidades del negocio.	3 Resultados de exámenes de completitud del repositorio.
				5 Periódicamente comparar el grado de completitud y precisión respecto a los objetivos y tomar medidas correctivas, según sea necesario, para mejorar la calidad de los datos del repositorio.	
MEA01	Gestionar la Definición de Requisitos	MEA01.01	Establecer un enfoque de la supervisión.	1 Identificar las partes interesadas.	1 Requisitos de supervisión.
				2 involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidadción e información.	
				3 Mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía.	2 Métricas y objetivos de supervisión aprobado.
				4 Solicitar, priorizar y reservar recursos para la supervisión.	
				5 Validar periódicamente el enfoque utilizando e identificar los nuevos o cambiantes grupos de interés, requisitos y recursos.	
		MEA01.02	Establecer los objetivos de cumplimiento y rendimiento.	1 Definir y revisar periódicamente los objetivos y métricas con las partes interesadas.	1 Objetos de supervisión.
				2 Comunicar los cambios propuestos en las metas y tolerancias de rendimiento y cumplimiento con las partes interesadas clave.	
				3 Hacer público a los usuarios de la información los cambios en metas y tolerancias.	
				4 Evaluar si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART)	
		MEA01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	1 Recopilar datos de los procesos definidos, de forma automatizada.	1 Datos de supervisión procesados
				2 Evaluar la eficiencia y oportunidad y validar la integridad de los datos recopilados.	
				3 Consolidar los datos para soportar el cálculo de las métricas acordadas.	
				4 Utilizar herramientas y sistemas apropiados para el procesamiento y formateo de datos para análisis.	

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
MEA01	Gestionar la Definición de Requisitos	MEA01.04	Analizar e informar sobre el rendimiento.	1 Diseñar informes de rendimiento de procesos que sean concisos y ajustados a las diferentes necesidades de gestión y audiencias. 2 Comparar los valores de rendimiento con metas y estudios comparativos internos y cuando sea posible, con estudios comparativos externos. 3 Recomendar cambios a los objetivos y métricas, cuando sea procedente. 4 Distribuir los informes a las partes interesadas relevantes. 5 Analizar la causa de las desviaciones respecto a las metas, iniciar acciones correctivas. 6 Cuando sea factible, enlazar el cumplimiento de objetivos de desempeño con el sistema de compensación y gratificación de la organización.	1 Informes de desempeño.
		MEA01.05	Asegurar la implantación de medidas correctivas.	1 Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores. 2 Asegurar que se mantiene la asignación de responsabilidades en las acciones correctivas. 3 Hacer seguimiento de los resultados de las acciones comprometidas. 4 Informar de los resultados a las partes interesadas.	1 Acciones y asignaciones. correctivas 2 Estado y resultado de las
MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	MEA02.01	Supervisar el control interno.	1 Realizar actividades de evaluación y supervisión del control interno basadas en estándares de gobierno organizativos, marcos y prácticas aceptadas en la industria. 2 Considerar las evaluaciones independientes del sistema de control internO. 3 Identificar los límites del sistema de control interno de TI. 4 Asegurar que las actividades de control están operativas y que las excepciones son comunicadas puntualmente, seguidas y analizadas. 5 Mantener el sistema de control interno de TI. 6 Evaluar regularmente el rendimiento del marco de control de TI. 7 Evaluar el estado de los controles internos de los proveedores externos de servicios.	1 Resultados de las revisiones y supervisión del control interno. 2 Resultados de estudios comparativos y otras evaluaciones.
		MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	1 Entender y priorizar el riesgo de acuerdo con los objetivos organizativos. 2 Identificar los controles clave y desarrollar una estrategia adecuada para la validación de controles. 3 Identificar la información que indica de forma convincente si el entorno de control interno está operando de forma efectiva. 4 Desarrollar e implementar procedimientos eficientes para determinar si la información convincente está basada en criterios de información. 5 Mantener evidencia de la efectividad del control.	1 Evidencia de la efectividad del control.
		MEA02.03	Realizar autoevaluaciones de control.	1 Mantener planes y alcances e identificar los criterios de evaluación para la realización de las autoevaluaciones. 2 Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectiviada y eficiencia conjuntas de la supervisión continua. 3 Asignar la responsabilidad de la autoevaluación a las personas oportunas con el fin de asegurar la objetividad y la competencia. 4 Proporcionar revisiones independientes paa asegurar la objetividad de la autoevaluación. 5 Resumir y comunicar los resultados de las autoevaluaciones y los estudios comparativos para considerar acciones correectivas. 6 Definir un enfoque consistente y consensuado para la realización de autoevaluaciones de control y coordinación con auditores internos y externos.	1 Planes y criterios de autoevaluación. 2 Resultados de las autoevaluaciones. 3 Resultados de las revisiones de las autoevaluaciones.

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	MEA02.04	Identificar y comunicar las deficiencias de control.	1 Identificar, comunicar y registrar las excepciones de los controles y asigar responsabilidad de su resolución y comunicación de los resultados. 2 Considerar el riesgo para la empresa al establecer umbrales para el escalado de las excepciones y desajustes de los controles. 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. 4 Decidir qué excepciones de control deberían ser comunicadas a la persona responsable de la función y que excepciones debería ser escaladas. 5 Hacer seguimiento de todas las excepciones para asegurar que se han completado las acciones acordadas. 6 Identificar, iniciar, rastrear e implementar acciones correctivas que surjan de la evaluación de contrtol e informes.	1 Deficiencias de control 2 Acciones correctivas
		MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	1 Establecer adhesión a los códigos de ética y estándares aplicables y estándarres de aseguramiento. 2 Establecer la independencia de los proveedores de aseguramiento. 3 Establecer la competencia y cualificación de los proveedores de aseguramiento.	1 Resultados de las evaluaciones del proveedor de aseguramiento.
		MEA02.06	Planificar iniciativas de aseguramiento.	1 Determinar los destinatarios de las salidas de la iniciativa de aseguramiento y el objeto de la revisión. 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. 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.	
		MEA02.07	Estudiar las iniciativas de aseguramiento.	1 Definir el alcance actual. 2 Definir el plan de participación y los recursos necesarios. 3 Definir las prácticas de recolleción y evaluación de la información de los procesos bajo revisión. 4 Definir prácticas para validar el diseño de controles y resultados y determinar si el nivel de efectividad es compattible con el riesgo aceptable. 5 Donde la efectiviadad del control no es aceptable, definir prácticas para identificar el riesgo residual.	1 Evaluaciones de alto nivel 2 Planes de aseguramiento. 3 Criterios de evaluación
		MEA02.08	Ejecutar las iniciativas de aseguramiento.	1 Refinar la comprensión en materia de aseguramiento de TI. 2 Refinar el alcance de los objetivos de control clave en materia de aseguramiento de TI. 3 Probar la efectividad del diseño de control de los objetivos clave de control. 4 Alternativamente/adicionalmente probar los resultados de los objetivos clave de control. 5 Documetnar el impacto de las debilidades de control. 6 Supervisar las actividades de aseguramiento y asegurar que el trabajo realizado está completo, cumple con sus objetivos y tiene una calidad aceptables. 7 Proveer a la Dirección de un informe que resplade los resultados de la iniciativa y haga hincapié en las cuestiones clave y las acciones importantes.	1 Alcance de la revisión del aseguramiento 2 Plan de participación 3 Prácticas de revisión del aseguramiento

ID proceso	Nombre proceso	ID práctica	Nombre práctica	ACTIVIDADES	SALIDAS
		MEA02.08	Ejecutar las iniciativas de aseguramiento.	2 Refinar el alcance de los objetivos de control clave en materia de aseguramiento de TI. 3 Probar la efectividad del diseño de control de los objetivos clave de control. 4 Alternativamente/adicionalmente probar los resultados de los objetivos clave de control. 5 Documetnar el impacto de las debilidades de control. 6 Supervisar las actividades de aseguramiento y asegurar que el trabajo realizado está completo, cumple con sus objetivos y tiene una calidad aceptables. 7 Proveer a la Dirección de un informe que resplade los resultados de la iniciativa y haga hincapié en las cuestiones clave y las acciones importantes.	del aseguramiento 2 Plan de participación 3 Prácticas de revisión del aseguramiento
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	MEA03.01	Identificar requisitos externos de cumplimiento.	1 Asignar 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 2 Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de TI. 3 Valorar el impacto de los requisitos legales 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. 4 Obtener asesoramiento independiente, si procede, sobre notificaciones en legislaciones, regulaciones y estándares aplicables. 5 Mantener un inventario actualizado de requisitos legales, regulatorios y contractuales aplicables, su impacto y las acciones necesarias. 6 Mantener un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa.	1 Registro de requisitos de cumplimiento. 2 Inventario de acciones de cumplimiento necesarias.
		MEA03.02	Optimizar la respuesta a requisitos externos.	1 Revisar y ajustar con regularidad políticas, estándares, procedimientos y metodologías para que mantengan su eficacia en asegurar el cumplimiento requerido y la gestión del riesgo empresarial. 2 Comunicar los nuevos requisitos y las modificaciones de los existentes al personal que corresponda.	1 Comunicaciones de las modificaciones en los requisitos de cumplimiento. 2 Políticas, principios, procedimientos y estándares actualizados.
		MEA03.03	Confirmar el cumplimiento de requisitos externos.	1 Evaluar regularmente las políticas, estándares, procedimiento y metodologías de la organización para todas las funciones corporativas. 2 Gestionar las deficiencias de cumplimiento en las políticas, estándares y procedimientos dentro de plazos razonables. 3 Evaluar periódicamente los procesos y actividades tanto de TI como de negocio. 4 Revisar regularmente para detectar patrones reiterados de fallos de cumplimiento.	1 Deficiencias de cumplimiento identificadas. 2 Confirmaciones de cumplimiento.
		MEA03.04	Obtener garantía de cumplimiento de requisitos externos.	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. 2 Realizar revisiones regulares internas y externas para evaluar los niveles de cumplimiento. 3 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. 4 Supervisar e informar de los incidentes de incumplimiento. 5 Consolidar a nivel empresariasl los informes sobre requisitos legales, regulatorios y contractuales, involucrando a todas las unidades de negocio.	1 Informes de garantías de cumplimiento. 2 Informes de incidentes de incumplimiento y causas raíces.