



UNIVERSIDAD DEL BÍO-BÍO
FACULTAD DE CIENCIAS EMPRESARIALES
ESCUELA DE INGENIERÍA CIVIL INFORMÁTICA

“Propuesta de Modelo de Gobierno de TI para Subgerencia de Informática de Empresa de Servicios Sanitarios ESSBIO.”

Proyecto de Título presentado en conformidad a los requisitos para obtener el Título
de Ingeniero Civil en Informática

Débora Firmani Zárate

Profesor Guía:
Dra. Elizabeth E. Grandón Toledo

Concepción, Chile
Febrero 2015

Agradecimientos

A mi profesora guía, Elizabeth Grandón que con paciencia y tan valorable disposición me ayudó en todo este proceso con todos sus consejos y propuestas, siempre motivándome con su amable sonrisa.

A Andrés Puente por darme la oportunidad de crecer como profesional y darme la chance de aportar con un grano de trigo con mi trabajo, siempre motivándome a dar lo mejor de mí.

A Mitzi Vera porque contestaste todas las preguntas que te hice siempre con tan buena disposición, son pequeños detalles que de verdad valoro.

A Alejandra Segura porque sin tener el deber, me diste una mano con consejos prácticos y precisos, eres una excelente profesora.

A mis papás porque el apoyo espiritual y emocional que me brindan cada día son un pilar fundamental en mi vida.

A Jesús porque a él le debo todo lo que soy y lo que tengo... tú cumples mis sueños y vas conmigo en el camino hacia ellos.

Índice

Índice de Figuras	4
Índice de Tablas	5
1. INTRODUCCIÓN.....	7
2. OBJETIVO GENERAL	9
3. OBJETIVOS ESPECÍFICOS	9
4. JUSTIFICACIÓN.....	9
5. MARCO TEÓRICO.....	10
5.1 Concepto de Gobierno.....	10
5.1.1 <i>Gobierno Corporativo</i>	10
5.1.2 <i>Definición Gobierno de TI</i>	11
5.1.3 <i>Gobierno de TI</i>	12
5.2 Modelos de Gobierno de TI	16
5.2.1 <i>COBIT 4.1</i>	16
5.2.2 <i>COBIT 5</i>	22
5.2.3 <i>ISO/IEC 38500:2000</i>	28
5.2.4 <i>Comparación entre Modelos</i>	32
5.3 Algunos estándares que apoyan el gobierno TI.....	37
6. ANÁLISIS SITUACIÓN ACTUAL	38
6.1 Datos Generales Empresa.....	38
6.1.1 <i>Visión de la Empresa</i>	38
6.1.2 <i>Misión de la Empresa</i>	38
6.1.3 <i>Valores Corporativos de la Compañía</i>	38
6.1.4 <i>Plan Estratégico de la Empresa</i>	39
6.2 Datos Subgerencia de Informática de ESSBIO	41
6.2.1 <i>Visión de la Subgerencia de Informática</i>	41
6.2.2 <i>Misión de la Subgerencia de Informática</i>	41
6.2.3 <i>Plan Estratégico de Trabajo</i>	41
6.3 Modelo de Organización Actual de Subgerencia de Informática.....	43
6.3.1 <i>Organigrama Subgerencia de Informática ESSBIO</i>	44
6.3.2 <i>BPM</i>	45
6.3.3 <i>Operaciones</i>	45
6.3.4 <i>Infraestructura</i>	45
6.3.5 <i>Seguridad y Aseguramiento de la Calidad</i>	46
6.3.6 <i>Soporte Corporativo SAP</i>	46
6.4 Arquitectura de Información	47
7. PROPUESTA DE MODELO GOBIERNO TI.....	48
7.1 Pirámide de Gobierno TI para Subgerencia de Informática de ESSBIO	48
7.1.1 <i>Principios del Gobierno TI</i>	50
7.1.2 <i>Estructura De Relaciones</i>	52
7.1.3 <i>Niveles de Dirección y Control</i>	52
7.1.4 <i>Dominios de Gobierno TI</i>	54
7.1.5 <i>Procesos</i>	55
7.2 Definición de Procesos Propuestos	58
7.2.1 <i>Evaluar, Dirigir y Monitorear</i>	58
7.2.2 <i>Planificar y Organizar (Pl-Or)</i>	68
7.2.3 <i>Construir e Implementar (Co-Im)</i>	74

7.2.4	<i>Entregar y Dar Soporte (En-DS)</i>	82
7.2.5	<i>Supervisar y Evaluar (Su-Ev)</i>	88
8.	CONCLUSIONES	90
9.	REFERENCIAS	92
10.	ANEXO I: MAPEO PROCESOS DE TI A LOS PRINCIPIOS DE GOBIERNO TI	96
11.	ANEXO II: DESCRIPCIÓN DE PROCESOS COBIT 4.1	97
a.	<i>Planear y Organizar (PO)</i>	97
b.	<i>Adquirir e Implementar (AI)</i>	98
c.	<i>Entregar y Dar Soporte (DS)</i>	99
d.	<i>Monitorear y Evaluar (ME)</i>	101
2.	ANEXO III: ENTREVISTAS.....	102
10.1	<i>Oficial de Seguridad y Control de Calidad</i>	102
10.2	<i>Gestión TI y procesos de Negocio</i>	103
10.3	<i>Soporte Corporativo SAP</i>	104
10.4	<i>Infraestructura TI</i>	105
10.5	<i>Operaciones</i>	106
11.	ANEXO IV: MARCOS COMPLEMENTARIOS DE GOBIERNO TI	108
11.1	<i>ITIL</i>	108
11.2	<i>ISO 27001</i>	111
12.	ANEXO V: GLOSARIO	115

Índice de Figuras

FIGURA 1 ADMINISTRACIÓN DE LAS TI Y GOBIERNO DE TI. FUENTE: PETERSON (2003)	13
FIGURA 2 PIRÁMIDE CON LA OPERACIÓN, ADMINISTRACIÓN Y GOBIERNO DE TI. FUENTE: WEILL ET AL. (2003)	14
FIGURA 3 CUBO DE DEFINICIÓN DE GOBIERNO DE TI. FUENTE: SIMONSSON & JOHNSON (2006)	15
FIGURA 4 CUBO DE COBIT 4.1. FUENTE: ITGI, COBIT 4.1 (2007).....	16
FIGURA 5 FRAMEWORK COMPLETO DE COBIT 4.1 FUENTE: ITGI, COBIT 4.1 (2007)	17
FIGURA 6 ÁREAS DE ENFOQUE DE GOBIERNO DE TI. FUENTE: ITGI (2007)	18
FIGURA 7 METAMODELO DE COBIT 4.1. FUENTE: SOUZA N & FERREIRA N (2013).....	19
FIGURA 8 MATRIZ RACI PROCESO "DEFINIR UN PLAN ESTRATÉGICO". FUENTE: FUENTE: (ITGI, COBIT 4.1, 2007)	21
FIGURA 9 PRINCIPIOS DE COBIT 5. FUENTE: ISACA (2012)	23
FIGURA 10 MATRIZ RACI PROCESO EDM02 ASEGURAR LA ENTREGA DE BENEFICIO FUENTE: ISACA (2012)	25
FIGURA 11 CATALIZADORES DE COBIT 5. FUENTE: ISACA (2012)	27
FIGURA 12 MODELO DE GOBIERNO CORPORATIVO DE TIC ISO/IEC 38500:2000. FUENTE: ISO/IEC (2008)	29
FIGURA 13 ÁREAS CLAVES DE GOBIERNO Y GESTIÓN DE COBIT. FUENTE: ISACA (2012).....	36
FIGURA 14 CUADRO DE ENLACE DE PRINCIPIOS ISO/IEC 38500:2000 CON ELEMENTOS COBIT 5. FUENTE: ELABORACIÓN PROPIA.	36
FIGURA 15 PLAN ESTRATÉGICO ESSBIO. FUENTE: ESSBIO (2014)	40
FIGURA 16 PLAN ESTRATÉGICO SUBGERENCIA INFORMÁTICA AÑOS 2014-2016. FUENTE: ELABORACIÓN SUBGERENTE INFORMÁTICA ESSBIO	43
FIGURA 17 MODELO DE ORGANIZACIÓN ACTUAL DE SUBGERENCIA DE TI FUENTE: ELABORACIÓN SUBGERENTE INFORMÁTICA ESSBIO.....	44
FIGURA 18 ORGANIGRAMA SUBGERENCIA DE INFORMÁTICA ESSBIO. FUENTE: ESSBIO (2014)	44
FIGURA 19 ARQUITECTURA DE INFORMACIÓN. FUENTE: ELABORACIÓN SUBGERENTE INFORMÁTICA ESSBIO.....	47
FIGURA 20 PIRÁMIDE DE GOBIERNO: ESTRUCTURA DE RELACIONES Y NIVELES DE DIRECCIÓN Y CONTROL. FUENTE: ELABORACIÓN PROPIA	50
FIGURA 21 PIRÁMIDE DE GOBIERNO TI: NIVELES DE DIRECCIÓN Y CONTROL Y DOMINIOS DE GOBIERNO. FUENTE: ELABORACIÓN PROPIA	54
FIGURA 22 CLASIFICACIÓN PROCESOS SEGÚN DOMINIO DE GOBIERNO TI.....	58
FIGURA 23 NIVEL Y DOMINIO DE PROCESO "DEFINIR UNA PLAN ESTRATÉGICO DE TI". FUENTE: ELABORACIÓN PROPIA	59
FIGURA 24 NIVEL Y DOMINIO DE PROCESO "DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA	60
FIGURA 25 NIVEL Y DOMINIO DE PROCESO "MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI". FUENTE: ELABORACIÓN PROPIA	61
FIGURA 26 NIVEL Y DOMINIO DE PROCESO "DEFINIR PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI". FUENTE: ELABORACIÓN PROPIA	62
FIGURA 27 NIVEL Y DOMINIO DE PROCESO "ADMINISTRAR LA INVERSIÓN TI". FUENTE: ELABORACIÓN PROPIA.....	64
FIGURA 28 NIVEL Y DOMINIO DE PROCESO "DEFINIR CARTERA DE PROYECTOS TI PARA LA COMPAÑÍA". FUENTE: ELABORACIÓN PROPIA	66
FIGURA 29 NIVEL Y DOMINIO DE PROCESO "ADMINISTRAR LA CALIDAD". FUENTE: ELABORACIÓN PROPIA	68
FIGURA 30 NIVEL Y DOMINIO DE PROCESO "EVALUAR Y ADMINISTRAR RIESGOS DE TI". FUENTE: ELABORACIÓN PROPIA	70
FIGURA 31 NIVEL Y DOMINIO DE PROCESO "ESTABLECER FRAMEWORK DE ADMINISTRACIÓN DE PROGRAMAS Y PROYECTOS". FUENTE: ELABORACIÓN PROPIA.....	72
FIGURA 32 NIVEL Y DOMINIO DE PROCESO "ADMINISTRAR LA TECNOLOGÍA". FUENTE: ELABORACIÓN PROPIA.....	74
FIGURA 33 NIVEL Y DOMINIO DE PROCESO "DISPONIBILIZAR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA". FUENTE: ELABORACIÓN PROPIA	76
FIGURA 34 NIVEL Y DOMINIO DE PROCESO "ADMINISTRAR CAMBIOS". FUENTE: ELABORACIÓN PROPIA	78

FIGURA 35 NIVEL Y DOMINIO DE PROCESO "DEFINIR Y ADMINISTRAR CATÁLOGO DE SERVICIOS". FUENTE: ELABORACIÓN PROPIA 80

FIGURA 36 NIVEL Y DOMINIO DE PROCESO "GARANTIZAR LA SEGURIDAD DE LOS SI/TI". FUENTE: ELABORACIÓN PROPIA 83

FIGURA 37 NIVEL Y DOMINIO DE PROCESO "DEFINIR MODELO DE SOPORTE SI/TI". FUENTE: ELABORACIÓN PROPIA 84

FIGURA 38 NIVEL Y DOMINIO DE PROCESO "ADMINISTRAR LA CONFIGURACIÓN". FUENTE: ELABORACIÓN PROPIA 85

FIGURA 39 NIVEL Y DOMINIO DE PROCESO "ADMINISTRAR OPERACIONES TECNOLÓGICAS". FUENTE: ELABORACIÓN PROPIA 86

FIGURA 40 NIVEL Y DOMINIO DE PROCESO "GARANTIZAR EL CUMPLIMIENTO REGULATORIO". FUENTE: ELABORACIÓN PROPIA . 89

FIGURA 41 CICLO DE VIDA DEL SERVICIO TI-ITIL 108

FIGURA 42 CICLO DEMING PARA UN SGSI. FUENTE: ELABORACIÓN PROPIA EN BASE A LA NORMA ISO 27001 112

Índice de Tablas

TABLA 1 PRINCIPALES FUNCIONES DEL GOBIERNO DE TI. FUENTE: ADAPTADO DE HAMAKER Y HUTTON (2003)..... 12

TABLA 2 ADMINISTRACIÓN TI VS GOBIERNO DE TI. FUENTE: CANO (2006)..... 13

TABLA 3 MÉTRICAS BSC PARA PROCESO DE APO13 "GESTIONAR LA SEGURIDAD". FUENTE: ISACA (2012) 24

TABLA 4 GUÍA ORIENTATIVA PARA GOBIERNO DE TI BASADO EN ISO/IEC 38500:2000 FUENTE: BALLESTER (2009) 30

TABLA 5 MATRIZ DE RESUMEN. CONCEPTOS GENERALES DE MARCOS DE GOBIERNO DE TI. FUENTE: ELABORACIÓN PROPIA 32

TABLA 6 MAPEO DE CATALIZADORES ENTRE COBIT 4.1 Y COBIT 5. FUENTE: ELABORACIÓN PROPIA..... 33

TABLA 7 MAPEO COBIT 4.1 VS COBIT 5 A NIVEL DE PROCESO. FUENTE: FRANCO.IT-GRC (2012) 34

TABLA 8 PRINCIPIOS INVOLUCRADOS EN PROCESO "DEFINIR UN PLAN ESTRATÉGICO DE TI". FUENTE: ELABORACIÓN PROPIA..... 59

TABLA 9 MATRIZ RACI PROCESO "DEFINIR UN PLAN ESTRATÉGICO DE TI". FUENTE: ELABORACIÓN PROPIA 59

TABLA 10 ENTRADAS Y SALIDAS DE PROCESO "DEFINIR UN PLAN ESTRATÉGICO DE TI". FUENTE: ELABORACIÓN PROPIA 59

TABLA 11 PRINCIPIOS INVOLUCRADOS EN PROCESO "DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA 60

TABLA 12 MATRIZ RACI PROCESO "DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA 60

TABLA 13 ENTRADAS Y SALIDAS DE PROCESO "DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA 60

TABLA 14 PRINCIPIOS INVOLUCRADOS EN PROCESO "MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI". FUENTE: ELABORACIÓN PROPIA 61

TABLA 15 MATRIZ RACI PROCESO "MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI". FUENTE: ELABORACIÓN PROPIA 61

TABLA 16 ENTRADAS Y SALIDAS DE PROCESO "MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI". FUENTE: ELABORACIÓN PROPIA 61

TABLA 17 PRINCIPIOS INVOLUCRADOS EN PROCESO "DEFINIR PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI". FUENTE: ELABORACIÓN PROPIA 62

TABLA 18 MATRIZ RACI PROCESO "DEFINIR PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI". FUENTE: ELABORACIÓN PROPIA 62

TABLA 19 ENTRADAS Y SALIDAS DE PROCESO "DEFINIR PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI". FUENTE: ELABORACIÓN PROPIA 63

TABLA 20 PRINCIPIOS INVOLUCRADOS EN PROCESO "ADMINISTRAR LA INVERSIÓN TI". FUENTE: ELABORACIÓN PROPIA..... 64

TABLA 21 MATRIZ RACI PROCESO "ADMINISTRAR LA INVERSIÓN TI". FUENTE: ELABORACIÓN PROPIA 64

TABLA 22 ENTRADAS Y SALIDAS DE PROCESO "ADMINISTRAR LA INVERSIÓN TI". FUENTE: ELABORACIÓN PROPIA 65

TABLA 23 PRINCIPIOS INVOLUCRADOS EN PROCESO "DEFINIR CARTERA DE PROYECTOS TI PARA LA COMPAÑÍA". FUENTE: ELABORACIÓN PROPIA 66

TABLA 24 MATRIZ RACI PROCESO "DEFINIR CARTERA DE PROYECTOS TI PARA LA COMPAÑÍA". FUENTE: ELABORACIÓN PROPIA 66

TABLA 25 ENTRADAS Y SALIDAS DE PROCESO "DEFINIR CARTERA DE PROYECTOS TI PARA LA COMPAÑÍA". FUENTE: ELABORACIÓN PROPIA 67

TABLA 26 PRINCIPIOS INVOLUCRADOS EN PROCESO "ADMINISTRAR LA CALIDAD". FUENTE: ELABORACIÓN PROPIA 68

TABLA 27 MATRIZ RACI PROCESO "ADMINISTRAR LA CALIDAD". FUENTE: ELABORACIÓN PROPIA 69

TABLA 28 ENTRADAS Y SALIDAS DE PROCESO "ADMINISTRAR LA CALIDAD". FUENTE: ELABORACIÓN PROPIA	69
TABLA 29 PRINCIPIOS INVOLUCRADOS EN PROCESO "EVALUAR Y ADMINISTRAR RIESGOS DE TI". FUENTE: ELABORACIÓN PROPIA	70
TABLA 30 MATRIZ RACI PROCESO "EVALUAR Y ADMINISTRAR RIESGOS DE TI". FUENTE: ELABORACIÓN PROPIA.....	70
TABLA 31 ENTRADAS Y SALIDAS DE PROCESO "EVALUAR Y ADMINISTRAR RIESGOS DE TI". FUENTE: ELABORACIÓN PROPIA	71
TABLA 32 PRINCIPIOS INVOLUCRADOS EN PROCESO "ESTABLECER FRAMEWORK DE ADMINISTRACIÓN DE PROGRAMAS Y PROYECTOS". FUENTE: ELABORACIÓN PROPIA.....	72
TABLA 33 MATRIZ RACI PROCESO "ESTABLECER FRAMEWORK DE PROGRAMAS Y PROYECTOS". FUENTE: ELABORACIÓN PROPIA	72
TABLA 34 ENTRADAS Y SALIDAS DE PROCESO "ESTABLECER FRAMEWORK DE PROGRAMAS Y PROYECTOS". FUENTE: ELABORACIÓN PROPIA.....	73
TABLA 35 PRINCIPIOS INVOLUCRADOS EN PROCESO "ADMINISTRAR LA TECNOLOGÍA". FUENTE: ELABORACIÓN PROPIA	74
TABLA 36 MATRIZ RACI PROCESO "ADMINISTRAR LA TECNOLOGÍA". FUENTE: ELABORACIÓN PROPIA	74
TABLA 37 ENTRADAS Y SALIDAS DE PROCESO "ADMINISTRAR LA TECNOLOGÍA". FUENTE: ELABORACIÓN PROPIA.....	75
TABLA 38 PRINCIPIOS INVOLUCRADOS EN PROCESO "DISPONIBILIZAR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA". FUENTE: ELABORACIÓN PROPIA	76
TABLA 39 MATRIZ RACI PROCESO "DISPONIBILIZAR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA". FUENTE: ELABORACIÓN PROPIA.....	76
TABLA 40 ENTRADAS Y SALIDAS DE PROCESO "DISPONIBILIZAR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA". FUENTE: ELABORACIÓN PROPIA	77
TABLA 41 PRINCIPIOS INVOLUCRADOS EN PROCESO "ADMINISTRAR CAMBIOS". FUENTE: ELABORACIÓN PROPIA.....	78
TABLA 42 MATRIZ RACI PROCESO "ADMINISTRAR CAMBIOS". FUENTE: ELABORACIÓN PROPIA	78
TABLA 43 ENTRADAS Y SALIDAS DE PROCESO "ADMINISTRAR CAMBIOS". FUENTE: ELABORACIÓN PROPIA	79
TABLA 44 PRINCIPIOS INVOLUCRADOS EN PROCESO "DEFINIR Y ADMINISTRAR CATÁLOGO DE SERVICIOS". FUENTE: ELABORACIÓN PROPIA.....	80
TABLA 45 MATRIZ RACI PROCESO "DEFINIR Y ADMINISTRAR CATÁLOGO DE SERVICIOS". FUENTE: ELABORACIÓN PROPIA	80
TABLA 46 ENTRADAS Y SALIDAS DE PROCESO "DEFINIR Y ADMINISTRAR CATÁLOGO DE SERVICIOS". FUENTE: ELABORACIÓN PROPIA	81
TABLA 47 PRINCIPIOS INVOLUCRADOS EN PROCESO "GARANTIZAR LA SEGURIDAD DE LOS SI/TI". FUENTE: ELABORACIÓN PROPIA	83
TABLA 48 MATRIZ RACI PROCESO "GARANTIZAR LA SEGURIDAD DE LOS SI/TI". FUENTE: ELABORACIÓN PROPIA.....	83
TABLA 49 ENTRADAS Y SALIDAS DE PROCESO "GARANTIZAR LA SEGURIDAD DE LOS SI/TI". FUENTE: ELABORACIÓN PROPIA	83
TABLA 50 PRINCIPIOS INVOLUCRADOS EN PROCESO "DEFINIR MODELO DE SOPORTE SI/TI". FUENTE: ELABORACIÓN PROPIA.....	84
TABLA 51 MATRIZ RACI PROCESO "DEFINIR MODELO DE SOPORTE SI/TI". FUENTE: ELABORACIÓN PROPIA.....	84
TABLA 52 ENTRADAS Y SALIDAS DE PROCESO "DEFINIR MODELO DE SOPORTE SI/TI". FUENTE: ELABORACIÓN PROPIA	84
TABLA 53 PRINCIPIOS INVOLUCRADOS EN PROCESO "ADMINISTRAR LA CONFIGURACIÓN". FUENTE: ELABORACIÓN PROPIA.....	85
TABLA 54 MATRIZ RACI PROCESO "ADMINISTRAR LA CONFIGURACIÓN". FUENTE: ELABORACIÓN PROPIA	85
TABLA 55 ENTRADAS Y SALIDAS DE PROCESO "ADMINISTRAR LA CONFIGURACIÓN". FUENTE: ELABORACIÓN PROPIA	85
TABLA 56 PRINCIPIOS INVOLUCRADOS EN PROCESO "ADMINISTRAR OPERACIONES TECNOLÓGICAS". FUENTE: ELABORACIÓN PROPIA.....	86
TABLA 57 MATRIZ RACI PROCESO "ADMINISTRAR OPERACIONES TECNOLÓGICAS". FUENTE: ELABORACIÓN PROPIA	86
TABLA 58 ENTRADAS Y SALIDAS DE PROCESO "ADMINISTRAR OPERACIONES TECNOLÓGICAS". FUENTE: ELABORACIÓN PROPIA..	87
TABLA 59 PRINCIPIOS INVOLUCRADOS EN PROCESO "GARANTIZAR EL CUMPLIMIENTO REGULATORIO". FUENTE: ELABORACIÓN PROPIA.....	89
TABLA 60 MATRIZ RACI PROCESO "GARANTIZAR EL CUMPLIMIENTO REGULATORIO". FUENTE: ELABORACIÓN PROPIA	89
TABLA 61 ENTRADAS Y SALIDAS DE PROCESO "GARANTIZAR EL CUMPLIMIENTO REGULATORIO". FUENTE: ELABORACIÓN PROPIA	89
TABLA 62 TABLA DE MAPEO DE PROCESOS TI A LOS PRINCIPIOS DE GOBIERNO TI.....	96
TABLA 63 DIAGRAMA DE PROCESOS DE ITIL v2011. FUENTE: BAUSET-CARBONELL & RODENES-ADAM (2012)	110

1. INTRODUCCIÓN

La información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. Las tecnologías de la información (TI) están avanzando cada vez más y se han generalizado en las empresas y en entornos sociales, públicos y de negocios (Isaca, 2012).

En la década anterior, el término “gobierno” ha tomado realce en el pensamiento empresarial en respuesta a algunos ejemplos que han demostrado la relevancia de un buen gobierno. En el otro extremo de la balanza, se le ha dado relevancia para confrontar los incidentes corporativos a nivel global. Empresas de éxito han reconocido que el comité de dirección y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluyan las TI en el enfoque del gobierno y la gestión (Isaca, 2012).

Entendiendo el gobierno corporativo como un conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa, Wilkin and Chenhall (2010) dieron cuenta que éste es la primera influencia para dar forma al gobierno de TI, estableciendo la taxonomía de gobierno de TI. Ellos estudiaron los conceptos de alineación estratégica, administración de riesgos, administración de recursos, entrega de valor y medición del desempeño. Estos son los facilitadores más significativos del gobierno de TI.

Por otra parte, se observa que la adopción de un solo marco de mejores prácticas de TI puede no ser suficiente para una organización en particular. A pesar del diferente enfoque de las diferencias conceptuales y estructurales, los marcos de mejores prácticas de TI no son, en principio, incompatibles, y pueden ser utilizados en conjunto para promover la mejora de la gestión de la tecnología de la organización. Incluso, dentro de un marco de gobierno TI pueden absorberse otros marcos de trabajo. Estos pueden tener una clasificación distinta a gobierno TI, que pueden complementar o completar según las necesidades propias de la organización a su propio gobierno TI. En este contexto, uno de los retos en la actualidad en la gestión de TI es cómo analizar, adaptar, integrar y comparar los diferentes marcos de mejores prácticas de TI (Souza N & Ferreira N, 2013).

El desafío, por lo tanto en este trabajo, es construir un marco de gobierno de TI propio para la subgerencia de informática de la empresa de Servicios Sanitarios ESSBIO. Este marco tiene como principal objetivo darle valor al negocio y estar alineado a su estrategia. Para ello, luego de un análisis, integrará los marcos de TI existentes, adaptando los conceptos, prácticas y modelos, adecuándolos a las necesidades y cultura propia de la empresa.

En una primera instancia, en este documento se plantea un marco teórico que estudia los conceptos generales de gobierno corporativo y gobierno de TI. Luego se explican tres modelos de gobierno principales, COBIT 4.1, COBIT 5 y la Norma Internacional ISO/IEC 38500:2000 en el cual luego de definirlos, se realiza un análisis comparativo para identificar las diferencias más importantes entre éstos.

Una vez definidos los modelos formales, se realiza un análisis de la situación actual de la unidad donde se procura implementar un modelo de gobierno adaptado propio. En esta sección se estudia y analiza el modelo en el cual se basa la subgerencia de TI (unidad en cuestión), sus estructuras, plan de trabajo y organigrama. Además se estudia la misión y visión de la compañía en la cual se halla inmersa dicha subgerencia y cómo su estructura actual de administración se asemeja a los criterios de los modelos formales expuestos.

Finalmente se propone un modelo de gobierno TI propio basado en los conceptos básicos de gobierno TI presentados. Este modelo extrae de los modelos formales ideas, principios, conceptos y procesos para conformar el propio. Es un marco de trabajo orientado a procesos ya que la estrategia de la compañía incita a tener cultura orientada a procesos y resultados (sección 6.1.4). La propuesta comienza con una definición propia de gobierno TI y luego, en base a dicha definición, se expone una pirámide de tres caras, las cuales son “niveles de gobierno”, “dominios de gobierno” y “estructura organizacional”. Cada uno de estos aspectos es explicado y justificado. Posteriormente, se expone un manual de los procesos y cómo éstos deben ser entendidos. Cada uno de estos procesos contiene una definición, objetivo del proceso y cómo éstos se aplican dentro de la pirámide de tres caras. Por último se define un set de procesos, según las necesidades propias de la subgerencia de informática.

2. OBJETIVO GENERAL

Proponer un modelo de gobierno de TI para la subgerencia de informática de ESSBIO que esté alineado con la misión y visión de la compañía, y por ende también, a su estrategia. Dicha propuesta debe estar basada en modelos formales, y a la vez debe considerar los aspectos propios de la cultura organizacional, con el fin de apoyar el desarrollo de una administración de la información y de los SI/TI en forma eficaz y eficiente. Lo anterior tiene como finalidad colaborar con el cumplimiento de las estrategias y los objetivos de la empresa para generar valor y mitigar los riesgos asociados a las TI.

3. OBJETIVOS ESPECÍFICOS

- Definir un modelo de gobierno de TI específico para ESSBIO basado en un estudio investigativo y adaptado a las necesidades y cultura de la subgerencia de informática de la compañía.
- Identificar las brechas entre la situación actual y el modelo de gobierno de TI propuesto en base a una comparación entre ambos objetos con el propósito de generar un plan de implementación para la disminución de estas diferencias.

4. JUSTIFICACIÓN

Este proyecto tiene como finalidad la investigación teórica y práctica de modelos de gobierno de TI para luego dar una propuesta concreta que pueda dar directrices claras de cómo debe operar y dirigir la subgerencia de informática de ESSBIO. El fin último es dar soluciones pertinentes a los desafíos y/o problemas que deba abordar dicha subgerencia de manera eficiente, eficaz y natural. Por lo anterior, es necesario establecer un gobierno de TI que aborde la administración instaurando procedimientos, estructuras y comportamientos para dirigir y controlar la subgerencia de informática hacia el logro de sus objetivos.

Para lograr una propuesta de valor, es necesario comprender los modelos de gobierno de TI existentes y luego comprender la situación actual de la subgerencia TI de la organización. Para generar dicho valor, la propuesta planteada debe estar alineada a la estrategia de la compañía y tener en consideración sus procesos de negocio. Sumado a lo anterior, esta propuesta debe estar preparada para adaptar las TI de manera activa a los cambios que se produzcan en el negocio.

5. MARCO TEÓRICO

5.1 Concepto de Gobierno

5.1.1 Gobierno Corporativo

La empresa es un organismo vivo en la que participan múltiples actores que están interesados en distintos aspectos que ésta brinda. Los inversionistas, ejecutivos, proveedores, clientes, administradores, etc. la perciben de forma diferente e interactúan con ella en función de su propia perspectiva. Cada actor aporta a la empresa entradas diferentes y espera salidas que incluso a veces, pudieran contraponerse. Por otro lado, la empresa contiene múltiples elementos y recursos, los cuales se deben administrar y controlar adecuadamente. Por toda aquella cantidad de matices y aristas que contiene una empresa se torna totalmente necesario estructurarla y definir cómo la empresa va a moverse para subsistir.

Todo lo anteriormente explicado se funda bajo el concepto de “gobierno corporativo”. Para Lunardi (2008) la idea de gobierno corporativo remonta de la década de 1930, desde el desarrollo de los mercados de capitales. Silveira (2002) señala que en 1932, Berle y Mean introdujeron el “problema de la agencia”. Jensen y Meckling (1976) explican el “problema de la agencia” como un contrato explícito en el que una parte, el agente, se compromete a llevar a cabo determinadas acciones a favor de la otra parte, el principal. El problema de la agencia se produce cuando el agente no puede tomar la mejor decisión para el principal y comienza a actuar buscando su propio interés. De esta forma, el gobierno corporativo es un conjunto de principios o mecanismos que guían la toma de decisiones en una organización para que sea económicamente sostenible y fiable para sus grupos de interés (accionistas, inversionistas, ejecutivos) y minimizar el “problema de la agencia”. Por lo tanto, las buenas prácticas de gobierno corporativo tienen como meta el aumento del valor de la empresa, para que el acceso al capital se facilite y, de esta manera, contribuir a su sostenibilidad (IBGC, 2006).

El gobierno corporativo ha llegado a ser crucial en el actual modelo de negocio, en el que las grandes corporaciones venden acciones en el mercado de capitales. Debido a esto, después de un largo período de estancamiento teórico, el gobierno corporativo se vuelve a estudiar en mayor medida a partir de los años 1980 y 1995, cuando Monks y Minow publican el libro de gobierno corporativo (Lunardi, 2008; Andrade & Rossetti, 2004).

Existen múltiples definiciones de gobierno corporativo, pero en su sentido más amplio puede decirse que el concepto incorpora el conjunto de acuerdos legales, culturales e institucionales, que determina lo que la corporación puede hacer, quién controla sus actuaciones, cómo se ejerce dicho control y cómo se reparten los riesgos y resultados derivados de las actividades que desarrollan (Blair, 1995).

Para Flores (2004), el gobierno corporativo se define como el conjunto de relaciones entre la dirección de la organización, su consejo de administración y otras partes involucradas. Además de proporcionar un marco que permita clarificar los objetivos de las

organizaciones, cómo puede servirles y para monitorear su desempeño. Por lo tanto, el gobierno corporativo crea mecanismos, estructuras e incentivos que conforman el modelo de control de la gestión social del sistema y dirige el comportamiento de los administradores para la ejecución de las metas organizacionales, además de suministrar a la alta dirección los recursos empresariales para identificar los riesgos que están relacionados con el negocio (Martin, Dos Santos, & Dias, 2004).

Para Lorente (2011) los agentes implicados en el gobierno corporativo son: el Gerente (CEO), el Consejo de Dirección, los ejecutivos y los inversores, además de otros agentes empresariales como son los proveedores, los financiadores, clientes y la comunidad en general. A todos ellos les interesa y beneficia un buen gobierno corporativo, de manera que directivos, ejecutivos y trabajadores reciban mejores salarios y reputación, que a los inversores les revierta mayor capital, que los clientes reciban mejores productos y servicios, y que la comunidad y el medio ambiente se vean protegidos y beneficiados.

5.1.2 *Definición Gobierno de TI*

Weill y Ross (2006) presentan el concepto de gobierno de TI como “la especificación de derechos de decisión y marco de responsabilidades para fomentar comportamientos deseables en el uso de TI.” (p. 8)

Según Pelanda (2006), el gobierno de TI tiene como meta identificar los valores y la importancia estratégica de las TI en la empresa y asegurarse de que soporten sus operaciones y que puedan cumplir con la implementación de las estrategias de crecimiento de la organización. Al mismo tiempo garantizar que las expectativas de TI sean cumplidas y los riesgos inherentes a TI se reduzcan.

El buen desempeño del gobierno de TI trae buenos resultados para la organización. Según Bowen et al. (2007), la gestión de los recursos de TI ayuda a conseguir el éxito de la organización y un gobierno de TI eficaz genera beneficios reales para la organización, tales como: la credibilidad, los productos de referencia, la prestación de servicios y la disminución de costes.

Para Fernandes y Abreu (2008), el gobierno de TI busca participación en las decisiones de TI con otros directivos de la organización, así como establecer las normas, la organización y los procesos que guían el uso de las Tecnologías de la Información y Comunicación (TICs) por los usuarios, departamentos, unidades de negocio, proveedores y clientes.

Jaeger-Neto et al. (2009) señalan que en base a la estrategia de la organización, y siendo parte importante de esta estrategia, el gobierno de TI es el uso de las mejores prácticas y procesos organizacionales que buscan un comportamiento deseable para que las TI ayuden a la realización de las estrategias definidas para obtener el éxito empresarial. Además argumentan que el gobierno corporativo y de TI puede influir significativamente en el desempeño de la organización, a través de la creación de valor para el negocio y la gestión de riesgos equilibrado con el retorno de la inversión. Así, algunos de los principios de gobierno corporativo se adoptaron en el gobierno de TI.

Para ITGI (2009), el gobierno de TI es responsabilidad del directorio y la gerencia ejecutiva de la organización. Un factor crucial para el gobierno de TI es identificar a los tomadores de decisiones y quiénes responderán por la ejecución de ellas.

ITGI (2011) define que el propósito del gobierno de TI es dirigir las TI y garantizar que su desempeño cumpla con los siguientes objetivos: alineamiento de TI con la organización y la aplicación de los beneficios prometidos; uso de las TI para permitir a la organización explorar oportunidades y maximizar los beneficios; el uso responsable de los recursos de TI; y la gestión de los riesgos relacionados con TI.

El gobierno de TI se presenta como una herramienta para permitir la alineación entre las estrategias de negocio y de TI, más allá de favorecer un mayor profesionalismo a los procesos de toma de decisiones de TI.

Para efectos de este estudio se definirá el gobierno TI como la “estructura de relaciones y procesos para dirigir y controlar las tecnologías de la información con el fin de garantizar que éstas soportan y habilitan la estrategia de la empresa y el logro de sus objetivos”.

5.1.3 Gobierno de TI

Hamaker (2003) establece que el gobierno corporativo y el gobierno de TI son ambos componentes del gobierno global de la organización. Posteriormente Hamaker y Hutton (2004) establecen que “los principales procesos que sostienen un gobierno de TI efectivo son los mismos que los de un buen gobierno corporativo. Por tanto, el constante escrutinio al que es sometido el gobierno corporativo afecta directamente a las TI y a la dirección que ha de tomar el gobierno de TI” (pág. 1). Más aún, puesto que en el momento actual las TI pueden considerarse como críticas para el buen funcionamiento de muchos negocios, el gobierno corporativo sería incompleto sin un adecuado gobierno de TI. Estos autores establecen como principales funciones específicas del gobierno de TI las que aparecen en la Tabla 1

Tabla 1 Principales funciones del gobierno de TI. Fuente: Adaptado de Hamaker y Hutton (2003)

Alineación y Planificación Estratégica	Financiación
<ul style="list-style-type: none"> • Comité de Dirección de las TI (proceso prioritario) <ul style="list-style-type: none"> – Alineación con los objetivos de negocio • Estrategia de TI y estándares de arquitectura • Planificación de los proyectos de TI • Dar soporte a las iniciativas estratégicas de la organización 	<ul style="list-style-type: none"> • Presupuesto de operación de las TI • Gestión de los activos TI • Gestión de contratos de las TI • Planificación y asignación de los recursos de TI
Operaciones de TI	Modelos de Control
<ul style="list-style-type: none"> • Desarrollo de aplicaciones • Dar soporte a la producción • Arquitectura tecnológica • Diseño, implementación y operación de redes • Centro de atención a los usuarios • Gestión de la seguridad de la información • Continuidad del servicio y recuperación ante desastres • Gestión de la relación con proveedores 	<ul style="list-style-type: none"> • Políticas de gestión de la información • Estándares • Procedimientos técnicos • Gestión de la documentación de los sistemas • Asegurar la calidad • Cumplimiento de la legislación y normativas

Es necesario destacar una diferenciación entre operación, administración y gobierno de TI (Weill, Broadbent, & Blosch, 2003). Las operaciones se centran en la infraestructura de las TI; la administración aborda la arquitectura TI, entendida como la organización lógica de los procesos de negocio y los proyectos de TI; y el gobierno pone énfasis en la toma de

decisiones para cumplir los objetivos locales y corporativos en el contexto de los procesos de negocio y los proyectos de TI (Weill & Ross, 2006).

Peterson (2003) indica las diferencias principales entre administración de las TI y gobierno de TI. Como muestra la Figura 1, la administración de las TI se centra en ofertar internamente productos y servicios de TI y a gestionar sus operaciones en explotación; mientras que el gobierno de TI es más directivo y se centra en la evaluación y transformación de las TI actuales para adaptarlas a las demandas presentes y futuras del negocio (orientación interna) y a las expectativas de los clientes (orientación externa).

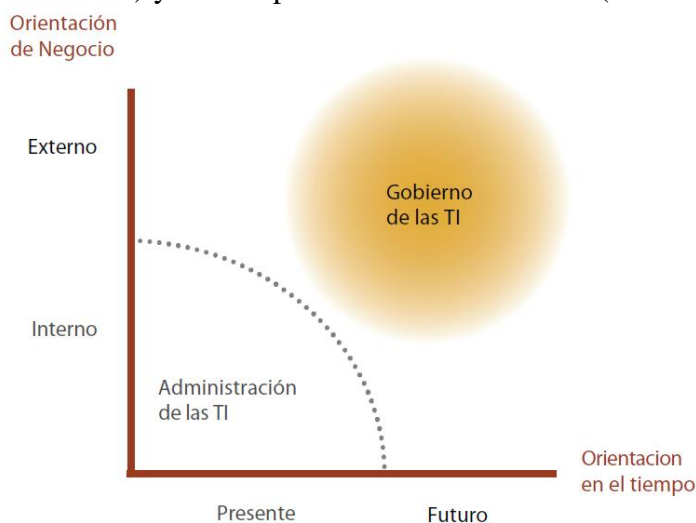


Figura 1 Administración de las TI y Gobierno de TI. Fuente: Peterson (2003)

Peterson además añade que esta diferencia no le resta importancia ni complejidad a la administración de las TI, pero sí advierte que la administración podría ser delegada a un proveedor externo, mientras que el gobierno de TI debe permanecer dentro de la organización.

Para Cano (2006) las características propias de cada término se encuentran en la Tabla 2

Tabla 2 Administración TI vs Gobierno de TI. Fuente: Cano (2006)

Administración de las TI	Gobierno de TI
<ul style="list-style-type: none"> • Rendir cuentas • Usar adecuadamente los recursos • Cumplir normas y establecer procedimientos • Mantener el ciclo de los procesos • Gestionar la cartera de proyectos • Responder a las exigencias de la dirección • Responder a las exigencias de los usuarios • Implementar buenas prácticas reconocidas internacionalmente 	<ul style="list-style-type: none"> • Alinear estratégica y tácticamente las TI y el negocio • Orientar y dirigir las TI • Establecer un marco de referencia para la toma de decisiones • Definir valores y principios para las TI • Promover ciclos de procesos que incluyan la gestión del cambio • Responder a las exigencias de los agentes de la empresa y a la sociedad • Mirar al futuro y visualizar oportunidades de negocio generadas por la TI

Los tres niveles en el ámbito de las TI enunciadas anteriormente se explican en la Figura 2: Operación de TI, que trata sobre la continuidad y competencia de la infraestructura TI de la

organización; Administración de TI, que procura alcanzar la credibilidad a la hora de diseñar y gestionar la arquitectura de las TI de la organización; Gobierno de TI, que pretende alcanzar el compromiso y la evidencia de que las TI son un elemento estratégico que proporciona un valor añadido a la empresa. Los modelos de compromiso de las TI suponen el establecimiento de un sistema de mecanismos de gobierno que pretenden el cumplimiento de los objetivos locales y corporativos en el contexto de los procesos de negocio y de los proyectos de TI.

La forma piramidal del modelo de madurez propuesto, indica que, para llegar a alcanzar el nivel más alto (el gobierno de TI), la empresa tiene que asegurarse que ha alcanzado satisfactoriamente los niveles inferiores.



Figura 2 Pirámide con la Operación, Administración y Gobierno de TI. Fuente: Weill et al. (2003)

En resumen, bien podría afirmarse que el gobierno de TI es una parte fundamental del gobierno corporativo, entendiéndolo como un set de buenas prácticas y responsabilidades que ejerce el consejo administrativo y el directorio de la empresa. El objetivo es proporcionar una dirección con estrategia, y de esa forma, cerciorar que las metas son logradas, proveer una gestión de riesgos correcta y comprobar que los recursos de la organización son administrados adecuadamente. Lo anterior se debe llevar a cabo tomando en cuenta las demandas de los distintos grupos de interés y los constantes cambios del entorno. Según lo anterior, el gobierno de TI comprende el liderazgo, las estructuras organizativas y los procesos que aseguran que las TI de la organización soportan y extienden los objetivos y estrategias de la misma. Estos componentes se traducen en funciones relacionadas con la alineación y planificación estratégica, la financiación de las TI, las operaciones de TI y los modelos de control. Asimismo refleja que la responsabilidad del gobierno de TI radica en la alta dirección.

Para ampliar esta definición, Simonsson y Johnson (2006) basados en una extensa revisión bibliográfica incluyendo algunas de las aquí definidas, realizan una definición propia que se sustenta en tres dimensiones: Alcance, Dominio y Procesos de toma de decisiones (Figura 3)

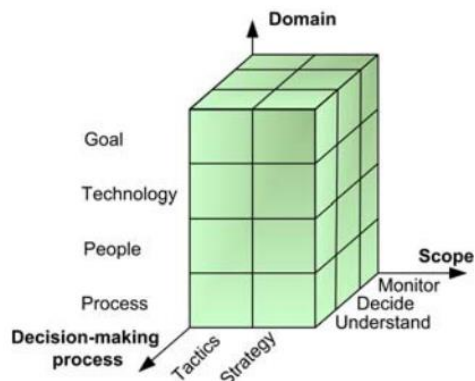


Figura 3 Cubo de Definición de Gobierno de TI. Fuente: Simonsson & Johnson (2006)

La dimensión “dominio” hace referencia a las decisiones que deberían ser consideradas y comprende cuatro áreas: Objetivos, el cual comprende las decisiones que tienen relación con la estrategia, desarrollo y perfeccionamiento de las políticas y procedimientos de TI y objetivos de control que deben medirse; Tecnología, representa a los elementos físicos que considere la dirección, como pueden ser el hardware y software actuales; Personas, incluye la estructura de relaciones dentro de la organización y los roles y responsabilidades de los diferentes agentes; Procesos, incluye la gestión y la implementación de procesos de TI. Ejemplos de decisiones a tomar en relación con los procesos son las actividades necesarias para llevar a cabo las tareas relacionadas con las TI.

La dimensión “proceso de toma de decisiones” comprende tres fases: Comprensión, la que implica que antes de que la organización tome decisiones importantes tiene que comprenderlas en toda su extensión. Las acciones deben ser analizadas, reflexionadas y transformadas en un modelo. Este modelo no tiene por qué ser un modelo formal expresado documentalmente, puede ser simplemente un concepto claro presente en la mente del directivo que toma las decisiones; Decisión, la cual permite que una vez que se ha creado el modelo, ya se puede tomar las decisiones de acuerdo con los principios corporativos de TI, en un espacio de tiempo concreto, por las personas adecuadas, etc.; Monitoreo, la que se puede llevar a cabo implementando objetos de control para cada proceso con el fin de evaluar su comportamiento real. De esta manera el directivo puede comparar los valores reales con los que deberían obtenerse del modelo diseñado.

Por último en la dimensión “alcance” se clasifica en función de su horizonte temporal en decisiones de corto y largo plazo. Dependiendo del alcance, las decisiones se dividen en: tácticas y estratégicas. Las primeras son decisiones de TI de administración de bajo nivel, muy detalladas y precisas y llevadas a cabo de manera inmediata y que afectan muy directamente a las TI. Por su parte, las decisiones estratégicas son aquellas tomadas al más alto nivel, que se caracterizan por no ser detalladas, por un largo alcance temporal y por estar orientadas a los objetivos de negocio.

5.2 Modelos de Gobierno de TI

5.2.1 COBIT 4.1

COBIT 4.1 (Control Objectives for Information and Related Technology, por sus siglas en inglés) fue creado en el año 2007 por el ISACA (Information Systems Audit and Control Association, por sus siglas en inglés) como una guía para la gestión de TI, organizada con el fin de monitorear el desempeño de las tecnologías de la información, asegurando que los recursos de TI están alineados de manera efectiva con la estrategia del negocio de la organización.

El modelo conceptual de COBIT 4.1 está representado en un cubo cuyas caras están relacionadas entre sí, como se muestra en la Figura 4. Estas caras o dimensiones son: Procesos de TI, la cual corresponde a la capa frontal del cubo; Requerimientos de Negocio, correspondiente a la capa superior del cubo; y Recursos de TI, que es la capa derecha del cubo.

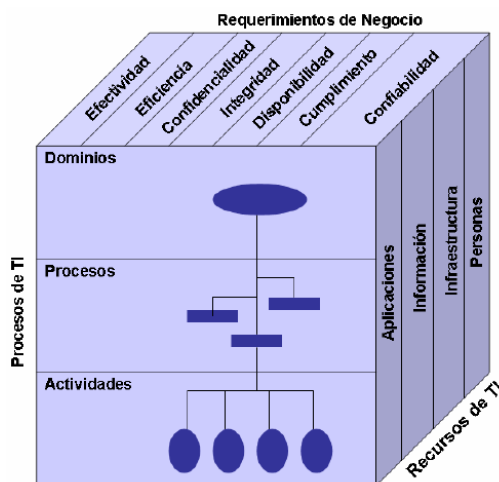


Figura 4 Cubo de COBIT 4.1. Fuente: ITGI, COBIT 4.1 (2007)

La capa frontal del cubo de la Figura 4, denominada Procesos de TI, está organizada en una estructura de dominios, los cuales comprenden procesos y éstos, a su vez, actividades. Básicamente, el modelo identifica cuatro dominios:

Planificar y Organizar (PO): centrado en la estrategia y la táctica de TI para contribuir, de hecho, con los objetivos de negocio de la organización (ITGI, 2007).

Adquirir e Implementar (AI): su atención se centra en la aplicación de la estrategia de TI. Aquí, las soluciones de TI se identifican, desarrollan, adquieren, implementan y se integran con los procesos de negocio (ITGI, 2007).

Entrega y Soporte (DS): se centra en temas relacionados con la entrega de los servicios en sí, lo que incluye la prestación de servicios, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas (ITGI, 2007)

Monitorear y Evaluar (ME): su objetivo es evaluar los procesos de TI desde el punto de vista de la calidad y el cumplimiento de los requisitos de control con regularidad, abarcando la administración del desempeño, el monitoreo del control interno, el

cumplimiento regulatorio y la aplicación del gobierno (Souza N & Ferreira N, 2013; ITGI, 2007).

La Figura 5 muestra la relación entre los cuatro dominios e identifica los procesos y actividades asociados a cada uno.

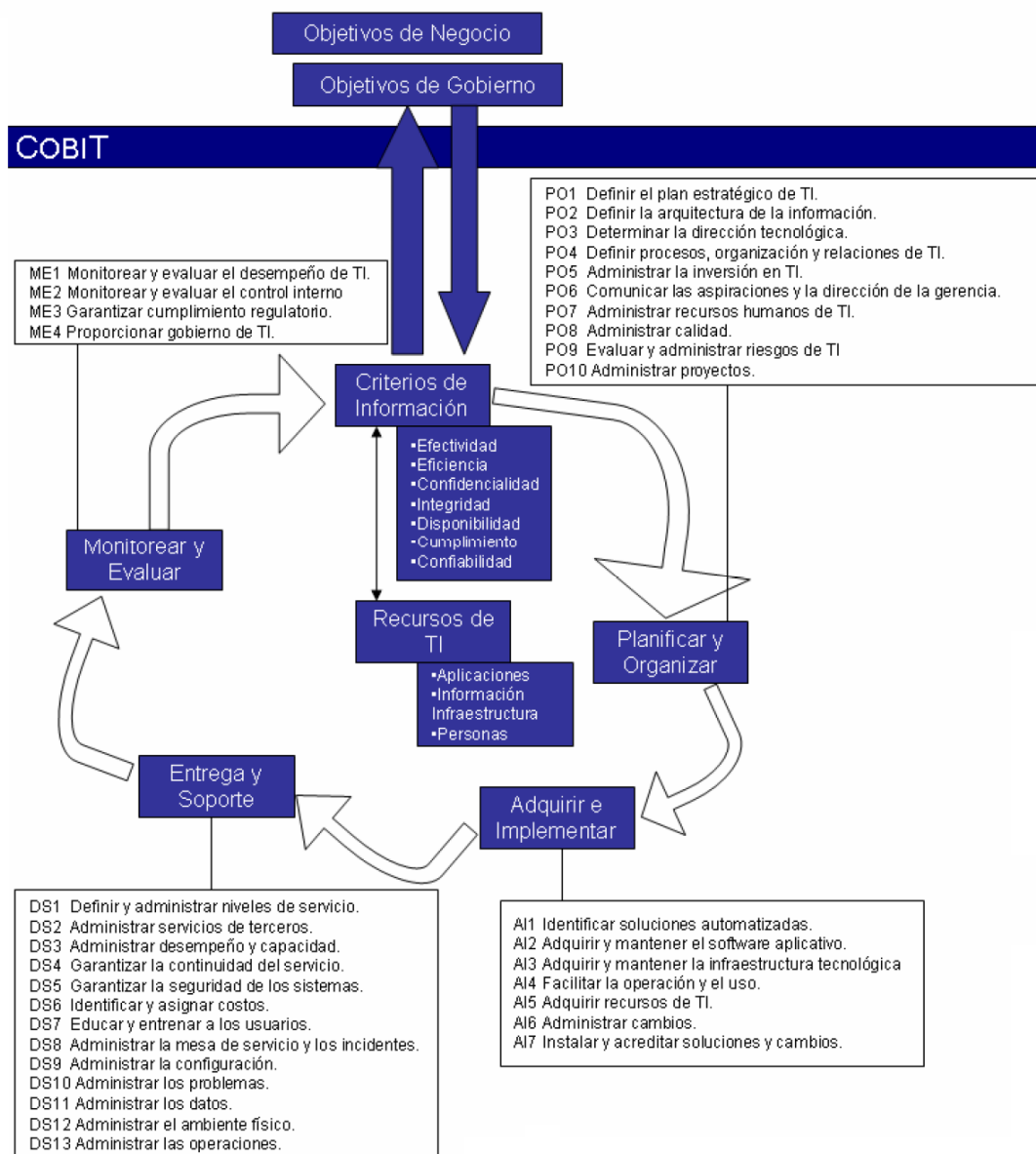


Figura 5 Framework completo de COBIT 4.1 Fuente: ITGI, COBIT 4.1 (2007)

En la capa superior de requerimientos del negocio, el modelo propuesto por COBIT 4.1, establece que para satisfacer los objetivos del negocio, la información tiene que ajustarse a criterios de: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Por último, la capa lateral del cubo se vincula a las dimensiones anteriores en los aspectos relacionados con los recursos de TI, que son: aplicaciones, información, infraestructura y personas.

Las áreas de enfoque para el gobierno de TI, de acuerdo con COBIT 4.1, se presentan en el pentágono que se muestra en la Figura 6.



Figura 6 Áreas de enfoque de gobierno de TI. Fuente: ITGI (2007)

1. Alineamiento estratégico.

Se enfoca en garantizar la alineación entre los planes de negocio de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

2. Entrega de Valor.

Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

3. Gestión del Riesgo.

Requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

4. Gestión de Recursos.

Se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

5. Medición del desempeño.

Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio con el uso, por ejemplo, de balanced scorecard que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

Para satisfacer las necesidades de gestión de la medición y el control de TI, COBIT 4.1 ofrece, 34 procesos de TI, con directrices que contienen herramientas de evaluación y medición para el entorno de TI de la organización. Esto incluye el modelo de madurez, factores críticos de éxito, indicadores clave de metas e indicadores clave de desempeño para cada proceso (Van Grembergen, 2004).

Para explicar la estructura de COBIT 4.1 fue utilizado un metamodelo (Figura 7), a través de la metodología de MetaFrame, basada en la disciplina de metamodelado conceptual y metodología Entidad / Relación extendido (Souza N & Ferreira N, 2013).

Metamodelo COBIT 4.1

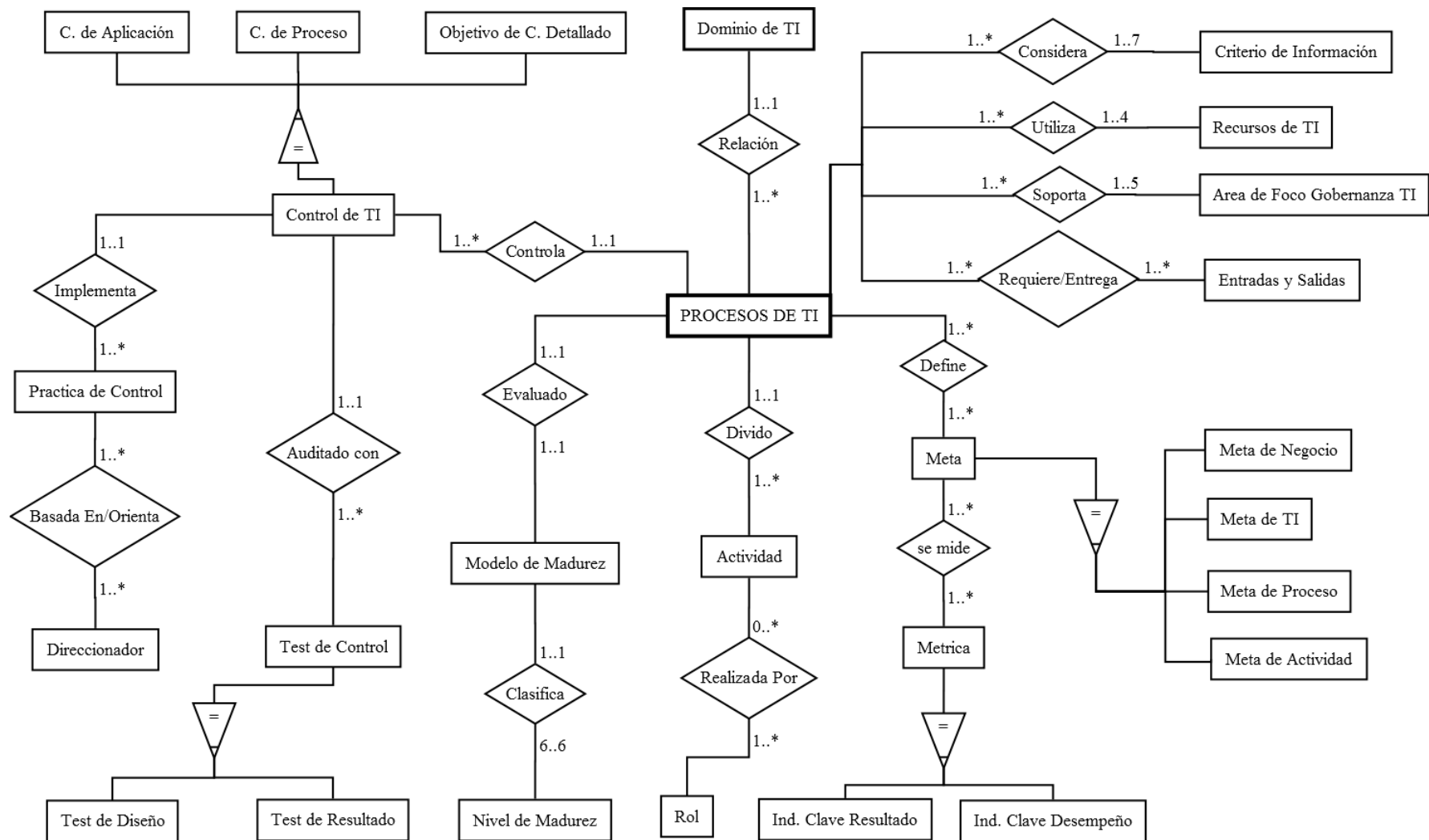


Figura 7 Metamodelo de COBIT 4.1. Fuente: Souza N & Ferreira N (2013)

Resumen Metamodelo COBIT 4.1

El metamodelo ontológico presentado en la Figura 7 representa las estructuras conceptuales que constituyen el marco COBIT 4.1. Estos conceptos son simbolizados como tipos de entidad (rectángulos), tipos de relaciones (diamantes), cardinalidades (números alrededor de las relaciones), tipos de constructor (triángulos) y líneas de conexión de entidades a relaciones.

En el metamodelo COBIT 4.1, el tipo de entidad central es el “proceso de TI”. Éstos pertenecen a determinados dominios de TI especificado en la Figura 5. El tipo de entidad “dominio de TI” representa los cuatro dominios que agrupan uno o más procesos de TI (PO, AI, DS, ME).

Los procesos son divididos en una o más actividades. En cada actividad participa uno o más roles, las cuales pueden ser:

- **Responsible** (Responsable): Se refiere a la persona encargada de conseguir que las actividades se completen satisfactoriamente. Responde a la pregunta: ¿Quién está ejecutando la tarea? Roles que toman la responsabilidad operacional principal en completar la tarea listada y en generar el resultado deseado.
- **Accountable** (Responsable de que se haga): El individuo, grupo o entidad que tiene la responsabilidad última sobre una materia, proceso o alcance. Responde a la pregunta: ¿A quién hay que pedir cuentas por el éxito de la tarea?
- **Informed** (Informado): Se refiere a aquellas personas que son actualizadas con el progreso de una actividad (comunicación unidireccional). Responde a la pregunta: ¿Quién recibe información? Los roles que son informados de la consecución de metas y/o los entregables de la tarea. El rol ‘Accountable’ por supuesto debería siempre recibir información apropiada para supervisar la tarea, al igual que otros roles responsables para cada una de sus áreas de interés.
- **Consulted** (Consultado): Se refiere a aquellas personas cuyas opiniones son buscadas en una actividad (comunicación bidireccional). Responde a la pregunta ¿Quién proporciona las entradas? Roles claves que proporcionan entradas. Hay que subrayar que los roles responsables de ejecutar la tarea y los que son responsables de que se haga también deben obtener la información de otras unidades o de socios externos; sin embargo, deben considerarse las entradas de los roles listados y, si se requiere, se debe tomar una acción adecuada para su escalado, incluyendo la información del dueño del proceso y/o del comité de supervisión.

Estos roles se pueden visualizar mediante una matriz RACI (**R**esponsible, **A**ccountable, **C**onsulted y **I**nformed por sus siglas en inglés). Un ejemplo de esta matriz se puede ver en la Figura 8, la cual proyecta la matriz del proceso “Definir un Plan Estratégico”.

Matriz RACI

Funciones												
Actividades	Chief Executive Officer	Chief Financial Officer	Ejecutivo del Negocio	Chief Information Officer	Dueño de Proceso de Negocio	Jefe de Operaciones	Arquitecto en Jefe	Project Management de TI	Cumplimiento, Auditoría, Riesgo y Seguridad			
Relacionar las metas del negocio con las de TI	C	I	A/R	R	C							
Identificar dependencias críticas y desempeño actual	C	C	R	A/R	C	C	C	C				C
Construir un plan estratégico para TI	A	C	C	R	I	C	C	C	I			C
Construir planes tácticos para TI	C	I		A	C	C	C	C	R			I
Analizar portafolios de programas y administrar portafolios de servicio y proyectos	C	I	I	A	R	R	C	R	C			I

Una matriz **RACI** identifica quien es Responsable, quien debe rendir cuentas (A), quien debe ser Consultado y/o Informado

Figura 8 Matriz RACI Proceso “Definir un plan estratégico”. Fuente: Fuente: (ITGI, COBIT 4.1, 2007)

Cada proceso de COBIT 4.1 considera de uno a siete elementos de criterios de información, que podrían ser: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y/o confiabilidad.

Cada Proceso utiliza de una a 4 elementos de Recursos de TI, que pueden ser: Aplicaciones, Personas, Información y/o Infraestructura.

Un proceso de TI también soporta de una a cinco áreas de foco de gobierno de TI, estas son: alineación estratégica, entrega de valor, administración de riesgos, administración de recursos y medición del desempeño, las que fueron explicadas anteriormente en esta misma sección.

Cada proceso TI requiere y/o entrega uno o más elementos de entrada y/o salida, que contienen insumos o resultados (documentos, acciones, etc.) desde otros procesos de COBIT 4.1 o de procesos externos.

Cada proceso de COBIT 4.1 es evaluado de acuerdo a su Modelo de Madurez específico. La entidad “Modelo de Madurez” provee un perfil para cada proceso basado en una calificación de seis elementos de nivel de madurez: Inicial, Repetible pero intuitivo, Definido, Administrado y Medible y por último, Optimizado.

Un proceso de TI define una o más metas. Una meta puede representar a las siguientes tipos de entidades: Metas del Negocio, Metas de TI, Metas de Proceso o Metas de Actividades. Una meta es medida por una o más métricas. Una métrica representa a indicadores claves de Resultado (KGI por sus siglas en inglés) o Indicadores Clave de Desempeño (KPI por sus siglas en inglés).

Un Proceso de TI es controlado por uno o más Controles de TI. La entidad Control de TI representa los siguientes tipos: Control de Aplicación, Control de Procesos u Objetivo de Control Detallado que controla un proceso de TI en Particular.

Un Control de TI es implementado por una o más prácticas de Control. Una práctica de Control implementa sólo un Control TI en particular. Una práctica de Control se basa en uno o más direccionadores, que puede ser de valor o riesgo.

Un Control TI es auditado por uno o más elementos de Test de Control, que a su vez audita un Control TI específico. Un Test de Control representa a las entidades Test de Diseño y Test de Resultados¹.

ISACA lanzó el 10 de abril del 2012 la nueva edición de este marco de referencia. COBIT 5 es la última edición del framework mundialmente aceptado, el cual proporciona una visión empresarial del gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

COBIT 5 se basa en COBIT 4.1, y a su vez se amplía mediante la integración de otros importantes marcos, lo cual será explicado a continuación.

5.2.2 COBIT 5

COBIT 5, describe un set de buenas prácticas para la Alta Dirección y la administración. Este set establece un conjunto de controles sobre las tecnologías de la información y los organiza en torno a un marco lógico de los procesos relacionados a las TI. (De Haes, Van Grembergen, & Debreceeny, 2013)

De acuerdo a ISACA (2012), “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. 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” (p.13).

COBIT 5 no es un marco aislado, sino que se alinea a otras normas existentes, como las versiones de COBIT más antiguas, algunos estándares como: ISO 38500:2000 complementándose esencialmente en los principios de éste (Evaluar, Dirigir y Monitorizar) (Isaca, 2012); la ISO 15504 alineándose a ella en el concepto para procesar capacidad (De Haes, Van Grembergen, & Debreceeny, 2013) y VALIT para abarcar el aporte de Valor, entre otros.

Principios COBIT 5

Este marco se construye en torno a cinco principios básicos (Figura 9) que serán brevemente explicados a continuación:

¹ En el Anexo I se ofrece una descripción resumida de cada proceso del marco



Figura 9 Principios de COBIT 5. Fuente: Isaca (2012)

1. Necesidades de las Partes Interesadas:

a. Estrategia del Negocio/Alineamiento de TI.

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

COBIT 5 estableció una lista genérica de los objetivos empresariales, metas relacionadas con las TI, y su interrelación o “cascada”, la cual es el punto de entrada primordial para el marco. Existe una suposición explícita de que las organizaciones deberían comenzar con el análisis del estado de alineamiento Negocio-TI a través de la definición de las metas de la Empresa vinculando estas metas a los objetivos relacionados con las TI y luego a los procesos de TI que se encuentran en COBIT.

En la cascada de metas, la empresa y los objetivos relacionados con la TI se clasifican en perspectiva: financiera, cliente, interna y por último, aprendizaje y crecimiento.

b. El cuadro de Mando Integral (Balanced Scorecard)

Para verificar si efectivamente se están cubriendo las necesidades de las partes interesadas, se debe establecer un proceso de medición (Elbashit, Collier, & Michael J., 2008). COBIT se basa en conceptos como Balanced Scorecard (BSC) desarrollado por Kaplan y Norton (1996), y en su versión adaptada para el dominio de TI.

COBIT 5 ofrece medidas de resultado a nivel de procesos de TI. La Tabla 3 muestra un ejemplo para el proceso de Gestión de la seguridad (APO13), proporcionando metas específicas del proceso y las métricas relacionadas.

La consolidación de estos indicadores en la empresa, relacionada con TI, y los niveles de procesos de COBIT, permite a las organizaciones construir un cuadro de mando integral

para todo el entorno de TI. Esto permite a las organizaciones desarrollar un instrumento de medición para verificar satisfacción de las necesidades de los stakeholders.

Tabla 3 Métricas BSC para proceso de APO13 “Gestionar la Seguridad”. Fuente: Isaca (2012)

Metas de proceso	Métricas Relacionadas
1. Un sistema está en el lugar que considere y aborde eficazmente los requisitos de seguridad de la información empresarial	<ul style="list-style-type: none"> • Número de roles de seguridad clave definidos claramente • Número de incidentes relacionados con seguridad
2. Un plan de seguridad se ha establecido, aceptado y comunicado a toda la empresa	<ul style="list-style-type: none"> • Nivel de satisfacción de los interesados con el plan de seguridad en la empresa • Número de soluciones de seguridad desviadas del plan • Número de soluciones de seguridad desviadas de la arquitectura empresarial
3. Las soluciones de seguridad de información se implementan y operan constantemente en toda la empresa.	<ul style="list-style-type: none"> • Número de servicios con alineación confirmada al plan de seguridad • Número de incidentes de seguridad causados por la no adherencia al plan de seguridad • Número de soluciones desarrolladas con alineación confirmada al plan de seguridad

2. Cubrir la Empresa de Extremo a Extremo

Cubre todas las funciones y los procesos dentro de la organización; COBIT 5 no solamente se concentra en la “Función de la TI”, sino trata la tecnología de la información y tecnologías relacionadas como activos que necesitan ser manejados como cualquier otro activo, por todos en la organización.

Con respecto a este tema, COBIT 5 abarca tanto los procesos de TI como los procesos de negocio que están relacionados con TI. La colaboración y relaciones recíprocas y las dependencias entre tareas de gestión empresarial, gestión de TI, y las partes externas es un elemento importante del gobierno de TI. COBIT 5 ofrece gráficos RACI, al igual que en COBIT 4.1, en el que se incluyen tanto los roles del negocios como los de TI. Para ilustrar esto, la Figura 10 muestra un ejemplo gráfico RACI para el proceso EDM02 “Asegurar la entrega de beneficio”.

En una matriz RACI de COBIT 5 se definen los roles de la misma forma que en COBIT 4.1. (Responsable, Accountable, Informed, Consulted). No obstante, en COBIT 5 se establecen más roles participando en una práctica.

EDM02 RACI Chart																											
Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executive	Business Process Owners	Strategy Executive Committee	Steering (Programmer/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operation	Head IT Administration	Service Manger	Information Security Manager	Business Continuity Manager	Privacy Officer	
EDM02.01 Evaluar la optimización de valor	A	R	R	C	R		R			C	C		C	C	C	C	C	R	C	C	C						
EDM02.02 Dirigir la optimización de valor	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I	I
EDM02.03 Monitorear la optimización de valor	A	R	R	C	R		R			R	C	C	C	C	C	C	C	R	C	C	C						

Figura 10 Matriz RACI Proceso EDM02 Asegurar la entrega de beneficio Fuente: Isaca (2012)

3. Aplicar un Marco de Referencia único integrado

El tercer principio explica que COBIT 5 se alinea a un alto nivel con otros estándares y marcos pertinentes. Por lo tanto, puede servir como marco general para el gobierno y la gestión de las TI corporativas. COBIT 5 integra todas las materias de gobierno de TI de ISACA anteriores en COBIT 4, Val IT y Risk IT (ITGI, 2007; 2009; 2010).

En su planteamiento general, COBIT 5 identifica un conjunto de facilitadores de gobierno y gestión, que incluye 37 procesos.

En la capa de gobierno, hay cinco procesos en el dominio Evaluar, Dirigir y Monitorizar (EDM). Estos procesos establecen las responsabilidades de la junta directiva para evaluar, dirigir y supervisar el uso de los activos de TI para crear valor para la empresa. Establece responsabilidades en términos de valor (por ejemplo, criterios de inversión), riesgos (por ejemplo, el apetito de riesgo), recursos (por ejemplo, la optimización de recursos), y proporciona transparencia en relación con TI a los stakeholders.

En el ámbito de la gestión, hay cuatro subdominios: “Alinear, Planificar y Organizar” (APO); “Construir, adquirir e implementar” (BAI por sus siglas en inglés); “Entrega, servicio técnico y soporte” (DSS por sus siglas en inglés); y “Monitorizar, evaluar y valorar” (MEA por sus siglas en inglés).

El dominio APO se refiere a cómo las TI pueden contribuir de la mejor manera a la consecución de los objetivos de negocio. Se requiere un marco de gestión y procesos específicos relacionados con la estrategia y tácticas, arquitectura empresarial, la innovación y la administración de portafolios de TI. Otros procesos importantes en este ámbito abordan la gestión de los presupuestos y costos, recursos humanos, relaciones, acuerdos de servicios, proveedores, la calidad, el riesgo y la seguridad.

El dominio BAI hace que la estrategia TI sea concreta a través de la identificación, en detalle, los requisitos de TI y la gestión de los programas y proyectos de inversión. Este dominio considera, además, la capacidad de gestión, cambio organizacional, los cambios de TI, la aceptación y la transición, el conocimiento, los activos y configuraciones.

El dominio de entrega, servicio y soporte (DSS) se refiere a la prestación efectiva de los servicios de TI necesarios. Contiene los procesos de gestión de las operaciones, las solicitudes de servicio e incidentes, problemas, continuidad, servicios de seguridad y los controles de los procesos de negocio.

El cuarto dominio de gestión, MEA, incluye aquellos procesos que son responsables de la evaluación de la calidad en el cumplimiento de los requisitos de control de todos los procesos mencionados anteriormente. Se ocupa de la gestión del desempeño, el monitoreo del control interno y el cumplimiento de normas de regulación. (Isaca, 2012)

4. Permitir un Enfoque Holístico

El cuarto principio explica que la aplicación eficiente y eficaz del gobierno y la gestión de la empresa de TI requiere un enfoque holístico. Este enfoque tiene en cuenta varios componentes que interactúan: procesos, estructuras organizativas y los recursos humanos. Este desafío está relacionado con la implementación de lo que se describe en la literatura de gestión estratégica como la necesidad de un sistema de organización, es decir, cómo una empresa consigue que su gente trabaje en conjunto para cumplir con el negocio (De Wit & Meyer, 2005). Tal sistema de organización requiere la definición y aplicación de las estructuras (por ejemplo, unidades de organización y funciones) y procesos (para asegurar que las tareas son coordinadas e integradas), y la atención a las personas y los aspectos relacionales (por ejemplo, cultura, valores, creencias conjuntas).

COBIT 5 incorpora un modelo de “Catalizadores” en su marco (Figura 11). Estos son factores que, individual y colectivamente, influyen en que algo va a funcionar, en este caso, el gobierno y la gestión sobre las TI corporativas. El marco describe siete categorías de catalizadores, de los cuales los “procesos”, “las estructuras organizacionales” y “la cultura, el comportamiento y la ética” se relacionan estrechamente con el concepto de sistemas de organización.

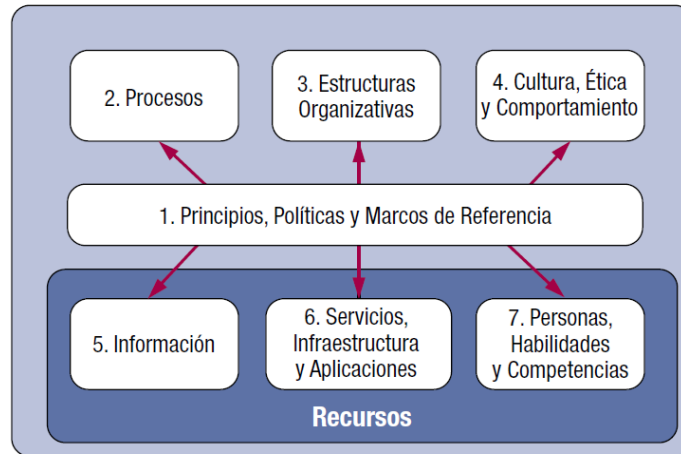


Figura 11 Catalizadores de COBIT 5. Fuente: Isaca (2012)

- **Principios, Políticas y Marcos**

Son el vehículo para trasladar el comportamiento deseado en guías prácticas para la gestión diaria.

- **Procesos**

Describen un conjunto de prácticas y actividades organizadas para cumplir con ciertos objetivos y producir un conjunto de salidas para alcanzar los objetivos generales relacionados con TI.

- **Estructuras Organizacionales**

Son las entidades claves en la toma de decisiones de la empresa.

- **Cultura, Ética y Comportamiento**

La cultura, ética y comportamiento de los individuos y de la empresa muchas veces son sobrestimados como un factor de éxito en las actividades de gobierno y gestión.

- **Información**

Requerida para mantener la empresa en ejecución y bien gobernada. En el nivel operacional, la información es un producto clave de la empresa.

- **Servicios, Infraestructura y Aplicaciones**

Incluye la infraestructura, la tecnología y las aplicaciones para proveer a la empresa los servicios y procesamiento de Tecnología de la Información.

- **Personas, Habilidades y Competencias**

Requeridas para completar con éxito las actividades y para tomar las decisiones correctas y acciones correctivas.

5. Separar el Gobierno de la Gestión

Por último, el principio 5 trata la diferencia que COBIT 5 hace entre gobierno y gestión. Esto se basa principalmente en la orientación de la norma ISO/IEC sobre “gobierno

corporativo de TI” (ISO/IEC, 2008) y los marcos generales de gobierno, tales como COSO. Había elementos de gobierno dentro de las versiones anteriores de COBIT, pero que se mezclaron con los aspectos de gestión. En COBIT 5, la organización de los procesos de gobierno sigue el modelo EDM (Evaluar-Dirigir-Monitorizar). Según lo establecido en la norma ISO 38500:2000, los procesos de gobierno de TI son responsabilidad del consejo de administración de la empresa y el aseguramiento de los objetivos se logran mediante la evaluación de las necesidades de las partes interesadas; establecer la dirección a través de establecimiento de prioridades y la toma de decisiones; y monitorear el desempeño, el cumplimiento y el progreso según los planes que se establecieron. Sobre la base de estas actividades de gobierno, el negocio y gestión de TI: planear, construir, ejecutar, y monitorear actividades (una traducción de COBIT del ciclo de Deming: Plan, Do, Check, Act) en alineación con la dirección establecida por el órgano de gobierno para alcanzar los objetivos empresariales.

Para cumplir con los principios mencionados, la dimensión de los Procesos de TI se organiza en una estructura de cinco dominios, separados en dos áreas, una de gobierno (EDM) y otra de Gestión (APO, BAI, DSS y MEA).

5.2.3 ISO/IEC 38500:2000

La Norma ISO 38500 es un estándar internacional que provee directrices para el gobierno corporativo de TI y ayuda a los miembros de altos niveles de una organización a entender y cumplir cabalmente sus obligaciones legales, regulatorias y éticas respecto del uso de TI en las organizaciones.

Esta norma define el buen gobierno de TI como el sistema usado por la alta dirección de la organización para controlar el uso presente y futuro de las TI en la organización, de manera que se consigan los planes y objetivos de la misma.

Bases de la Norma ISO/IEC 38500:2000

La Norma se basa en que la alta dirección *evalúe, dirija y monitoree* el uso que se hace de las TI en sus organizaciones, tal como se muestra en la Figura 12. No obstante, estas son directrices generales y no indican algún tipo de actividades, entradas, salidas, ni proceso alguno para indicar el cómo se utilizarán, sino que tiene como fin indicar el QUÉ debe cumplirse, dejando a criterio de los usuarios el CÓMO.

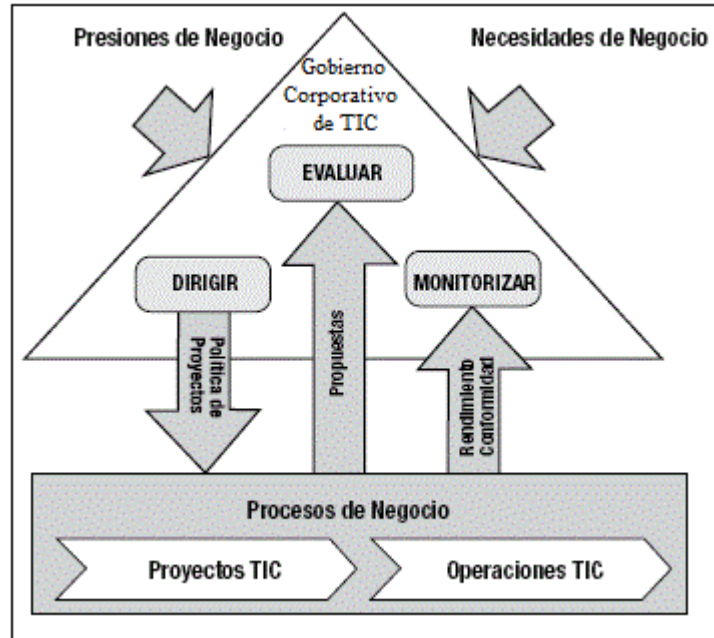


Figura 12 Modelo de gobierno corporativo de TIC ISO/IEC 38500:2000. Fuente: ISO/IEC (2008)

- **Evaluar:** La dirección debe examinar y juzgar sobre el uso actual y futuro de las TI, incluyendo estrategias, propuestas y acuerdos de cómo se proveerán los recursos necesarios (ya sea internos, externos, o ambos). (ISO/IEC, 2008)
- **Dirigir:** La dirección debe asignar la responsabilidad, y la preparación directa y aplicación de planes y políticas.
Asegurar la correcta transición de los proyectos a la producción considerando los impactos en la operación, el negocio y la infraestructura.
Impulsar una cultura de buen gobierno de TI en la organización. (ISO/IEC, 2008)
- **Monitorizar:** La dirección debe vigilar, a través de sistemas de medición adecuados, el rendimiento de las TI. Deben convencerse que el rendimiento está en conformidad con los planes, en particular con respecto a los objetivos de negocio. (ISO/IEC, 2008)

Principios de la Norma ISO/IEC 38500:2000

La norma define seis principios de un buen gobierno corporativo de TIC:

Responsabilidad

Los individuos y grupos dentro de la organización deben comprender y aceptar su responsabilidad con respecto a la oferta y la demanda de TI. Las personas con responsabilidad de las acciones también tienen la autoridad para llevar a cabo esas acciones. (ISO/IEC, 2008)

Estrategia

Se consideran los planes estratégicos de TI para satisfacer las necesidades actuales y futuras derivadas de la estrategia de negocio. La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TI. (ISO/IEC, 2008)

Adquisición

Las adquisiciones de TI se hacen por razones válidas, sobre la base de adecuada y análisis en curso, con la decisión clara y transparente de decisiones. Hay equilibrio adecuado entre los beneficios, oportunidades, costos y riesgos, tanto a corto y largo plazo. (ISO/IEC, 2008)

Rendimiento

Las TI debe estar dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras. (ISO/IEC, 2008)

Conformidad

Cumple con todas las legislaciones y normas obligatorias. Las políticas y prácticas están claramente definidas, aplicadas y ejecutadas. (ISO/IEC, 2008)

Factor Humano

Las políticas de TI, las prácticas y decisiones demuestran respeto al factor humano, incluyendo las necesidades actuales y futuras de todas las personas involucradas. (ISO/IEC, 2008).

En la Tabla 4 se ofrece una mirada global de cómo cada principio mencionado anteriormente debe cumplir sus bases (Dirigir, Monitorizar y Evaluar).

Tabla 4 Guía Orientativa para gobierno de TI basado en ISO/IEC 38500:2000 Fuente: Ballester (2009)

Principios	Dirigir	Monitorizar	Evaluar
Responsabilidad	Planes con Responsabilidad Asignada	Mecanismos establecidos gobierno de TI	Asignación Responsabilidades
	Recibir información y Rendir Cuentas	Asignación Responsabilidades (entendimiento)	Competencias de Responsables
		Desempeño responsable gobierno de TI	
Estrategia	Creación y uso de Planes y Políticas	Progreso Propuestas Aprobadas	Progreso Propuestas Aprobadas
	Asegurarse Beneficios TI en el Negocio	Alcanzar Objetivos en Plazos establecidos	Evaluar actividades TIC y Alineamiento
	Alentar propuestas innovadoras	Utilizar Recursos Asignados	Mejores Prácticas
		Uso de TIC, alcanzando Beneficios esperados	Satisfacción Interesados
			Valoración y Evaluación de Riesgos
Adquisición	Activos TI Adquieren manera apropiada	Inversiones y Capacidades Requeridas	Alternativas Propuestas
	Documentos Capacidad Requerida	Entendimiento Interno/Externo Necesidades Negocio	Propuestas Aprobadas
	Acuerdos de Provisión respalden Necesidades Negocio.		Análisis de Riesgo / Valor
			Inversiones
Rendimiento	Asignación Recursos suficientes	Grado TIC Sustenta Negocio	TIC Sustenta Procesos Negocio Dimensionado y Capacidad
	Asignar Prioridades y Restricciones	Recursos e Inversiones Priorizados Necesidades Negocio	Riesgos: Continuidad Operaciones

	Datos Correctos, Actualizados, Protegidos	Políticas Precisión Datos	Riesgos: Integridad Información, Protección Activos
		Políticas Uso Eficiente TIC	Decisiones uso TIC apoyo al Negocio
			Eficacia y Desempeño gobierno de TI
Cumplimiento	TI Cumple Obligaciones, Normas y Directrices	Cumplimiento y Conformidad (Auditorias/Informes)	TIC Cumple Obligaciones, Normas y Directrices
	Establecer y Aplicar Políticas (uso TI Interno)	Oportunos, Completos, Adecuados (Necesidades Negocio)	Conformidad gobierno de TI
	Personal TIC cumple directrices Desarrollo y Conducta	Actividades de TIC	
	Ética rija acciones relacionadas TIC		
Factor Humano	Actividades TI Compatibles Factor Humano	Actividades TIC, identificar, prestar atención	Actividades TIC, identificar
	Informar cualquier individuo (riesgos, problemas)	Prácticas de trabajo consistente uso apropiado TIC	Actividades TIC, considera debidamente
	Administración Riesgos Según Políticas y Procedimientos.		
	Escalado a los Decisores		

5.2.4 Comparación entre Modelos

La Tabla 5 muestra un cuadro resumen entre los tres framework de gobierno de TI con el fin de facilitar la comprensión. Posteriormente se hace una comparativa en mayor detalle entre modelos.

Tabla 5 Matriz de Resumen. Conceptos generales de marcos de gobierno de TI. Fuente: Elaboración Propia

Framework	Objetivo	Definición IT Governance	Estructura y/o Principios	Dominios		Referencia
COBIT 4.1	Alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.	Estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la empresa y añadir valor mientras se balancean los riesgos versus el retorno sobre TI y sus procesos.	<ol style="list-style-type: none"> 1. Aportar Valor 2. Gestión del Riesgo 3. Gestión de los Recursos 4. Gestión del Rendimiento 5. Alineamiento Estratégico 	<ol style="list-style-type: none"> 1. Planear y Organizar 2. Adquirir e Implementar 3. Entregar y Dar Soporte 4. Monitorear y Evaluar 		(ITGI, COBIT 4.1, 2007)
ISO 38500	Usar las tecnologías de la información de manera efectiva, óptima y eficiente en las organizaciones, con la finalidad de: Generar confianza en los stakeholders en el gobierno corporativo de TIC de la organización. Informar y guiar a la alta dirección en el gobierno de TI en su organización. Proveer de bases para la evaluación objetiva del gobierno corporativo TIC	Sistema por el cual el uso de TI actual y futuro es dirigido y controlado. El gobierno corporativo de TI consiste en evaluar y dirigir el uso de las TI para apoyar a la organización y monitorear su uso para el logro de los planes. Esto incluye la estrategia y políticas para el uso de TI dentro de la organización	<ol style="list-style-type: none"> 1. Responsabilidad 2. Estrategia 3. Adquisición 4. Rendimiento 5. Conformidad 6. Factor Humano 	<ol style="list-style-type: none"> 1. Evaluar 2. Dirigir 3. Monitorizar 		(ISO/IEC, 2008)
COBIT 5	<p>Proveer de un marco de trabajo integral que ayude a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas.</p> <p>Permitir 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</p>	<p>Un enfoque de gobierno que garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la empresa y la consecución de las metas corporativas. También incluye el gobierno funcional de TI, por ejemplo, garantizando que las capacidades de TI son provistas de forma eficiente y efectiva.</p>	<ol style="list-style-type: none"> 1. Satisfacer las Necesidades de las Partes Interesadas 2. Cubrir la Empresa Extremo a Extremo 3. Aplicar un Marco de Referencia único integrado 4. Hacer Posible un Enfoque Holístico 5. Separar el Gobierno de la Gestión 	Gobierno	Gestión	(Isaca, 2012)
				<p>Evaluar Orientar y Supervisar</p>	<ol style="list-style-type: none"> 1. Alinear, Planificar y Organizar 2. Construir, Adquirir e Implementar 3. Entregar, Dar Servicio y Soporte 4. Supervisar, Evaluar y Valorar 	

COBIT 4.1 vs COBIT 5

Los principales cambios y/o adiciones en COBIT 5:

1. **Nuevos Principios de GEIT:** COBIT 5 ha integrado el contenido de COBIT 4.1, VALIT y Risk IT en un Modelo de Referencia de Procesos.
2. **Catalizadores.** COBIT 5 integra el concepto de catalizadores en su marco, el cual no se encuentra de forma explícita en COBIT 4.1. La Tabla 6 muestra el mapeo de los Catalizadores entre ambas versiones.

Tabla 6 Mapeo de Catalizadores entre COBIT 4.1 y COBIT 5. Fuente: Elaboración Propia

Mapeo de Catalizadores COBIT	
COBIT 5	COBIT 4.1
Principios, Políticas y Marcos de Referencia	Mencionados Algunos Procesos
Procesos	Eje Central del Framework
Estructura Organizativa	Implícita en la Matriz RACI
Cultura, Ética y Comportamiento	Mencionados Algunos Procesos
Información	Recursos
Servicios, Infraestructura y Aplicaciones	Recursos
Personas, Habilidades y Competencias	Recursos

3. **Nuevo Modelo de Referencia de Procesos:** COBIT 5 se basa en un modelo de referencia de proceso con un nuevo dominio de gobierno y varios procesos nuevos y modificados que ahora cubren las actividades empresariales de extremo a extremo, es decir, el negocio y las áreas funcionales de TI.
4. **Prácticas y Actividades:** Las prácticas de gobierno y de administración de COBIT 5 son equivalentes a los objetivos de control de COBIT 4.1 y los procesos de Val IT y Risk IT. Las actividades de COBIT 5 son equivalentes a las prácticas de control de COBIT 4.1 y a las prácticas de administración de Val IT y Risk IT.
5. **Metas y Métricas más desarrolladas:** COBIT 5 sigue el mismo concepto y objetivo de métricas de COBIT 4.1, Val IT y Risk IT, pero éstas se renombran como objetivos de la empresa, objetivos relacionados con la TI y objetivos de proceso reflejando una visión de empresa.
6. **Entradas y Salidas a nivel de práctica:** COBIT 5 ofrece entradas y salidas para cada práctica de manejo, mientras que COBIT 4.1 las proporciona a nivel de proceso.
7. **Matriz RACI:** Los modelos de responsabilidad RACI de COBIT 5 incorpora un set de nuevos actores dentro de la matriz haciéndola más completa.
8. **Método de Medición de Madurez de los Procesos:** En COBIT 5 desaparece el modelo de madurez de capacidades- CMM aplicado a los procesos de COBIT 4.1 para introducir un modelo basado en la ISO/IEC 15504.

9. Procesos Nuevos y Modificados: La cantidad de procesos se ha incrementado de 34 a 37. Si bien los objetivos de control que corresponden a cada proceso de COBIT 4.1, se mantienen mayoritariamente dentro del mismo Dominio, existen excepciones como las siguientes:

- PO10 – Administrar los proyectos, pasó al Dominio BAI de COBIT 5.
- AI5 – Procurar recursos de IT, pasó al Dominio APO de COBIT 5.
- DS1 – Definir y Administrar los niveles de servicio, pasó al Dominio APO de COBIT 5.
- DS2 – Administrar los servicios de Terceros, pasó al Dominio APO de COBIT 5.
- DS3 – Administrar el desempeño y la capacidad, pasó al Dominio BAI de COBIT 5.
- DS6 – Identificar y asignar costos, pasó al Dominio APO de COBIT 5.
- DS7 – Educar y Entrenar a los usuarios, pasó al Dominio APO de COBIT 5.

En el dominio APO – Administrar, Planear y Organizar, es donde se observa mayor reorganización interna de los objetivos de control, es decir que un antiguo proceso de COBIT 4, ahora puede estar distribuido como parte de hasta 5 procesos del mismo dominio en COBIT 5.

El proceso DS12 – Administrar el Ambiente Físico ahora forma parte del DSS5-Gestionar los Servicios de Seguridad.

Existen nuevos procesos cuyo contenido es mayormente producto de COBIT 5, destacándose:

- EDM1 – Definir el Framework para el gobierno
- APO1 – Definir el Framework para el Management
- APO4 – Gestionar Innovación
- APO13 – Gestionar Seguridad (también hay un Proceso DSS05 Gestionar los Servicios de Seguridad)
- BAI8 – Gestión del Conocimiento

A continuación, se expone en la Tabla 7 el mapeo realizado entre los procesos de COBIT 4.1 y su cobertura en COBIT5, destacando que se tomó como fuente el material de ISACA incluido en Anexo de la Guía de Procesos de Referencia, consolidados a nivel Proceso, destacando al Proceso de COBIT 5 que mayor cobertura (en porcentaje) les brinda a los objetivos de control del antiguo proceso de COBIT 4.1.

Tabla 7 Mapeo COBIT 4.1 vs COBIT 5 a nivel de Proceso. Fuente: Franco.IT-grc (2012)

COBIT 4.1		COBIT 5	
ID Proceso	Nombre Proceso	ID Proceso	Nombre Proceso
PO	Planear Y Organizar	APO	Alinear, Planear y Organizar
P01	Definir un Plan Estratégico de TI	APO02	Gestionar la Estrategia
P02	Definir la Arquitectura de la Información.	APO03	Gestionar la Arquitectura Empresarial
P03	Determinar la Dirección Tecnológica	APO02	Gestionar la Estrategia
		APO04	Gestionar la Innovación
P04	Definir los Procesos, Organización y Relaciones de TI	APO01	Gestionar el Marco de Gestión de TI
P05	Administrar la Inversión en TI	APO06	Gestionar el Presupuesto y Los Costes

P06	Comunicar las Aspiraciones y la Dirección de la Gerencia	APO01	Gestionar el Marco de Gestión de TI
P07	Administrar Recursos Humanos de TI	APO07	Gestionar Los Recursos Humanos
P08	Administrar la Calidad	APO11	Gestionar la Calidad
P09	Evaluar y Administrar los Riesgos de TI	APO12	Gestionar el Riesgo
P10	Administrar Proyectos	BAI01	Gestionar los Programas y Proyectos
AI	Adquirir e Implementar	BAI	Construir, Adquirir e Implementar
AI1	Identificar soluciones automatizadas	BAI02	Gestionar la Definición de Requisitos
AI2	Adquirir y mantener software aplicativo	BAI03	Gestionar la Identificación y la Construcción de Soluciones
AI3	Adquirir y mantener infraestructura tecnológica	BAI03	Gestionar la Identificación y la Construcción de Soluciones
AI4	Facilitar la operación y el uso	BAI08	Gestionar el Conocimiento
AI5	Adquirir recursos de TI	APO10	Gestionar los Proveedores
AI6	Administrar cambios	BAI06	Gestionar los Cambios
AI7	Instalar y acreditar soluciones y cambios	BAI07	Gestionar la Aceptación del Cambio y de la Transición
DS	Entregar y Dar Soporte	DSS	Entregar, Dar Soporte y Servicio
DS1	Definir y administrar los niveles de servicio	APO09	Gestionar los Acuerdos de Servicio
DS2	Administrar los servicios de terceros	APO10	Gestionar los Proveedores
DS3	Administrar el desempeño y la capacidad	BAI04	Gestionar la Disponibilidad y la Capacidad
DS4	Garantizar la continuidad del servicio	DSS04	Gestionar la Continuidad
DS5	Garantizar la seguridad de los sistemas	DSS05	Gestionar los Servicios de Seguridad
DS6	Identificar y asignar costos	APO06	Gestionar el Presupuesto y Los Costes
DS7	Educar y entrenar a los usuarios	APO07	Gestionar Los Recursos Humanos
DS8	Administrar la mesa de servicio y los incidentes	DSS02	Gestionar las Peticiones e los Incidentes del servicio
DS9	Administrar la configuración	BAI10	Gestionar la Configuración
DS10	Administrar los problemas	DSS03	Gestionar los Problemas
DS11	Administrar los datos	DSS04	Gestionar la Continuidad
DS12	Administrar el ambiente físico	DSS01	Gestionar las Operaciones
		DSS05	Gestionar los Servicios de Seguridad
DS13	Administrar las operaciones	DSS01	Gestionar las Operaciones
ME	Monitorizar y Evaluar	MEA	Supervisar, Evaluar y Valorar
ME1	Monitorear y Evaluar el Desempeño de TI	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad
ME2	Monitorear y Evaluar el Control Interno	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno
ME3	Garantizar el Cumplimiento Regulatorio	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
		EDM	Evaluar, Orientar y Supervisar
ME4	Proporcionar gobierno de TI	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de gobierno
		EDM02	Asegurar la Entrega de Beneficios
		EDM03	Asegurar la Optimización del Riesgo
		EDM04	Asegurar la Optimización de los Recursos
		EDM05	Asegurar la Transparencia hacia las partes interesadas

COBIT 5 vs ISO 38500:2000

En la versión de COBIT5 existe una separación entre procesos de Gestión y procesos orientados al gobierno de TI, en claro alineamiento con la norma ISO/IEC 38500 (Evaluar, Dirigir, Monitorizar). El dominio sobre el gobierno en el modelo de procesos COBIT 5 tiene cinco procesos, cada uno de los cuales tiene definidas prácticas EDM. Este es el principal lugar en COBIT 5 donde se definen actividades relativas al gobierno. La Figura 13 muestra cómo las prácticas de gobierno están interactuando con las prácticas de Gestión.

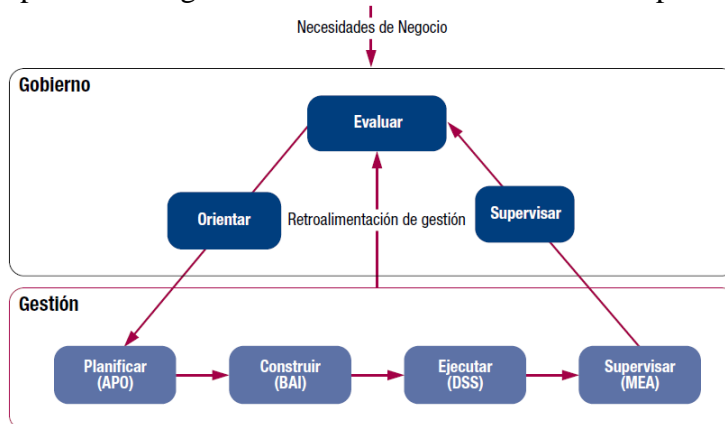


Figura 13 Áreas Claves de gobierno y Gestión de COBIT. Fuente: Isaca (2012)

Los principios de la norma ISO/IEC 38500:2000 se indican en la Figura 14, enlazándolos uno a uno con las orientaciones de COBIT 5 definidas en distintos elementos del framework, como catalizadores (procesos, personas, estructuras organizativas, etc.), metas u otros.

ISO 38500:2000	V/S	COBIT 5
Responsabilidad	→	Procesos, Estructuras Organizativas y Matriz RACI
Estrategia	→	Dominio APO, Proceso EDM02, Metas Empresariales, Metas Relacionadas a TI
Adquisición	→	Dominio BAI, Procesos APO05, APO12, APO11, EDM03, EDM04, EDM05
Rendimiento	→	Metas y Métricas, Evaluación de Capacidades, Procesos APO02, APO09, MEA01.
Conformidad	→	Evaluación de Capacidades, Procesos APO02, MEA02, MEA03
Comportamiento Humano	→	Catalizadores Personas, habilidades y Competencias, Cultura, Ética y Comportamiento, Procesos APO07, BAI02, BAI05, BAI08.

Figura 14 Cuadro de Enlace De Principios ISO/IEC 38500:2000 con Elementos COBIT 5. Fuente: Elaboración propia.

5.3 Algunos estándares que apoyan el gobierno TI

Los marcos de referencia con herramientas sólidas son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio y que los servicios y la información satisfagan los requisitos de calidad, financieros y de seguridad.

De acuerdo con los marcos de control presentados se observa la presencia de estándares que apoyan el gobierno de TI en alguno de ellos, los que permiten materializar el “cómo” para diferentes controles de TI. Se podrían mencionar la norma ISO 27001, norma ISO 20000, BS 7799, ITIL, PMBok, CMMI, entre otros (Smits & Hillegersberg, 2013). En la sección de Anexos se definen dos de estos estándares: ITIL y la norma ISO 27001. Se eligieron los estándares mencionados ya que éstos son los más utilizados según las entrevistas (Smits & Hillegersberg, 2013).

6. ANÁLISIS SITUACIÓN ACTUAL

6.1 Datos Generales Empresa

A continuación se presenta la información general de la empresa en cuestión, extraída del sitio web oficial de la organización.

6.1.1 Visión de la Empresa

- Ser un operador de clase mundial en servicios sanitarios al que sus clientes elegirían por su eficiencia y alta calidad de servicio (Essbio, 2014).

6.1.2 Misión de la Empresa

- Proveer soluciones y servicios de alta calidad en el ciclo integral del agua (agua potable, alcantarillado y descontaminación de aguas servidas) y en la gestión integral de residuos.
- Entregar un servicio de excelencia, basado en un profundo conocimiento de nuestros clientes, altos niveles de eficiencia e innovación, y un verdadero compromiso de responsabilidad social con la comunidad y el medioambiente.
- En el contexto de la permanente generación de valor para nuestros accionistas.
- Todo esto gracias al trabajo de un equipo de personas satisfechas y orgullosas con su vida. (Essbio, 2014)

6.1.3 Valores Corporativos de la Compañía

- **Transparencia**
Valor orientado del trabajo, que busca realizar acciones y tener conductas que no oculten o silencien la realidad de los hechos.
- **Confianza**
Enfocado a que las personas realicen acciones coherentes y consistentes, de manera que los otros lo perciban creíble y predecible, afianzando la relación.
- **Respeto**
Orientado a relacionarse con los otros, reconociendo, aceptando y apreciando sus cualidades y derechos hacia todos los sectores.
- **Excelencia**
Vista como una práctica común de cada miembro de la compañía, que hará creíble la transparencia, sustentable la confianza y permanente el respeto.

6.1.4 Plan Estratégico de la Empresa

El plan estratégico de la compañía está descrito en la Figura 15, cuya meta principal es aumentar el valor de la compañía. Contiene tres objetivos primordiales: Asegurar la rentabilidad del negocio, el crecimiento del negocio y la sostenibilidad del mismo. Cada uno de los tres objetivos se lograrán proponiendo sub-metas. Para asegurar la rentabilidad del negocio se debe disminuir los costos y/o aumentar los ingresos. Para dar crecimiento al negocio se debe potenciar el crecimiento de Biodiversa, empresa filial de ESSBIO, y crecer de esta manera en el negocio sanitario. Finalmente, para dar sostenibilidad simplemente se propone como sub-meta el mismo principio: asegurar la sostenibilidad del negocio. A su vez, cada una de estas sub-metas, contiene el cómo alcanzarlas y el plan indica en el esquema este nivel de detalle.

Por otro lado, también existen otras metas que no impactan directamente en la meta principal. No obstante, influyen de forma transversal en todas las metas incluidas en el plan estratégico. Dichas metas son las que se encuentran en el último nivel del diagrama (Figura 15): metas de procesos de información, el instaurar el estilo ESSBIO y el establecimiento de la cultura.

Por último, cuando se ejecuta el plan estratégico debe tener en cuenta los siguientes cinco enfoques al momento de seguir sus metas:

- **Reputación Integral:**

Construida alrededor de la credibilidad, confiabilidad y coherencia que los diferentes actores que impactan o se ven impactados por lo que hacemos, reconocen en nosotros.

- **Líder en desarrollo Regional:**

Ser un actor clave en el desarrollo de las regiones donde interactuamos, construyendo alianzas estratégicas con nuestros públicos de interés.

- **Servicio Impecable:**

Considera una operación intachable que responda a las expectativas de nuestros clientes, autoridad y dueño.

- Capacidad de anticipación, de llegar a tiempo
- Eficiencia – cumplir, pero a un costo “justo”
- Orden y limpieza
- Entregamos un servicio que cumple los estándares de calidad

- **Innovación y emprendimiento:**

Hacer las cosas de la misma forma no nos permitirá diferenciarnos o alcanzar la reputación que anhelamos, necesitamos pensar y hacer las cosas de manera diferente, necesitamos innovar en procesos, ideas y actitudes.

- **Personas:**

Considera equipos de alto desempeño caracterizados por su pro-actividad, trabajo transversal y orientación a los resultados. Implica una actitud diferente frente a los desafíos y problemas.

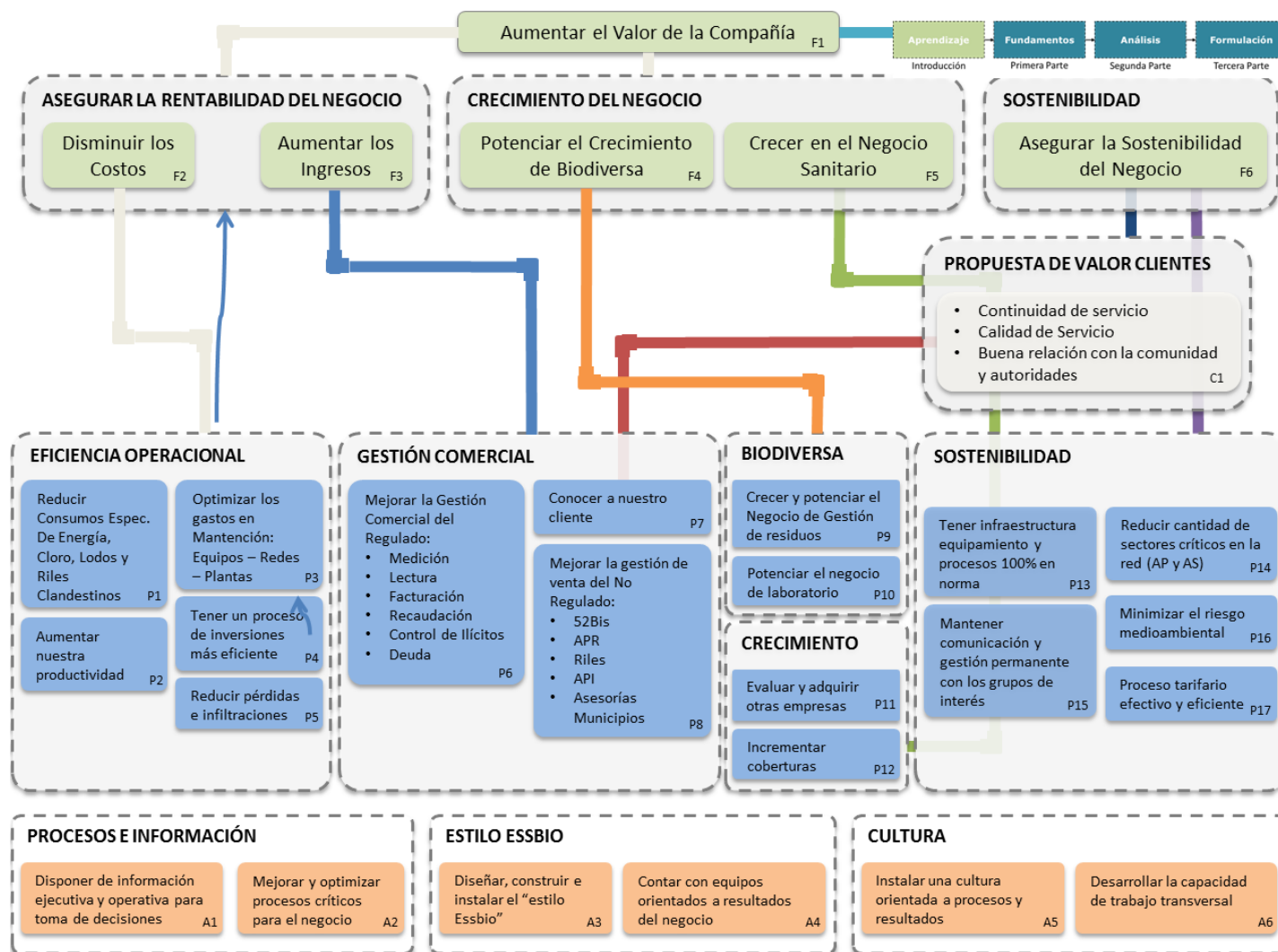


Figura 15 Plan Estratégico ESSBIO. Fuente: Essbio (2014)

6.2 Datos Subgerencia de Informática de ESSBIO

A continuación se presenta la información asociada a la subgerencia de informática de la organización.

6.2.1 *Visión de la Subgerencia de Informática*

- Ser un área de informática referente para el resto de sanitarias y empresas del país, basando nuestro trabajo en una relación de partners con nuestros clientes internos y desarrollando un trabajo del más alto nivel. (Essbio, Portal de Colaboración ESSBIO S.A., 2014)

6.2.2 *Misión de la Subgerencia de Informática*

- Desarrollar soluciones que generen alto valor al negocio, por medio de la transformación y mejoramiento de los procesos corporativos y la innovación tecnológica, asegurando la continuidad operacional y garantizando la seguridad de la información, enmarcado en servicios informáticos de alta calidad.
- Generar soluciones con base tecnológica, alineados al plan estratégico y objetivos de la compañía, que permitan una optimización constante de los procesos de negocio.
- Garantizar la continuidad operacional de los procesos de negocio que posean apoyo tecnológico.
- Asegurar la rentabilidad de las inversiones computacionales e informáticas.
- Garantizar la continuidad, disponibilidad, seguridad y calidad de los servicios Informáticos corporativos.
- Optimizar los costos operacionales en el uso de tecnologías y sistemas de información. (Essbio, Portal de Colaboración ESSBIO S.A., 2014)

6.2.3 *Plan Estratégico de Trabajo*

Se cuenta con un plan de trabajo que abarca tres años. Este plan está resumido en la pirámide de la Figura 16, el cual comprende cuatro períodos principales. El primer período se denomina de transición. En esta fase se define las bases para tener una subgerencia de informática de excelencia, el cual comprende la definición de la visión y misión del área en base a lo que se quiere lograr y proyectar; la administración, el cual define los parámetros con los cuales esta subgerencia opera y cómo se comunican sus actores; y la estructura y organización de la subgerencia, el cual comprende su organización interna basado en pilares que sostienen el modelo de organización actual explicado más adelante en este documento con la Figura 17.

El segundo período se denomina consolidación. En esta fase se consideran cuatro etapas principales: Modelo operativo y gestión, la cual establece los distintos modelos para la realización de las diferentes funciones de la subgerencia de informática, tales como modelo de gestión de proyectos, modelo de infraestructura, entre otros. Por otro lado, en esta etapa, se establecen las políticas de seguridad de la información, la gestión del aseguramiento de

la calidad y todos los estándares, modelos y/o metodologías que se deban establecer para un funcionamiento con excelencia. La segunda etapa comprendida en el período de consolidación, es la formalización. Aquí se debe documentar, bajo los lineamientos de la compañía, todos los procedimientos, fuentes, modelos y procesos de la subgerencia de informática, con el fin de que ésta genere conocimiento sostenido en el tiempo. La tercera etapa de este período es la de contar con indicadores y gestión, la cual busca tener parámetros internos de comparación para evaluar el desempeño de la subgerencia dentro de la compañía. Por último, en este período se establece un plan de desarrollo de la agenda de proyectos, que también se incluye en el período siguiente.

Sumado a lo anterior, en este período aparece un nuevo pilar de la pirámide que acompaña a todo el resto de los períodos: el pilar de la eficiencia. Esta columna surge luego que ya se han asentado las bases de la estrategia, pensando en que en ese momento se puede comenzar a pensar en cómo ser más eficientes; eficientes en los modelos, procedimientos, administración y todo lo que abarque la subgerencia.

El siguiente período, denominado mejora continua, comprende tres etapas: la continuación del plan de desarrollo; el portafolio de proyectos-agenda de desarrollo, el cual se genera desde un trabajo en equipo con otras áreas de la compañía. Este trabajo pretende descubrir, según la visión y proyección particular de cada área, y la detección de necesidades desde su punto de vista, cuáles son las mejores soluciones tecnológicas que se deben incluir en el portafolio de proyectos; y por último la etapa de cobertura de procesos y negocio, el cual, mediante un conocimiento exhaustivo del negocio, propone soluciones de negocio para cubrir sus procesos desde la subgerencia de informática hacia las demás áreas de la compañía.

Finalmente, se concluye con un período de excelencia que cuenta con dos etapas. La primera, que corresponde a estándares comparable, la cual establece indicadores que le permite contrastarse con otras áreas de TI de otras compañías. La segunda etapa, procesos que hablen, que incluye una formalización y profundización de los procesos tal, que éstos por sí mismo muestren las necesidades tecnológicas que hacen falta. Lo anterior tiene como objetivo conocer certeramente el porcentaje de cobertura que tienen los procesos con tecnologías actualmente para así generar propuestas que amplíen dicha cobertura.

En este plan de trabajo se incorporan dos conceptos que participan de modo transversal: la capacitación, el cual procura tener expertos en cada área que no sólo solucionen problemas temporalmente, sino que generen soluciones de negocio que perduren y solidifiquen a la compañía. El segundo concepto incorporado es el modelo de gobierno de TI, el cual debe establecer cuál es el modelo en el cual se debe basar la subgerencia de informática para operar en todos sus aspectos.

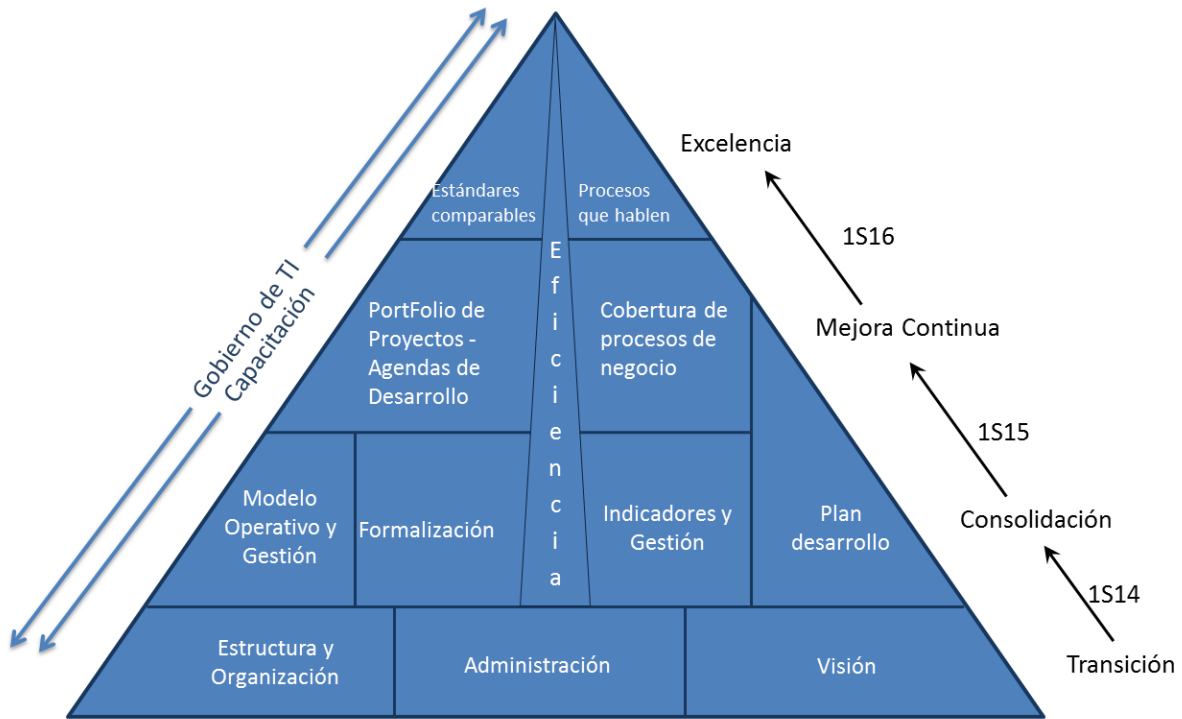


Figura 16 Plan Estratégico Subgerencia Informática Años 2014-2016. Fuente: Elaboración Subgerente Informática ESSBIO

6.3 Modelo de Organización Actual de Subgerencia de Informática

Modelo Actual de la Subgerencia de Informática

El objetivo principal de la subgerencia de informática consiste en desarrollar soluciones que generen **alto valor al negocio**, por dicho motivo, se encuentra encabezando el diagrama del modelo actual (Figura 17). Este valor debe ser medible y capitalizable, de tal manera que se compruebe cuánto valor generó alguna solución en comparación con lo que se proyectó que se generaría.

Los cuatro pilares que sostienen el modelo son: Soluciones de Negocio, Visión Transversal alineada a la Estrategia, Unidad de Servicios de Negocio, Tecnología como medio y no como fin. Al considerar estos cuatro pilares, se asegura que los proyectos y/o tareas que se desarrollen generan valor al negocio y definen en sí la estructura y organización de la subgerencia, que se compone de cinco áreas: BPM, Operaciones, Infraestructura, Seguridad/QA y Soporte Corporativo SAP. (Puente, 2014). A raíz de esta estructura se compone el organigrama de la subgerencia (Figura 18): Encabezando el organigrama se encuentra el subgerente de informática, segundo, se encuentra el oficial de seguridad y control de calidad, monitorizando de manera transversal a la subgerencia todos los temas relacionados al cargo, dando informes directos a su jefatura. Luego, se encuentran los cuatro departamentos mencionados anteriormente, el cual cada uno cuenta con un grupo humano para realizar las labores pertinentes según sea la propia organización de cada área.



Figura 17 Modelo de Organización Actual de Subgerencia de TI Fuente: Elaboración Subgerente Informática ESSBIO

6.3.1 Organigrama Subgerencia de Informática ESSBIO

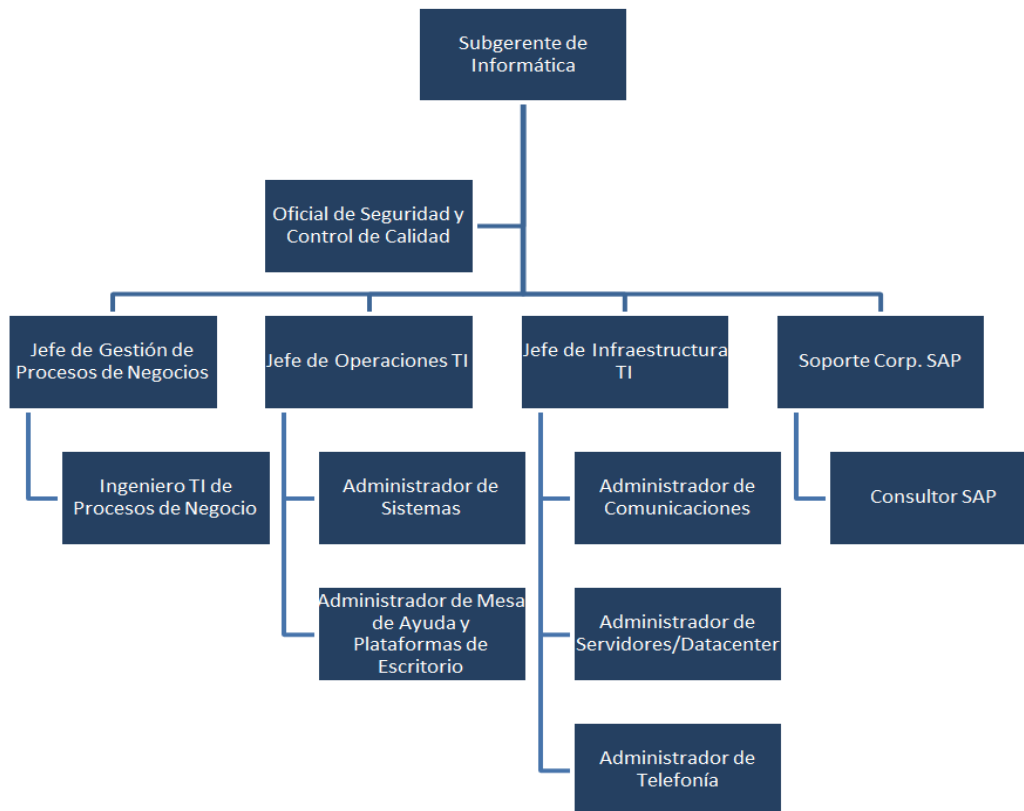


Figura 18 Organigrama Subgerencia de Informática ESSBIO. Fuente: Essbio (2014)

6.3.2 *BPM*

El Área encargada de Gestión de Procesos de Negocio desde que una iniciativa es propuesta por un usuario hasta que es implementada. (Puente, 2014).

El objetivo primordial de este departamento es apoyar a todas las áreas del negocio para desarrollar soluciones que generen valor a la compañía.

Actualmente las iniciativas nacen desde los usuarios, quienes generan propuestas tecnológicas, las cuales son analizadas por este departamento para comprobar la viabilidad de un nuevo proyecto. El análisis se realiza de acuerdo a una serie de criterios bien definidos, principalmente, cuánto valor genera al negocio. Luego, la iniciativa es presentada al comité de inversión, el cual es encargado de aprobar o posponer dicho proyecto (Muñoz M. , 2014).

En la primera etapa de análisis se verifica si la propuesta es acorde a la estrategia de la compañía. Si corresponde a un proyecto nuevo, a la mejora de algún sistema ya existente o bien, a la corrección del uso de la tecnología disponible. Luego, se verifica cómo la propuesta se comunica o afecta a otros procesos de la compañía, si tiene aspectos legales a considerar, si amerita ampliar su alcance u otras observaciones pertinentes (Muñoz M. , 2014).

6.3.3 *Operaciones*

Área encargada de garantizar la continuidad operacional de las soluciones existentes en la compañía y de las tecnologías de escritorio, trabajando con actividades de mantenimiento, tanto de crecimiento como de corrección para un uso de los sistemas completo y correcto. (Puente, 2014).

Este departamento, para asegurar la continuidad operacional de las soluciones, realiza diferentes funciones: administra una mesa de ayuda, la cual se encarga de verificar que cada solicitud por parte de los usuarios o ticket, se resuelva dentro de los plazos definidos por el catálogo de servicios (SLA); entrega soporte a los sistemas existentes, este proceso lo efectúa a través de la mesa de ayuda. Cada sistema tiene designado uno o varios administradores, los cuales, al llegar una solicitud a través de la mesa de ayuda, lo diagnostican y, si se trata de problemas de configuración, lo resuelven. Cuando escapa de dicho alcance, entonces es derivado a un proveedor externo; administra la plataforma de escritorio de la compañía, la cual se encarga de monitorear los contratos de los computadores, notebooks e impresoras de la empresa y de realizar la renovación de éstos cuando su vida útil caduca; y se encarga del licenciamiento de software (Ruiz, 2014).

6.3.4 *Infraestructura*

El área responsable de la mantención de hardware de comunicaciones y servidores de la compañía, además de la actualización, instalación y desinstalación de productos de software y sistemas de información (Puente, 2014).

Además este departamento se encarga de administrar los servidores y los enlaces de comunicación de toda la compañía. Esto incluye: Almacenamiento de datos, software, correo electrónico, seguridad, telefonía fija y móvil (Muñoz H. , 2014).

La administración de datos se gestiona mediante el servicio de proveedores externos que administran la infraestructura y la plataforma, quedando en manos de la compañía las aplicaciones y datos (Muñoz H. , 2014).

El contrato con los proveedores define SLA en temas de seguridad frente al acceso de extraños, y también frente a la disponibilidad de la información. En aspectos de la

disponibilidad, la compañía verifica este acuerdo mediante un administrador interno, quien registra cada incidencia ocurrida, generando informes que permitan las acciones correspondientes frente a la falta de los acuerdos convenidos (Muñoz H. , 2014).

6.3.5 *Seguridad y Aseguramiento de la Calidad*

Área encargada de generar políticas de seguridad de la información de la compañía y del aseguramiento de la calidad de las operaciones internas de la subgerencia de informática (Puente, 2014).

Dentro de sus actividades directas, está a cargo de la realización de documentación de políticas, procedimientos u otros documentos concernientes con la seguridad y aseguramiento de la calidad. Lo anterior incluye, por ejemplo, procedimientos de solicitud de habilitación de cuentas, procedimientos de respaldo de datos, políticas de seguridad de la información, catálogo de acuerdos de servicios, etc. (Vera, 2014)

Además de la elaboración de documentación concerniente a seguridad y calidad, debe revisar la documentación de los procedimientos elaborados por otros departamentos de la subgerencia de TI en el marco de la aseguración de la calidad de los procedimientos (Vera, 2014).

El oficial de seguridad y control de calidad es el nexo oficial entre la subgerencia de informática y la gerencia de auditoría de la empresa, dando fluidez a todos los procesos de auditoría externos a la subgerencia de TI.

Además de las funciones mencionadas anteriormente, participa de la administración de las cuentas de red y otros sistemas de la compañía con el propósito de asegurar la calidad de la prestación del servicio y el acceso a la información de la compañía (Vera, 2014).

6.3.6 *SopORTE Corporativo SAP*

Área encargada del soporte corporativo de SAP ERP en finanzas, logística, abastecimiento, venta no regulada (la cual corresponde a toda aquella venta que no está regulada por las leyes chilenas), mantención y proyectos (Puente, 2014).

Este departamento debe mantenerse actualizado con la agenda SAP y mantenerse en constante investigación de los productos que ofrece. Esto es con el fin de contribuir al negocio nuevas soluciones que están relacionadas con el sistema que posee la organización cuando es pertinente. En este aspecto, trabaja en conjunto con el departamento BPM, ya que cuando nace una iniciativa de proyecto, primero se verifica si existe una solución de negocio con los productos que dispone SAP para que sea gestionado mediante esta vía (Ceballos, 2014).

Este departamento, además, apoya al área de operaciones cuando hay necesidad de soporte en SAP, que no ha podido ser resuelto por el departamento de operaciones. En tal escenario, los consultores senior del departamento de soporte corporativo prestan el servicio de soporte, y en el caso que no puede ser resuelto por la unidad, se gestiona el soporte con consultores externos (Ceballos, 2014).

En adición a lo anterior, este departamento realiza la gestión de conocimiento de la empresa, el cual se encuentra en la fase de estructurar y promover herramientas para dicha administración. (Ceballos, 2014)

6.4 Arquitectura de Información

En cuanto a la arquitectura de la información, como nuestra la Figura 19, se tiene cuatro niveles: nivel operacional, nivel transaccional, nivel control de Gestión y nivel de planeamiento estratégico. Cada uno de estos niveles cuenta con algún sistema de clase mundial. (Puente, 2014)

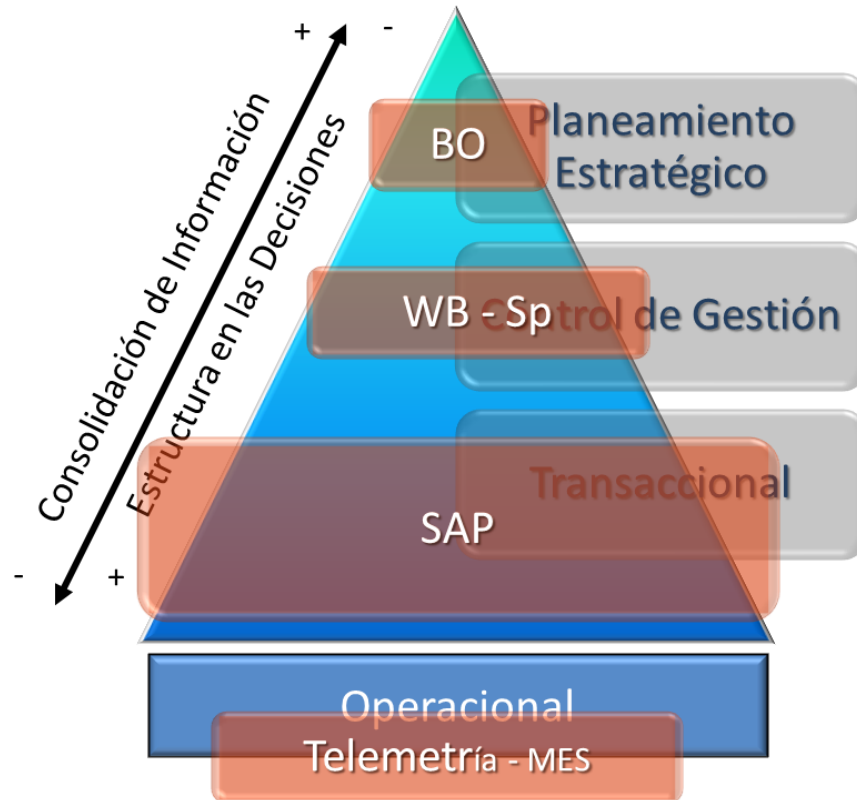


Figura 19 Arquitectura de Información. Fuente: Elaboración Subgerente Informática ESSBIO.

7. **PROPUESTA DE MODELO GOBIERNO TI**

En base a los conceptos revisados anteriormente en el marco teórico, se diseñó un modelo de gobierno TI adaptado a la situación actual de la subgerencia de informática.

Como se mencionó anteriormente, en el capítulo cinco de este trabajo, se define el gobierno TI como sigue:

“Estructura de relaciones y procesos para dirigir y controlar las tecnologías de la información con el fin de garantizar que éstas soportan y habilitan la estrategia de la empresa y el logro de sus objetivos”.

Esta definición responde a la necesidad que tiene la subgerencia de informática, nacida desde su plan estratégico, de conformar un Gobierno TI, que abarque las TI desde una mirada estratégica, sin pasar por alto la administración y correcta operación de los sistemas de información y tecnologías de información (SI/TI). Por lo tanto, debe considerar todo lo concerniente a la dirección y control de las tecnologías y a su vez, buscar la habilitación del logro de las metas de la empresa. Lo anterior permite situar a las TI en un plano estratégico dentro de la organización y a su vez dar curso al diario bregar de la subgerencia de informática.

7.1 Pirámide de Gobierno TI para Subgerencia de Informática de ESSBIO

Las personas y el cómo se organizan son la clave principal de cualquier organismo. Para un buen desempeño de gobierno TI no es la excepción, las personas son el núcleo, y el cómo se relacionen y asuman el rol y responsabilidad que les compete, será el factor determinante principal del éxito de gobierno TI. En base esta idea, se debe plasmar una estructura de relaciones como un componente primordial de gobierno TI, que deje claro este concepto. Para la compañía a la cual se hace la presente propuesta, tampoco es ajena esta idea. ESSBIO tiene dentro de su estrategia esta consideración incentivando el trabajo en equipo, la proactividad, el trabajo transversal e inculcando actitudes positivas en cada uno de los miembros del equipo. Por lo tanto, la propuesta de este gobierno plasma como eje el concepto de estructura de relaciones que tiene como principal objetivo, la entrega de valor a la empresa.

Por otro lado, se han establecido diferentes formas de llevar a cabo un gobierno TI. Para Peterson (2003) el gobierno TI cumple al considerar únicamente el plano estratégico de las TI en la compañía. Para Hamaker y Hutton (2003), el gobierno TI se amplía hasta el plano administrativo. Para Weill et al. (2003), abarca el plano completo, estratégico, administrativo y operacional. Por lo tanto, el establecer el punto de vista propio de la compañía es fundamental. En cada caso se debe considerar cuál es la perspectiva de la compañía frente a las TI, y cuál es la responsabilidad que toma frente a ellas. En base a dicho punto de vista, se debe plantear como segundo eje los niveles de dirección y control que asumirá el gobierno TI presente.

Como tercer aspecto fundamental de un gobierno TI es establecer y dejar clara la forma o base de cómo se planteará la implementación del gobierno TI. Esto es, cuáles serán sus

aspectos de trabajo, o en otras palabras, los dominios de gobierno TI. Estos dominios son los que engloban las áreas principales del gobierno TI. Por lo tanto, se debe velar para que cada una de ellas sea cubierta, de tal manera, que las TI sean correcta y completamente abordadas, y de esa manera generen el valor al negocio que realmente pueden y deben otorgar. Estas áreas finalmente decantarán en un grupo de procesos, los cuales son la célula que le da vida al gobierno TI. Los procesos son vitales para ESSBIO, el cual inculca desde su plan estratégico una cultura orientada a ellos. Por lo tanto, es completamente coherente, en base a la eficacia que los procesos otorgan, el plantear en el gobierno TI la estructura de procesos, la cual en esta propuesta se denomina dominios de gobierno.

En base a la definición de gobierno TI planteada, y las premisas anteriormente expuestas, se propone una pirámide de tres caras, las cuales se interrelacionan. La primera define la estructura de relaciones. La segunda cara define los niveles de dirección y control. Por último, la tercera cara establece los dominios de procesos definidos (Figura 20).

Como se puede apreciar en la Figura 20, la cara de “niveles de dirección y control” contiene tres niveles. El nivel más cerca del ápice de la pirámide es el estratégico y es el nivel que está más cerca de darle valor al negocio, lo cual se puede apreciar en la cara de “estructura de relaciones”. Sin embargo, este nivel estratégico está estrechamente relacionado con el comité de TI en la cara de estructura de relaciones, ya que éste es el responsable de tomar todas las decisiones estratégicas de TI, las cuales luego decantarán en el nivel inmediatamente inferior. El nivel administrativo en la cara de “niveles de dirección y control” también toma parte del comité de TI, porque éste debe dar las directrices generales de administración. Sin embargo, este nivel también abarca todas las decisiones de las áreas de servicio de negocio y parte de las decisiones del área de infraestructura. Lo anterior sucede por las funciones que le corresponde actualmente a cada departamento. Finalmente se encuentra el nivel operacional, el cual también abarca parte de las acciones del área de infraestructura y todos los aspectos del área de calidad y seguridad. Lo anterior, no significa que el área de calidad y seguridad no tenga labores administrativas, pero esta área se concentra en el nivel operacional ya que es en este nivel donde ejerce su mayor acción. La relación entre la cara de niveles de “dirección y control” y la cara de “dominios de gobierno TI” es tal cual como se visualiza en la pirámide (Figura 21). El nivel estratégico contiene un dominio: Evaluar/Dirigir/Monitorear (EDM). El nivel administrativo contiene dos dominios: Planificar/Organizar y Construir/Implementar. Finalmente el nivel operacional contiene dos dominios: Entregar/Dar Soporte y Supervisar/Evaluar.

La pirámide se apoya en una base de principios, los cuales deben ser considerados, aunque no necesariamente todos, en cada acción y/o decisión de la subgerencia de informática.

Los detalles de las tres caras de la pirámide y sus principios se definen a continuación.

y/o futura o bien, para agilizar las operaciones, aumentando así su eficiencia y/o eficacia.

Las TI deben ser creadas para dar solución y soporte a los procesos de la organización, proporcionando los servicios con la calidad adecuada para cubrir las necesidades actuales y futuras del negocio.

Este principio da sustento al primer ítem de la misión de la subgerencia de informática “desarrollar soluciones que generen alto valor al negocio”, en tanto que las tecnologías están al servicio de la empresa para generar respuestas a sus problemas y para agilizar sus procesos. Por lo anterior, debe ser establecido como un principio ya que las TI son para la organización y no la organización para las TI.

- **Alineación estratégica (AE):** Es la sincronía que existe entre la estrategia del negocio y las estrategias de TI y las acciones emanadas de ella con el fin de darles un respaldo válido.

Se consideran los planes estratégicos de TI para satisfacer las necesidades actuales y futuras derivadas de la estrategia de negocio. La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TI. Esto permite, que el trabajo que realiza la subgerencia de informática tenga las respuestas que la empresa espera de ella y que no opere en función de intereses o metas incompatibles o incoherentes con los requerimientos del negocio.

- **Responsabilidad (Re):** Obligación de los participantes de TI, tanto de la subgerencia de informática, sus clientes internos y los interesados del negocio, de responder con compromiso a las decisiones y acciones que sean pertinentes a cada uno según su rol frente a las TI.

Los individuos y grupos dentro de la organización deben comprender y aceptar su responsabilidad con respecto a la oferta y la demanda de TI. Las personas con responsabilidad de las acciones también tienen la autoridad para llevar a cabo esas acciones. Esto permite sustentar la relación de partners con los clientes internos como lo demanda la visión de la subgerencia de informática, poniendo a las TI en la perspectiva de los clientes internos, y de esta forma que ellos puedan cumplir su papel para el logro de las metas trazadas.

- **Adquisición (Ad):** Acto de hacer propio una solución tecnológica.

Las adquisiciones de TI se deben hacer por razones válidas, sobre una base adecuada y análisis en curso, con la decisión clara y transparente de decisiones. Hay equilibrio adecuado entre los beneficios, oportunidades, costos y riesgos, tanto a corto y largo plazo. Este principio asegura la rentabilidad de las inversiones de la subgerencia de informática, y de esa manera, que estas inversiones retornen utilidades, agilidad, ventaja competitiva y/o eficiencia al negocio.

- **Unidad de Servicios de Negocio (USN):** Unidad que proporciona valor a sus clientes para facilitarles los resultados deseados, sin que ellos tengan la necesidad de asumir los costes y riesgos específicos asociados.

La subgerencia de informática debe estar dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir

con las necesidades actuales y futuras. Por lo anterior, es fundamental que se establezca este principio como parte del gobierno TI. Esto permitirá que siempre sea visualizada como una unidad que soporta al negocio no sólo al momento de entregar un producto TI, sino también entregando el soporte adecuado a las tecnologías. Por otro lado, permite a los participantes de la subgerencia de informática tener siempre presente el sustentar con la mejor calidad al negocio y resolver los impases referentes a las TI que se presenten. Lo anterior permite que la información esté siempre disponible y operativa para la toma de decisiones del negocio, lo cual es un requerimiento primordial del negocio para las TI.

- **Conformidad (Co):** Acción y efecto de cumplir con las regulaciones y normas que establece la ley y la compañía.
Cumple con todas las legislaciones y normas obligatorias. Las políticas y prácticas están claramente definidas, aplicadas y ejecutadas. Este principio es fundamental ya que todas las decisiones, procedimientos, políticas y prácticas nunca deben pasar por alto las normativas tanto a nivel de la compañía como en los aspectos legales. Esto es parte de las exigencias de la compañía, la cual tiene como valores la transparencia, la confianza, el respeto y la excelencia.

7.1.2 Estructura De Relaciones

En la Figura 20 además de los principios anteriormente explicados, se visualizan dos caras de la pirámide: *Estructuras de Relaciones* y *Niveles de Dirección y Control*. En esta sección se explicará la Estructura de Relaciones.

Contar con una estructura de relaciones se torna fundamental para establecer las directrices de comunicación entre los interesados. Esta comunicación es vital entre los actores que se encuentran tanto dentro de la subgerencia de informática, así como con aquellos que se encuentran fuera de la misma. Esta estructura está basada en el modelo de organización actual (Figura 17) de la subgerencia de informática.

Como plataforma de todas las demás áreas se encuentra “calidad y seguridad”, ya que ésta debe proveer políticas y procesos que se ejecuten en toda la subgerencia de informática asegurando estos aspectos. Luego se encuentra el área de “infraestructura”, ya que las otras áreas restantes se sustentan en ella, por ende también las tecnologías de toda la compañía. En el siguiente nivel de la pirámide se encuentran las áreas de servicio de negocio, las cuales están ubicadas más cerca de la cúspide ya que su objetivo se acerca a brindarle valor al negocio. Estas áreas son: “BPM”, “Soporte SAP” y “Operaciones”. El alcance de cada una de las áreas continúa como ha sido definido en la sección de la situación actual (sección 6.3). Por último se encuentra un comité de TI que es el encargado de velar para que las TI se encuentren alineadas con el negocio y estén realmente generando valor a éste. Por tanto, es responsable de proveer los lineamientos generales de administración que faciliten que la estrategia de negocio y las prioridades se vean reflejadas en los planes tácticos de TI. Toda la estructura anteriormente descrita es fundamental para el gobierno TI, el cual busca una visión de TI en la organización como un aliado estratégico para la generación de valor al negocio.

7.1.3 Niveles de Dirección y Control

La exigencia de ESSBIO hacia las TI tiene una mirada completa. Esto significa, que a la misma vez que le demanda tener una mirada estratégica, también responsabiliza a la subgerencia de informática de una buena administración y operación de las tecnologías de la información. Lo anterior lleva a los encargados a abordar las TI en distintas perspectivas. En esta propuesta se plantea conducir las TI haciendo una diferencia por niveles como lo plantean Weill et al. (2003), la cual considera el nivel estratégico, el administrativo y el operacional. En este contexto, emerge la segunda cara de la pirámide denominada “Niveles de Dirección y Control” (Figura 20).

Estos niveles se enuncian y explican a continuación:

- Nivel estratégico: Es el encargado de la priorización y toma de decisiones con respecto de las TI en la compañía. Éstas se deben ejecutar velando que siempre estén alineadas con la visión, misión, valores y/o estrategia tanto de la compañía, como de la propia subgerencia de informática. En este contexto, evalúa las necesidades, condiciones y opciones de las partes interesadas. Define el alcance de estas decisiones para que luego pasen al plano administrativo.
- Nivel administrativo: El responsable de definir el “cómo” se llevan a cabo las decisiones emanadas del nivel estratégico, basándose en procesos de altos estándares de calidad, apoyados en lo posible en modelos reconocidos internacionalmente. Este nivel planifica y construye actividades alineadas con la dirección establecida por el nivel superior con el fin de alcanzar las metas empresariales.
- Nivel operacional: El cual ejecuta los procesos definidos y devuelve las salidas que del o los procesos se esperan hacia el nivel administrativo. Recibe las soluciones y las hace utilizables a los usuarios finales. Además, monitorea todos los procesos para asegurar que se sigue en la dirección definida.

El nivel estratégico se encuentra en el ápice de la pirámide, ya que éste existe para dar valor al negocio, luego las decisiones que se tomen en este ámbito son apoyadas directamente por el plano administrativo, el cual, a su vez, decanta en el nivel operacional, el cual es la ejecución de los procesos definidos en el nivel administrativo.

En la Figura 21 se visualizan dos caras de la pirámide: *Niveles de Dirección y Control*, la cual ya fue explicada anteriormente y la cara de *Dominios de Gobierno*, la cual será explicada a continuación.

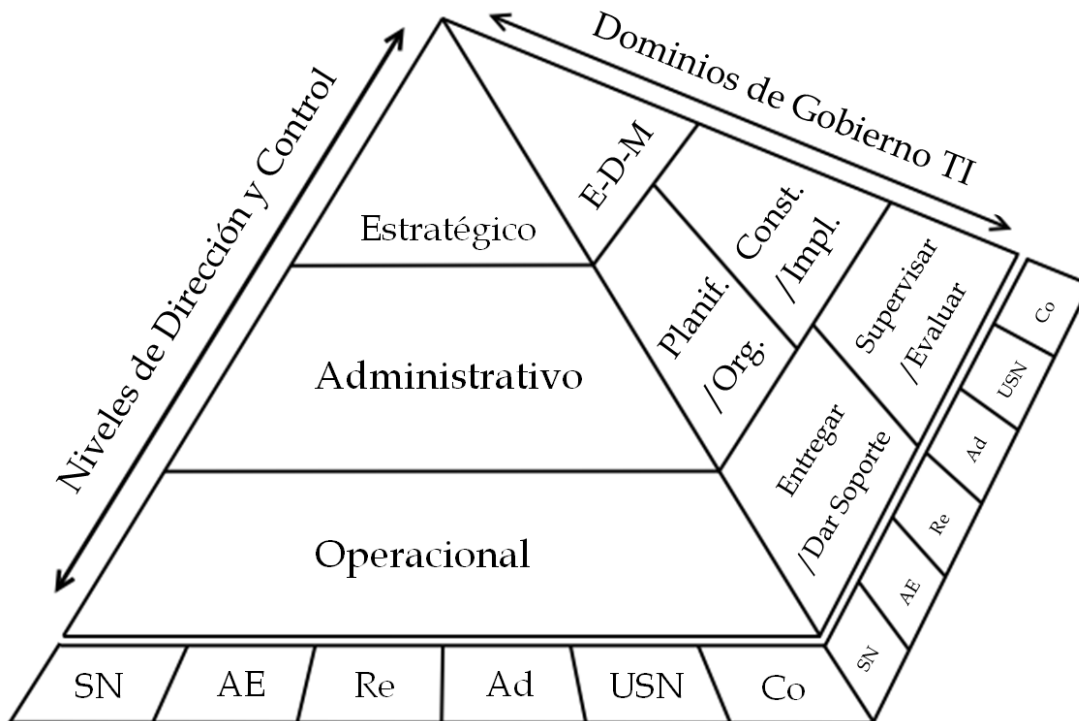


Figura 21 Pirámide de Gobierno TI: Niveles de Dirección y Control y Dominios de Gobierno. Fuente: Elaboración Propia

7.1.4 Dominios de Gobierno TI

Para profundizar en el nivel de dirección y control es necesario desplegar una nueva cara en la pirámide: *Dominios de Gobierno TI*. Tanto COBIT 4.1 como COBIT 5 hacen énfasis en este punto y es necesario para comprobar que todos los niveles de dirección y control se están ejecutando en completitud. Ambos marcos de gobierno TI mencionados se inspiran bajo los mismos conceptos que son planear, construir, ejecutar y supervisar. Luego, en base a dichos conceptos ofrecen un set de procesos por cada uno de ellos. A pesar de que la mayoría de los procesos requieren actividades de planificación, construcción, ejecución y supervisión, bien en el propio proceso, o en la cuestión específica a resolver, están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial. En esta propuesta se adhieren todos estos conceptos dentro de los niveles administrativo (planear y construir) y operacional (ejecutar y supervisar). Para cubrir el nivel estratégico, COBIT 5 toma los conceptos de la norma ISO/IEC 38500 ya que ésta ve el gobierno TI desde un punto exclusivamente estratégico y lo aborda bajo tres conceptos, evaluar, dirigir y monitorear. Como se indicó anteriormente, la subgerencia de informática debe comprender todas las perspectivas descritas, para lo cual amerita abordar las visiones de los tres marcos de gobierno mencionados y también se inspira en la norma ISO/IEC 38500.

En la Figura 21 se muestra la pirámide con la cara de *dominios de gobierno*, agrupados de acuerdo a los *niveles de dirección y control* nombrados y explicados anteriormente. En base a estos dominios luego se derivan procesos, lo cual se explicará en más detalle más adelante.

Los tres conceptos nombrados en el nivel estratégico se explican a continuación:

- **Evaluar (E):** El objetivo es examinar y juzgar sobre el uso actual y futuro de las TI, incluyendo estrategias, propuestas y acuerdos de suministro (ya sea interno, externas o ambas cosas)
- **Dirigir (D):** Tiene como fin determinar la asignación de responsabilidades, y la preparación directa y aplicación de los planes y políticas que se implementen. De esta manera se asegura la correcta transición de los proyectos a la producción considerando los impactos en la operación, el negocio y la infraestructura.
- **Monitorizar (M):** Se debe vigilar el rendimiento de las TI, asegurando que el rendimiento está en conformidad con los planes, en particular con respecto a los objetivos del negocio.

El *nivel administrativo* agrupa dos dominios, los cuales se nombran del mismo modo que COBIT 4.1, estos son:

- **Planificar y organizar:** Este dominio contiene procesos enfocados en las tácticas de TI para contribuir, de hecho, con los objetivos planteados en el nivel estratégico.
- **Construir e implementar:** Centrado en la aplicación de la estrategia de TI. Aquí las soluciones de TI se desarrollan, adquieren, implementan e integran con los procesos de negocio.

El *nivel operacional* de gobierno contiene dos dominios, que al igual que el nivel anterior, están adheridos del modelo de gobierno COBIT 4.1:

- **Entregar y dar soporte:** centrado en temas relacionados con la entrega de los servicios en sí, lo que incluye la prestación de servicios, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.
- **Supervisar y evaluar:** tiene como objetivos evaluar los procesos de TI desde el punto de vista de la calidad y el cumplimiento, de los requisitos de control con regularidad, abarcando la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

7.1.5 *Procesos*

Entiéndase como un proceso a un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos. Manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño (ITGI, COBIT 4.1, 2007).

Cada proceso corresponde a un “nivel de dirección y control” y luego a un “dominio de gobierno” de la pirámide anteriormente explicada.

Los procesos son una parte fundamental de este modelo de gobierno TI, ya que son éstos los que habilitan la ejecución del gobierno planteado.

Se propone en este marco un set de procesos definidos en la sección siguiente. COBIT ofrece un set de procesos, de los cuales muchos de ellos abarcan los aspectos de gobierno TI que se han abordado en esta propuesta. COBIT clasifica los procesos en dominios, los cuales se organizan de acuerdo a cuatro principios: planear, construir, ejecutar, y monitorear. En esta propuesta se va siguiendo esta misma representación por medio de la pirámide planteada, utilizando dominios que se inspiran también en los principios enumerados. Por lo anteriormente explicado, se han adoptado aquellos que siguen los lineamientos de las prácticas actuales de la subgerencia de informática y que responden a las necesidades futuras detectadas. Se excluyeron aquellos procesos que no son atingentes a las exigencias y/o necesidades del departamento en cuestión.

La mayoría de los procesos está infundido principalmente en el marco de gobierno COBIT 4.1 y en la medida que la literatura es accesible, se complementó con COBIT 5. Por otro lado, la forma en que los procesos están expuestos en esta propuesta es más simplificada del que propone COBIT, de tal manera que su implementación sea más sutil y no implique cambios bruscos. Esto tiene como finalidad que los involucrados se adapten más fácilmente al modelo.

Cada proceso también se enmarca en la cara de “estructura organizacional” de la pirámide. En este sentido, se expone en cada proceso los principios que abarca. Si el proceso influye fuertemente en cumplir el principio entonces se especifica con dos vistos bueno. Por otro lado, si influye débilmente en el cumplimiento del principio se especifica con un solo visto bueno. Por último, si el proceso no influye en el principio se deja en blanco. Lo explicado se muestra en una tabla denominada “Principios de Gobierno TI involucrados” de cada proceso. En la misma cara de la pirámide están definidas las estructuras de relaciones, las cuales para comprenderlas dentro del proceso, se definen mediante una matriz RACI. Esta matriz incluye a los involucrados en el proceso y se le asigna una letra según corresponda. La letra A (Accountable) quien es responsable de rendir una cuenta de la ejecución del proceso. La letra R (Responsible) es el responsable de que el proceso se ejecute, aunque no necesariamente debe ser quien lo ejecuta. La letra C (Consulted) es quien posee alguna información, atributo o capacidad necesaria para realizar la tarea. La letra I (Informed) es a quien se le debe informar sobre el avance y/o los resultados de la ejecución de la práctica. Luego la matriz presenta las prácticas que deben ejecutarse en el proceso y cuál es la labor de los involucrados.

Además de especificar qué lugar de la pirámide afecta el proceso se especifican métricas, que actúan como controladores del proceso. Es necesario indicar, que todas las métricas de cada proceso deben ser medidas de la misma forma, por ejemplo, con una escala Likert o porcentaje de cumplimiento de la métrica (Barriga Jiménez, González Gabaldón, Cantero-Sánchez, León Rubio, Gómez Delgado, & Medina Anzano, 1998). De esta forma, al momento de medir cada proceso o bien, todo el marco de gobierno, se tomarán todas las métricas utilizadas y se obtendrá información valiosa para la mejora continua del marco.

Por último, cada proceso tiene una tabla que contiene sus entradas y salidas para facilitar su comprensión y uso.

7.2 Definición de Procesos Propuestos

La Figura 22 muestra los procesos clasificados según el dominio de gobierno TI al cual pertenecen, luego están definidos desde el nivel estratégico de la pirámide hacia el operacional.

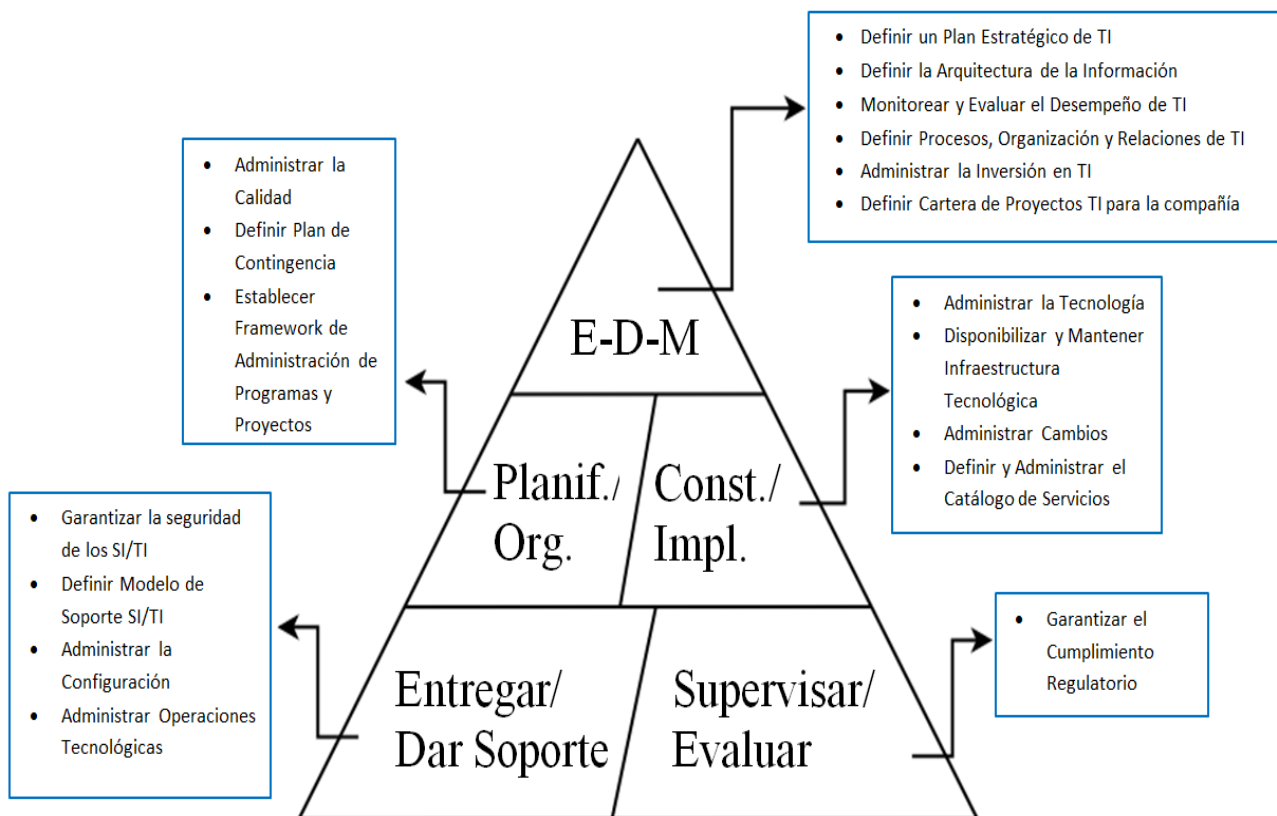


Figura 22 Clasificación Procesos según Dominio de Gobierno TI

7.2.1 Evaluar, Dirigir y Monitorear

A continuación se exponen los procesos correspondientes al dominio de evaluar, dirigir y monitorear. Estos procesos abarcan la evaluación, dirección y monitoreo desde un punto de vista estratégico. Por lo tanto, se abordan las disposiciones claves del gobierno y administración TI y abarcan decisiones de mediano y largo plazo.

7.2.1.1 Definir un Plan estratégico de TI (E-D-M 01)

Definición: Este proceso es necesario para gestionar y dirigir todos los recursos de TI de tal manera que estén alineados con la estrategia y prioridades del negocio, que a su vez se deben reflejar en portafolios que se ejecutan por planes estratégicos de TI que especifican objetivos concisos, planes de acción y tareas entendidas por el negocio y por TI.

Objetivo: Asegurar que los planes estratégicos de TI son consistentes con los objetivos del negocio.



Figura 23 Nivel y Dominio de Proceso "Definir una Plan Estratégico de TI". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	✓✓
Responsabilidad	✓
Adquisición	
Unidad de Servicios de Negocio	
Conformidad	

Tabla 8 Principios involucrados en Proceso "Definir un Plan Estratégico de TI". Fuente: Elaboración Propia

Matriz RACI: Definir un Plan Estratégico								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Entender la dirección de la Organización	A/R	R	R	R	R	R	R	R
2. Evaluar el entorno actual, la capacidad y el rendimiento del negocio y de TI (interno y externo).	R	A/R	C	C	C	C	C	C
3. Definir las capacidades de TI a alcanzar.	C	A/R	C	C	C	C	C	C
4. Analizar las brechas.	R	A/R	C	C	C	C	C	C
5. Definir el plan estratégico y hoja de ruta.	R	A/R	C	C	C	C	C	C
6. Analizar portafolio de programas y administrar portafolios de servicios y proyectos	I	A/R	R	R	R	R	I	I
7. Comunicar los objetivos y estrategia de TI y de la compañía.	R	A/R	R	R	R	R	I	I

Tabla 9 Matriz RACI Proceso "Definir un Plan Estratégico de TI". Fuente: Elaboración Propia

Métricas:

- Grado del cumplimiento de requerimientos del Negocio.
- Porcentaje de objetivos de TI en el plan estratégico de TI que dan soporte al plan estratégico del negocio.
- Hitos cumplidos con respecto a los hitos definidos en el plan inicial.

Entradas del Proceso	Salidas del Proceso
Estrategia y prioridades del negocio	Plan estratégico de TI
Portafolio de Programas	Hoja de ruta del plan estratégico
Portafolio de Proyectos	Portafolio de proyectos de TI actualizado
Reporte con indicadores de desempeño de TI	

Tabla 10 Entradas y Salidas de Proceso "Definir un Plan Estratégico de TI". Fuente: Elaboración Propia

7.2.1.2 Definir la Arquitectura de la Información (E-D-M 02)

Definición: La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los niveles de información y los sistemas apropiados que los respaldan para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad que garantice la integridad y consistencia de los datos.

Objetivos: Optimizar el uso de la información, garantizar la integración transparente de las aplicaciones hacia los procesos de negocio. Responder a los requerimientos de negocio de manera alineada con la estrategia del negocio.



Figura 24 Nivel y Dominio de Proceso "Definir la Arquitectura de la Información". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	✓✓
Responsabilidad	
Adquisición	✓
Unidad de Servicios de Negocio	✓
Conformidad	

Tabla 11 Principios involucrados en Proceso "Definir la Arquitectura de la Información". Fuente: Elaboración Propia

Matriz RACI: Definir la Arquitectura de la Información								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de
1. Crear y mantener modelo de información corporativo/empresarial	I	A/R	C	C	I	R	I	C
2. Establecer y Mantener esquema de clasificación de datos	I	A	C	C	I	R	C	I
3. Crear y mantener diccionario de datos corporativo		I	I	C	C	A/R	C	I
4. Usar el diseño de información, el diccionario de datos y el esquema de clasificación para planear los sistemas optimizados de negocio		I	R	R	R	A	I	

Tabla 12 Matriz RACI Proceso "Definir la Arquitectura de la Información". Fuente: Elaboración Propia

Métricas:

- Número de procesos críticos de negocio soportados por la actualización de infraestructura.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Esquema de clasificación de datos
Hoja de ruta del plan estratégico	Diccionario de datos
Revisión post implementación de proyectos implementados	Arquitectura de la información
Reporte sobre la capacidad	Clasificación de datos asignada
	Procedimientos y herramientas de clasificación de la información

Tabla 13 Entradas y Salidas de Proceso "Definir la Arquitectura de la Información". Fuente: Elaboración Propia

7.2.1.3 Monitorear y Evaluar el desempeño de TI (E-D-M 03)

Definición: El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones.

Objetivo: Entender y transparentar los costos, beneficios, estrategias, políticas y servicios de TI de acuerdo con los requisitos de gobierno.



Figura 25 Nivel y Dominio de Proceso "Monitorear y Evaluar el desempeño de TI". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	✓
Responsabilidad	✓
Adquisición	
Unidad de Servicios de Negocio	✓ ✓
Conformidad	✓

Tabla 14 Principios involucrados en Proceso "Monitorear y Evaluar el desempeño de TI". Fuente: Elaboración Propia

Matriz RACI: Monitorear y Evaluar el desempeño de TI								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Establecer un enfoque de monitoreo		A/R	R	R	R	R		R
2. Identificar y recolectar objetivos medibles que apoyen a los objetivos del negocio	C	A/R	C	C	I	I		R
3. Crear cuadro de mandos		A/R	R			C		
4. Evaluar el desempeño		A/R	R	R	R	R		R
5. Reportar el desempeño		A/R	R	R	R	R		R
6. Identificar y monitorear las medidas de mejora del desempeño	C	A/R	R	R	R	R		R

Tabla 15 Matriz RACI Proceso "Monitorear y Evaluar el desempeño de TI". Fuente: Elaboración Propia

Métricas:

- Número de cambios a las metas para los indicadores de efectividad y eficiencia de los procesos de TI.
- Porcentaje de procesos críticos monitoreados.
- Metas de desempeño alcanzadas a nivel individual y a nivel de conjunto de éstas.
- Número de métricas que se pueden evaluar por comparación contra estándares de la industria y metas establecidas.

Entradas del Proceso	Salidas del Proceso
Reporte de costo/beneficio	Indicadores de desempeño a planeación de TI
Reportes de desempeño de los proyectos	Planes de acciones correctivas
Reportes de desempeño de los procesos del marco de trabajo	Tendencias y eventos de riesgos históricos
Reporte sobre la efectividad de los controles de TI	Reporte de desempeño del proceso
Reporte sobre el cumplimiento de las actividades de TI con los requerimientos externos legales y regulatorios	

Tabla 16 Entradas y Salidas de Proceso "Monitorear y Evaluar el desempeño de TI". Fuente: Elaboración Propia

7.2.1.4 Definir Procesos, Organización y Relaciones de TI (E-D-M 04)

Definición: Una organización de TI se debe definir tomando en cuenta las funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, y la disminución de la dependencia.

Objetivo: Establecer una posición de las TI en la organización, de tal manera que la visión de ésta sea clara y a su vez promueva una participación responsable y equilibrada por parte de todos los interesados.



Figura 26 Nivel y Dominio de Proceso "Definir Procesos, Organización y Relaciones de TI". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	✓ ✓
Responsabilidad	✓
Adquisición	
Unidad de Servicios de Negocio	✓
Conformidad	✓

Tabla 17 Principios involucrados en Proceso "Definir Procesos, Organización y Relaciones de TI". Fuente: Elaboración Propia

Matriz RACI: Definir Procesos, Organización y Relaciones de TI								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
	1. Definir un marco de trabajo para la definición de procesos, políticas y procedimientos para ejecutar el plan estratégico de TI.		A/R	I	I	I	I	I
2. Definir la Estructura Organizativa de TI.	I	A/R						
3. Establecer roles y responsabilidades de TI.		A/R	I	I	I	I	I	C
4. Gestionar la mejora continua de los procesos, políticas y procedimientos.		C	R	R	R	R	R	A/R
5. Establecer la propiedad y responsabilidad de los riesgos relacionados a TI en un nivel superior.		A/R	I	I	I	I	R	R
6. Implementar prácticas de supervisión dentro de la función TI.		C	R	R	R	R	R	A/R
7. Definir e identificar al personal clave de TI y minimizar la dependencia.		A	R	R	R	R	R	R
8. Establecer y mantener una estructura de enlace, comunicación y coordinación entre la subgerencia de TI y su entorno (offsite).		A	R	R	R	R	R	R

Tabla 18 Matriz RACI Proceso "Definir Procesos, Organización y Relaciones de TI". Fuente: Elaboración Propia

Métricas:

- Porcentaje de roles con descripciones de puestos y autoridad documentados.
- Número de actividades esenciales de TI, que no están aprobadas o que no están sujetas a los estándares de TI.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Organización y relaciones de TI
Hoja de ruta del plan estratégico	Roles y responsabilidades documentadas
Medidas para la mejora de la calidad	
Planes de acciones correctivas para riesgos relacionados con TI	
Planes de acciones correctivas en la evaluación del desempeño de TI	
Reporte sobre la efectividad de los controles de TI	
Catálogo de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI	

Tabla 19 Entradas y Salidas de Proceso "Definir Procesos, Organización y Relaciones de TI". Fuente: Elaboración Propia

7.2.1.5 Administrar la Inversión en TI (E-D-M 05)

Definición: Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. El marco debe considerar y estar alineado al proceso de inversión de la compañía, tomando en cuenta sus restricciones. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI y tomar medidas correctivas según sean necesarias.

Objetivo: Mejorar continuamente y de forma demostrable la generación de valor de TI y su contribución al negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario y la eficiencia en la inversión.



Figura 27 Nivel y Dominio de Proceso "Administrar la Inversión TI". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	✓
Responsabilidad	
Adquisición	✓ ✓
Unidad de Servicios de Negocio	
Conformidad	

Tabla 20 Principios involucrados en Proceso "Administrar la Inversión TI". Fuente: Elaboración Propia

Matriz RACI: Administrar la Inversión en TI								
Prácticas	Dominios de Gobierno TI							
	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Establecer y mantener un marco de trabajo para administrar el portafolio de programas de inversión	A	R	R	I	I			C
2. Dar prioridad a la asignación de los recursos	R	A	C	C				
3. Crear y mantener los presupuestos	A	R	R	C				
4. Modelar, mantener y administrar los costos	C	A/R	R	C	C	C		
5. Identificar, comunicar y monitorear la inversión, costo y valor de TI para el negocio	C	A/R	R	C	C			

Tabla 21 Matriz RACI Proceso "Administrar la Inversión TI". Fuente: Elaboración Propia

Métricas:

- Porcentaje del valor de la desviación respecto al presupuesto en comparación con el presupuesto total.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Reporte de costo/beneficio
Hoja de ruta del plan estratégico	Presupuestos de TI
Requerimientos de infraestructura	Cartera de inversión asociada al portafolio
Portafolio actualizado de los proyectos de TI	
Plan de desempeño y capacidad	
Revisión post implementación de proyectos implementados	

Tabla 22 Entradas y Salidas de Proceso "Administrar la Inversión TI". Fuente: Elaboración Propia

7.2.1.6 Definir Cartera de Proyectos TI para la Compañía (E-D-M 06)

Definición: Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares.

Objetivo: Construir las aplicaciones de acuerdo a los requerimientos y necesidades del negocio, cumpliendo con los plazos establecidos y a un costo razonable.



Figura 28 Nivel y Dominio de Proceso "Definir Cartera de Proyectos TI para la Compañía". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓✓
Alineación Estratégica	✓✓
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	✓
Conformidad	✓

Tabla 23 Principios involucrados en Proceso "Definir Cartera de Proyectos TI para la Compañía". Fuente: Elaboración Propia

Matriz RACI: Definir Cartera de Proyectos TI para la Compañía								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Traducir los requerimientos del negocio en especificaciones de diseño de alto nivel		C	A/R	C		C	I	I
2. Preparar diseño detallado y los requerimientos técnicos del software aplicativo			A/R	C		C		C
3. Especificar los controles de aplicación dentro del diseño			A/R	C			C	C
4. Personalizar e implementar la funcionalidad automatizada adquirida		I	A/R	C			C	C
5. Desarrollar las metodologías y procesos formales para administrar el proceso de desarrollo de la aplicación			A/R	I				C
6. Crear un plan de aseguramiento de la calidad del software para el proyecto			A/R	C		C		R
7. Dar seguimiento y administrar los requerimientos de la aplicación			A/R		C			I

Tabla 24 Matriz RACI Proceso "Definir Cartera de Proyectos TI para la Compañía". Fuente: Elaboración Propia

Métricas:

- Número de proyectos que no alcanzan los beneficios establecidos por un diseño o desarrollo deficiente.
- Porcentaje de proyectos que superan el presupuesto planeado.

Entradas del Proceso	Salidas del Proceso
Esquema de clasificación de datos	Especificaciones de los controles de seguridad de las aplicaciones
Diccionario de datos	Conocimiento de la aplicación y del paquete de software
Actualizaciones rutinarias del “estado de la tecnología”	SLAs planteados inicialmente
Reporte de costo/beneficio	Especificación de disponibilidad, continuidad y recuperación
Estándares de Calidad de normas, prácticas y procedimientos	Manuales de usuario, técnicos, de soporte y de administración
Marco de trabajo para la administración de proyectos de TI	
Planes detallados de los proyectos	
Descripción de proceso de evolutivos	

Tabla 25 Entradas y Salidas de Proceso "Definir Cartera de Proyectos TI para la Compañía". Fuente: Elaboración Propia

7.2.2 Planificar y Organizar (Pl-Or)

A continuación se presentan los procesos correspondientes al nivel de dirección y control administrativo. Primeramente los procesos de planificación y organización y posteriormente los procesos de construcción e implementación.

Los procesos de planificación y organización son los encargados de proyectar, preparar las decisiones emanadas desde el plano estratégico de TI para que éstas sean ejecutadas. Su enfoque es plantear las tácticas para que las decisiones tomadas sean exitosas.

7.2.2.1 Administrar la Calidad (Pl-Or 01)

Definición: Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo, adquisición y operación. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables.

Objetivo: Asegurar la operatividad y mantenibilidad de las soluciones tecnológicas y su mejora continua y transparencia para los interesados.



Figura 29 Nivel y Dominio de Proceso "Administrar la Calidad". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓ ✓
Alineación Estratégica	✓
Responsabilidad	✓
Adquisición	
Unidad de Servicios de Negocio	✓ ✓
Conformidad	✓

Tabla 26 Principios involucrados en Proceso "Administrar la Calidad". Fuente: Elaboración Propia

Matriz RACI: Administrar la Calidad								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Definir y establecer un sistema de administración de calidad	I	C	R	R	R	R	R	A/R
2. Definir los estándares calidad de normas, prácticas y procedimientos		C	R	R	R	R	R	A/R
3. Comunicar los estándares de calidad a los interesados		I	I	I	I	I	I	A/R
4. Crear y administrar un plan de calidad para la mejora continua		C	I	I	I	I	I	A/R
5. Integrar la gestión de calidad en las soluciones para el desarrollo y prestación de servicios		I	R	R	R	R	R	A
6. Medir, monitorear y revisar el cumplimiento de las metas de calidad		I	R	R	R	R	R	A/R

Tabla 27 Matriz RACI Proceso "Administrar la Calidad". Fuente: Elaboración Propia

Métricas:

- Porcentaje de procedimientos revisados de manera formal por aseguramiento de calidad en contraste de los procesos estandarizados.
- Porcentaje de defectos no descubiertos antes de entrar en producción.
- Resultado del muestreo de revisión de calidad de proyectos y/o servicios de TI.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Sistema de administración de calidad.
Hoja de ruta del plan estratégico	Estándares de calidad de normas, prácticas, políticas y procedimientos
Planes detallados de los proyectos	Medidas para la mejora de la calidad
Planes de acciones correctivas en la evaluación del desempeño de TI	

Tabla 28 Entradas y Salidas de Proceso "Administrar la Calidad". Fuente: Elaboración Propia

7.2.2.2 *Evaluar y Administrar Riesgos de TI (Pl-Or 02)*

Definición: Crear un plan de contingencia que documente estrategias de mitigación de riesgos. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe se debe expresado de tal manera que permita alinear los riesgos a un nivel aceptable de tolerancia.

Objetivo: Garantizar la continuidad operativa del negocio.



Figura 30 Nivel y Dominio de Proceso "Evaluar y Administrar Riesgos de TI". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	✓ ✓
Responsabilidad	✓
Adquisición	
Unidad de Servicios de Negocio	✓ ✓
Conformidad	✓

Tabla 29 Principios involucrados en Proceso "Evaluar y Administrar Riesgos de TI". Fuente: Elaboración Propia

Matriz RACI: Evaluar y Administrar Riesgos de TI								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Establecer un marco de trabajo de administración de riesgos de TI alineado al marco de trabajo de administración de riesgos de la compañía.	A	A/R	I	I	I	C	R	R
2. Entender los objetivos de negocio relevantes	C	A/R				R	R	R
3. Entender los objetivos de los procesos de negocio relevantes		C	A/C	C		R	R	I
4. Identificar los objetivos internos de TI y establecer el contexto de riesgo		A/C	I	I	I	R	R	R
5. Identificar eventos asociados con objetivos tanto del negocio como de TI		A/C	C	C	C	R	A/R	R
6. Desarrollar un marco de trabajo de continuidad de TI		C	C	C	C	R	A/R	
7. Definir y ejecutar procedimientos de control de cambios para asegurar que el plan de continuidad sea vigente		A	C	C	R	C		R
8. Probar regularmente el plan de continuidad de TI		I			A/R		R	R
9. Realiza un análisis de impacto al negocio y valoración de riesgo		A	C	C	C	C	R	
10. Planear la recuperación y reanudación de los servicios de TI		I		R	A/R	R	R	
11. Priorizar y planear actividades de control		C				R	A/R	
12. Aprobar y asegurar fondos para planes de acción de riesgos	A/R	I						
13. Mantener y monitorear un plan de acción de riesgos		A/C				R	A/R	R

Tabla 30 Matriz RACI Proceso "Evaluar y Administrar Riesgos de TI". Fuente: Elaboración Propia

Métricas:

- Porcentaje de procesos críticos de TI cubiertos por la evaluación de riesgos.
- Porcentaje de riesgos críticos de TI identificados con planes de acción elaborados.
- Número de procesos críticos del negocio que dependen de TI, no cubiertos por un plan de continuidad.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Evaluación de riesgos
Hoja de ruta del plan estratégico	Reporte de riesgos
Plan de administración de riesgos de los proyectos	Directrices de administración de riesgos relacionados con TI
Riesgos de proveedores	Planes de acciones correctivas para riesgos relacionados con TI
Resultados de pruebas de contingencia	Resultados de pruebas de contingencia
Amenazas y vulnerabilidades de seguridad	Criticidad de puntos de configuración de TI
Tendencias y eventos de riesgos históricos	Plan de almacenamiento de respaldos y de protección
Clasificación de datos asignada	Umbral de incidentes y/o desastres
Evaluación de riesgos	Requerimientos de servicios contra desastres incluyendo roles y responsabilidades.
Especificación de disponibilidad, continuidad y recuperación de los sistemas	
SLAs actualizados	
OLAs actualizados	
Manuales de usuario, técnicos, de soporte y de administración de los sistemas	

Tabla 31 Entradas y Salidas de Proceso "Evaluar y Administrar Riesgos de TI". Fuente: Elaboración Propia

7.2.2.3 Establecer Framework de Administración de Programas y Proyectos (PI-Or 03)

Definición: Establecer un framework de administración de programas y proyectos para la gestión de todos los proyectos de TI establecidos que garantice la correcta asignación de prioridades y la coordinación de todos los proyectos. Debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan de pruebas, revisión de pruebas y post-implantación después de la instalación garantizando la gestión de riesgos del proyecto y la entrega de valor para el negocio.

Objetivo: La entrega de resultados de proyectos basados en estándares dentro de marcos de tiempo, presupuesto y calidad acordados, reduciendo el riesgo y los costos inesperados, maximizando la contribución a los programas de inversión de TI y asegurando su continuidad.



Figura 31 Nivel y Dominio de Proceso "Establecer Framework de Administración de Programas y Proyectos". Fuente: Elaboración Propia.

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓ ✓
Alineación Estratégica	
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	
Conformidad	

Tabla 32 Principios involucrados en Proceso "Establecer Framework de Administración de Programas y Proyectos". Fuente: Elaboración Propia

Matriz RACI: Establecer Framework de Administración de Programas y Proyectos								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Establecer y mantener un marco de trabajo para la administración de proyectos de TI		R	A/R	C	I			I
2. Establecer y mantener un sistema de monitoreo y medición de desarrollo de proyectos		I	A/R	R	I	I		I
3. Administrar programa de calidad de proyectos		I	A/R	R			R	R/C
4. Administrar programa de riesgos de proyectos		C	A/R	R		R	R/C	I
5. Definir y administrar los productos y/o servicios de proyectos definiendo los responsables de la administración de dichos productos y servicios.		C	A/R	R		R	I	I
6. Definir estándares que apoyen la gestión de proyectos		C	A/R	R	I	I	R/C	R/C
7. Definir plan de implementación de proyectos		C	A/R	I	I	I		C

Tabla 33 Matriz RACI Proceso "Establecer Framework de Programas y Proyectos". Fuente: Elaboración Propia

Métricas:

- Porcentaje de proyectos que se alinean a las directrices definidas en el framework establecido.

Entradas del Proceso	Salidas del Proceso
Estándares de calidad de normas, prácticas y procedimientos	Framework para la administración de proyectos de TI
	Reportes de desempeño de los proyectos
	Plan de administración de riesgos de los proyectos
	Directrices de administración de los proyectos

Tabla 34 Entradas y Salidas de Proceso "Establecer Framework de Programas y Proyectos". Fuente: Elaboración Propia

7.2.3 Construir e Implementar (Co-Im)

A continuación se presentan los procesos correspondientes a la construcción e implementación. Estos procesos son la ejecución propiamente tal de los planes establecidos en el dominio anterior. Están ubicados en el nivel de dirección y control administrativo, en tanto que se están construyendo e implementando las soluciones de negocio.

7.2.3.1 Administrar la Tecnología (Co-Im 01)

Definición: Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias.

Objetivo: Contar con sistemas aplicativos estándares, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros.



Figura 32 Nivel y Dominio de Proceso "Administrar la Tecnología". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	✓
Responsabilidad	
Adquisición	✓✓
Unidad de Servicios de Negocio	
Conformidad	

Tabla 35 Principios involucrados en Proceso "Administrar la Tecnología". Fuente: Elaboración Propia

Matriz RACI: Administrar la Tecnología								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Mantener una comprensión del entorno empresarial	A	R		R		R	R	R
2. Evaluar el entorno tecnológico		A		R		R		
3. Evaluar el potencial de las tecnologías emergentes		A		R		R		
4. Recomendar nuevas iniciativas apropiadas para las necesidades de la empresa	C	A		R		R	C	
5. Crear y mantener un plan de infraestructura tecnológica		C	I	I	I	A/R	I	I
6. Comunicar los estándares tecnológicos establecidos	I	A	I	I	I	R	I	I
7. Monitorear la evolución tecnológica		I	R	R		A/R		

Tabla 36 Matriz RACI Proceso "Administrar la Tecnología". Fuente: Elaboración Propia

Métricas:

- Número y tipo de desviaciones con respecto al plan de infraestructura tecnológica.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Oportunidades Tecnológicas
Hoja de ruta del plan estratégico	Estándares Tecnológicos
Arquitectura de la información	Actualizaciones rutinarias del “estado de la tecnología”
Reporte sobre la capacidad	Plan de infraestructura tecnológica
Actualizaciones de estándares de tecnología	Requerimientos de infraestructura

Tabla 37 Entradas y Salidas de Proceso "Administrar la Tecnología". Fuente: Elaboración Propia

7.2.3.2 Disponibilizar y Mantener Infraestructura Tecnológica (Co-Im 02)

Definición: Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica, la cual incluye data center, enlaces de comunicación y redes. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas.

Objetivo: Disponibilizar y dar mantenimiento a una infraestructura integrada y estándar de TI.



Figura 33 Nivel y Dominio de Proceso "Disponibilizar y Mantener Infraestructura Tecnológica". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	
Responsabilidad	
Adquisición	✓
Unidad de Servicios de Negocio	✓✓
Conformidad	

Tabla 38 Principios involucrados en Proceso "Disponibilizar y Mantener Infraestructura Tecnológica". Fuente: Elaboración Propia

Matriz RACI: Disponibilizar y Mantener Infraestructura Tecnológica								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Definir procedimiento/proceso de adquisición o contratación de servicios de infraestructura		C				A/R		
2. Negociar la compra o servicio y adquirir/contratar la infraestructura requerida con proveedores (aprobados)		C				A/R		
3. Definir estrategia y planear la administración de infraestructura		C			C	A/R	C	C
4. Configurar componentes de la Infraestructura		I			I	A/R	I	
5. Definir medidas de control interno, seguridad y auditoría de la infraestructura		I				R	A	R

Tabla 39 Matriz RACI Proceso "Disponibilizar y Mantener Infraestructura Tecnológica". Fuente: Elaboración Propia

Métricas:

- Número de componentes de infraestructura que ya no se puede soportar (o que no se podrá en un futuro cercano).
- Fallas por concepto de infraestructura no adecuada

Entradas del Proceso	Salidas del Proceso
Plan de infraestructura tecnológica	Requerimientos de ambiente físico
Oportunidades Tecnológicas	Actualizaciones de estándares de tecnología
Estándares Tecnológicos	OLAs planeados inicialmente
Actualizaciones rutinarias del “estado de la tecnología”	
Estándares de calidad de normas, prácticas y procedimientos	
Planes detallados de los proyectos	
Plan de desempeño y capacidad	

Tabla 40 Entradas y Salidas de Proceso "Disponibilizar y Mantener Infraestructura Tecnológica". Fuente: Elaboración Propia

7.2.3.3 Administrar Cambios (Co-Im 03)

Definición: Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación.

Objetivo: Responder a los requerimientos del negocio de acuerdo con la estrategia del negocio, mientras se reducen los defectos y la repetición de trabajos en la prestación del servicio y en la solución.



Figura 34 Nivel y Dominio de Proceso "Administrar Cambios". Fuente: Elaboración Propia.

Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	✓
Responsabilidad	
Adquisición	✓
Unidad de Servicios de Negocio	✓
Conformidad	✓

Tabla 41 Principios involucrados en Proceso "Administrar Cambios". Fuente: Elaboración Propia

Matriz RACI: Administrar Cambios								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
	1. Desarrollar e implementar procedimiento para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de evolutivos		A	C	C	R	C	C
2. Evaluar impacto y dar prioridad a evolutivos en base a las necesidades del negocio		I	C	C	A/R	C	C	R
3. Garantizar que cualquier evolutivo crítico y de emergencia sigue el proceso aprobado		I			A/R	R	R	I
4. Autorizar cambios		I	C	I	A/R		I	I
5. Hacer seguimiento y reportar estados del evolutivo		I	I	I	A/R	R	I	R
6. Establecer proceso de revisión para garantizar la implantación completa de los evolutivos		C			A/R			R
7. Diseminar la información relevante referente a los evolutivos		A	R	R	R		I	I
8. Documentar evolutivos		I			A/R	I		R

Tabla 42 Matriz RACI Proceso "Administrar Cambios". Fuente: Elaboración Propia

Métricas:

- Adaptabilidad de soluciones a cambios del negocio
- Porcentaje de cambios totales que son soluciones de emergencia.
- Solicitudes de cambio pendientes.

Entradas del Proceso	Salidas del Proceso
Portafolio de proyectos de TI actualizado	Descripción de proceso de evolutivo
Medidas para la mejora de la calidad	Reportes de estatus de evolutivo
Planes de acciones correctivas para riesgos relacionados con TI	Autorización de evolutivos
Directrices de administración de los proyectos	
Planes detallados de los proyectos	
Cambios requeridos en el catálogo de servicios	
Cambios de seguridad requeridos	
Requerimientos de servicios nuevos y/o actualizados	
Solicitud de servicio y/o cambio en la mesa de Servicios	
Registro y reportes de incidentes	

Tabla 43 Entradas y Salidas de Proceso "Administrar Cambios". Fuente: Elaboración Propia

7.2.3.4 Definir y Administrar el Catálogo de Servicios (Co-Im 04)

Definición: Es necesario contar con una definición documentada y un acuerdo de TI y de niveles de servicios con los clientes internos. Lo anterior implica necesariamente administrar los servicios de proveedores con una clara definición de roles, responsabilidades y expectativas de éstos. Para que exista una administración del catálogo de servicios efectiva también se debe monitorear la efectividad y cumplimiento de los servicios que se entregan a los clientes internos, así como los que se reciben desde terceros, notificando a los interesados sobre el cumplimiento de los niveles de servicios. El monitoreo incluye también una revisión periódica del desempeño actual y la capacidad de los recursos de TI, incluyendo un pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias.

Objetivo: Asegurar la alineación de los servicios claves de TI con la estrategia del negocio, brindando servicios satisfactorios con transparencia acerca de los beneficios, riesgos y costos.



Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	✓✓
Conformidad	

Figura 35 Nivel y Dominio de Proceso "Definir y Administrar Catálogo de Servicios". Fuente: Elaboración Propia

Tabla 44 Principios involucrados en Proceso "Definir y Administrar Catálogo de Servicios". Fuente: Elaboración Propia

Matriz RACI: Definir y Administrar Catálogo de Servicios								
Prácticas	Dominios de Gobierno TI							
	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Crear un marco de trabajo para los servicios de TI		A/C			A/R			R
2. Construir un catálogo de servicios de TI		A	C		R			R
3. Definir los convenios de niveles de servicio (SLAs) para los servicios críticos de TI	I	A/R	C	C	C	C		R
4. Definir los convenios de niveles de operación (OLAs) para soportar los SLAs		I	R	R	A/R	R	C	C
5. Revisar los SLAs y los contratos de apoyo a clientes internos		A/R	C	I	I	I	I	R
6. Revisar y actualizar el catálogo de servicios de TI		A/R	C	C	C	R		R

Tabla 45 Matriz RACI Proceso "Definir y Administrar Catálogo de Servicios". Fuente: Elaboración Propia

Métricas:

- Número de servicios entregados por TI que no se encuentran en el catálogo de servicio.
- Porcentaje de servicios que cumplen con los niveles de servicios acordados.

Entradas del Proceso	Salidas del Proceso
Plan estratégico de TI	Reporte de revisión de contrato
Hoja de ruta del plan estratégico	Requerimientos de servicios nuevos y/o actualizados
Portafolio de proyectos de TI actualizado	SLAs actualizados
Clasificación de datos asignada	OLAs actualizados
SLAs planteados inicialmente	Portafolio de servicios actualizado
SLAs actualizados	Catálogo de proveedores
OLAs planeados inicialmente	Riesgos de proveedores
Requerimientos de servicios contra desastres incluyendo roles y responsabilidades	Reporte sobre la capacidad
Indicadores de desempeño a planeación de TI	Plan de desempeño y capacidad
Requerimientos de servicios contra desastres incluyendo roles y responsabilidades	Cambios requeridos
Especificación de disponibilidad, continuidad y recuperación	
Requerimientos de monitoreo de sistemas	

Tabla 46 Entradas y Salidas de Proceso "Definir y Administrar Catálogo de Servicios". Fuente: Elaboración Propia

7.2.4 *Entregar y Dar Soporte (En-DS)*

A continuación se exponen los procesos correspondientes a la entrega y soporte. Estos procesos cobran sentido una vez que las soluciones han sido construidas e implementadas y ya se encuentran operando como parte del negocio. Por lo tanto, se pretende que estas soluciones estén en pie en la subgerencia de informática, en tanto que esta es una unidad de servicios. Por lo anterior, se ubican en el nivel de dirección y control operacional.

7.2.4.1 Garantizar la Seguridad de los SI/TI (En-DS 01)

Definición: La necesidad de mantener la integridad de la información y de proteger los activos de TI debe ser un proceso que incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. Se debe incluir la realización de monitoreo de seguridad y pruebas periódicas así como la realización de acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Objetivo: Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

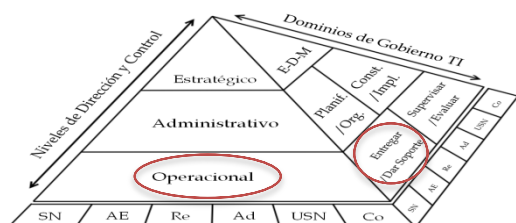


Figura 36 Nivel y Dominio de Proceso "Garantizar la Seguridad de los SI/TI". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	
Responsabilidad	✓
Adquisición	
Unidad de Servicios de Negocio	✓ ✓
Conformidad	✓

Tabla 47 Principios involucrados en Proceso "Garantizar la Seguridad de los SI/TI". Fuente: Elaboración Propia

Matriz RACI: Garantizar la Continuidad de los SI/TI								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
	1. Establecer modelo de seguridad formal		C		C	R	R	A/R
2. Administrar el acceso y seguridad a los activos de TI		C	I	I	I	A/R	A/R	
3. Supervisar la infraestructura para eventos relacionados con la seguridad		I				A/R	R	

Tabla 48 Matriz RACI Proceso "Garantizar la Seguridad de los SI/TI". Fuente: Elaboración Propia

Métricas:

- Número de incidentes de seguridad con impacto al negocio.
- Resultados de pruebas de seguridad

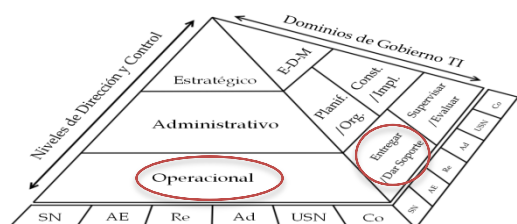
Entradas del Proceso	Salidas del Proceso
Arquitectura de la información	Requerimientos específicos de entrenamiento sobre conciencia de seguridad
Clasificación de datos asignada	Cambios de seguridad requeridos
Estándares Tecnológicos	Amenazas y vulnerabilidades de seguridad
Evaluación de riesgos	Políticas y planes de seguridad
Especificaciones de los controles de seguridad de las aplicaciones	
OLAs actualizados	

Tabla 49 Entradas y Salidas de Proceso "Garantizar la Seguridad de los SI/TI". Fuente: Elaboración Propia

7.2.4.2 Definir Modelo de Soporte SI/TI (En-DS 02)

Definición: Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-efecto y resolución y propuestas de mejora.

Objetivo: permitir el efectivo uso de los SI/TI garantizando la resolución y el análisis de las consultas de los usuarios finales, incidentes y preguntas.



Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	✓ ✓
Conformidad	

Figura 37 Nivel y Dominio de Proceso "Definir modelo de soporte SI/TI". Fuente: Elaboración Propia

Tabla 50 Principios involucrados en Proceso "Definir modelo de soporte SI/TI". Fuente: Elaboración Propia

Matriz RACI: Definir modelo de soporte SI/TI								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Establecer y mantener un marco de trabajo para el soporte de los SI/TI		C	C	C	A/R	I		C
2. Definir procedimientos de monitoreo y escalamiento basado en SLAs definidos.		I		C	A/R	C	R	
3. Administrar programa de riesgos de servicios de SI/TI		I	I	I	R	C	A/R	C
4. Definir políticas y estándares que apoyen la gestión de soporte de SI/TI		I	I	I	R	I	C	A/R

Tabla 51 Matriz RACI Proceso "Definir modelo de soporte SI/TI". Fuente: Elaboración Propia

Métricas:

- Porcentaje de incidentes resueltos dentro del lapso de tiempo acordado.
- Acumulación de consultas sin resolver.

Entradas del Proceso	Salidas del Proceso
Manuales de usuario, técnicos, de soporte y de administración de los sistemas	Marco de trabajo para la gestión de soporte de SI/TI
SLAs actualizados	
OLAs actualizados	

Tabla 52 Entradas y Salidas de Proceso "Definir modelo de soporte SI/TI". Fuente: Elaboración Propia

7.2.4.3 Administrar la Configuración (En-DS 03)

Definición: Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite.

Objetivo: Optimizar la infraestructura, activos informático-tecnológicos y capacidades de TI, y llevar registro de los activos de TI.



Figura 38 Nivel y Dominio de Proceso " Administrar la Configuración". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	✓✓
Conformidad	✓

Tabla 53 Principios involucrados en Proceso "Administrar la Configuración". Fuente: Elaboración Propia

Matriz RACI: Administrar la Configuración								
Prácticas	Dominios de Gobierno TI							
	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Establecer y mantener modelo de configuración			C		A/R	C	C	
2. Recopilar información sobre la configuración inicial y establecer líneas base					A/R	C		
3. Verificar y auditar la información de la configuración (incluye la detección de software no autorizado)		I			R	C		A/R
4. Actualizar el repositorio de configuración					A/R			

Tabla 54 Matriz RACI Proceso " Administrar la Configuración". Fuente: Elaboración Propia

Métricas:

- Porcentaje de licencias compradas y no registradas en el repositorio.
- Número de desviaciones identificadas entre el repositorio de configuración y las configuraciones actuales de activos.

Entradas del Proceso	Salidas del Proceso
Manuales de usuario, técnicos, de soporte y de administración de los sistemas	RFC (dónde y cómo aplicar el parche)
Componentes de configuración liberados	Detalles de configuración/activos de TI
Criticidad de puntos de configuración de TI	

Tabla 55 Entradas y Salidas de Proceso "Administrar la Configuración". Fuente: Elaboración Propia

7.2.4.4 Administrar Operaciones Tecnológicas (En-DS 04)

Definición: Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware.

Objetivo: Mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperarse de errores y fallas.



Figura 39 Nivel y Dominio de Proceso "Administrar Operaciones Tecnológicas". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	
Alineación Estratégica	
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	✓ ✓
Conformidad	

Tabla 56 Principios involucrados en Proceso "Administrar Operaciones Tecnológicas". Fuente: Elaboración Propia

Matriz RACI: Administrar Operaciones Tecnológicas								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de Negocio	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Crear procedimientos de operación (incluyendo manuales, planes de cambios, procedimientos de escalamiento, etc.)				I	A/R			R
2. Programación de cargas de trabajo y de programas en lote				I	A/R	I		
3. Monitorear la infraestructura y procesar y resolver problemas		I		I		A/R		R
4. Administrar y asegurar la salida física de información (reportes, medios, etc.)					A/R		C	
5. Aplicar cambios al programa y la infraestructura		I			A/R	A/R	C	C
6. Implementar un proceso para salvaguardar los dispositivos de autenticación contra interferencias, pérdida o robo.						A/R	R	
7. Programar y llevar a cabo mantenimiento preventivo							A/R	

Tabla 57 Matriz RACI Proceso "Administrar Operaciones Tecnológicas". Fuente: Elaboración Propia

Métricas:

- Número de niveles de servicio impactados por incidentes operativos.
- Horas de tiempo sin servicio no planeadas causadas por incidentes en la operación.
- Porcentaje de peticiones y trabajos programados que no se cumplen a tiempo.

Entradas del Proceso	Salidas del Proceso
Manuales de usuario, técnicos, de soporte y de administración de los sistemas	Tickets de incidentes
Liberación a producción	Bitácora de errores
Liberación de software y plan de distribución	Reportes de desempeño de los procesos
SLAs actualizados	
OLAs actualizados	
Plan de almacenamiento de respaldos y de protección	
Detalles de configuración/activos de TI	

Tabla 58 Entradas y Salidas de Proceso "Administrar Operaciones Tecnológicas". Fuente: Elaboración Propia

7.2.5 *Supervisar y Evaluar (Su-Ev)*

A continuación se expone el set de procesos de supervisión y evaluación. Estos procesos tienen como fin el cumplimiento de los estándares y requisitos que se le exigen a la TI. Se encuentra en el plano operacional debido a que estos procesos deben ser ejecutados en la operación de los sistemas y servicios del día a día, por ende, desde el nivel de dirección y control mencionado.

7.2.5.1 Garantizar el cumplimiento Regulatorio (Su-Ev 01)

Definición: Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.

Objetivo: Cumplir las leyes y regulaciones relacionados con TI.



Figura 40 Nivel y Dominio de Proceso "Garantizar el Cumplimiento Regulatorio". Fuente: Elaboración Propia

Principios de Gobierno TI involucrados	
Soluciones de Negocio	✓
Alineación Estratégica	
Responsabilidad	
Adquisición	
Unidad de Servicios de Negocio	✓
Conformidad	✓✓

Tabla 59 Principios involucrados en Proceso "Garantizar el cumplimiento Regulatorio". Fuente: Elaboración Propia

Matriz RACI: Garantizar el Cumplimiento Regulatorio								
Prácticas	Comité de Informática	Subgerente TI	Jefe Gestión de Procesos de	Jefe Soporte Corporativo SAP	Jefe de Operaciones TI	Jefe de Infraestructura TI	Oficial de Seguridad	Aseguramiento y Control de Calidad
1. Definir y ejecutar proceso para identificar los requerimientos legales, contractuales de políticas y regulatorio.		C	I	I	I	I	A/R	R
2. Evaluar cumplimiento de actividades de TI con políticas, estándares y procedimientos de TI		A	R	R	R	R	A	
3. Reportar aseguramiento positivo del cumplimiento de las actividades de TI con las políticas, planes y procedimientos de TI	I	I	I	I	I	I	A/R	
4. Brindar retro alimentación para alinear las políticas, estándares y procedimientos de TI con los requerimientos de cumplimientos		I	R	R	R	R	A	I
5. Integrar los reportes de TI sobre requerimientos legales con salidas similares provenientes de otras funciones del negocio	I/C	C	C	C	C		A/R	

Tabla 60 Matriz RACI Proceso "Garantizar el Cumplimiento Regulatorio". Fuente: Elaboración Propia

Métricas:

- Resultado de las revisiones de cumplimiento.

Entradas del Proceso	Salidas del Proceso
Requerimientos de cumplimiento legal y regulatorio vigentes	Catálogo de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI
Políticas de TI	Reporte sobre el cumplimiento de las actividades de TI con los requerimientos externos legales y regulatorios

Tabla 61 Entradas y Salidas de Proceso "Garantizar el Cumplimiento Regulatorio". Fuente: Elaboración Propia

8. CONCLUSIONES

Se ha establecido la importancia de contar con sistemas de la información y con tecnologías de información en las organizaciones. Esto es debido a las importantes mejoras que estos elementos le dan a las compañías para responder con rapidez y precisión a las demandas del entorno. Por otro lado, también agilizan la automatización de los procesos operativos, suministrando así una plataforma de información necesaria para la toma de decisiones (Ayala, 2014).

Sumado a lo anterior, gracias a la necesidad de que éstas cuenten con estructuras y directrices claras de organización, también se ha establecido la importancia de contar con modelos de administración. Aun así, según lo que se ha tratado en el marco teórico de este trabajo, la experiencia ha demostrado que no basta que las organizaciones tengan tecnologías de información y no es suficiente que se acojan bajo modelos de administración TI. Eso no significa que lo anterior esté incorrecto, pero con solo dichos elementos no es suficiente. También tiene que considerarse que estas tecnologías y su administración estén en sintonía con los intereses, necesidades y demandas del negocio. En ese contexto nace la necesidad de establecer un gobierno TI, de tal manera que sea éste el que se preocupe de asentar los lineamientos de TI con la organización y de establecer las bases para su gestión y administración.

No obstante lo anterior, dependerá todo desde el prisma de donde se mire. Como se ha mencionado a lo largo de esta tesis, hay autores que sostienen un punto de vista con relación al gobierno TI netamente estratégico (Peterson, 2003), (Cano, 2006). Por otro lado, otros autores sostienen, que el gobierno debe trascender también hacia el plano administrativo (Hamaker & Hutton, 2003). Para efectos de este trabajo, y en concordancia con las demandas de este caso en particular, se aborda el gobierno TI desde una perspectiva más amplia y completa llegando incluso al plano organizacional tal como lo plantea Weill et al. (2003).

Sin embargo, es necesario considerar también cada situación en particular, estudiar cómo se despliega la empresa en cuanto a las TI, cómo opera en su administración, cómo es su estructura organizacional, etc. Luego comprendida la situación actual, recién es posible considerar los modelos de gobierno TI existentes y tomar de ellos aquellos aspectos que son coherentes y realmente una ayuda para el negocio.

En base a las premisas anteriormente mencionadas, se propuso un modelo de gobierno TI para la empresa de servicios sanitarios señalada. Se estableció una pirámide de gobierno TI que abarca los principales aspectos de gobierno TI señalados en la literatura. Bajo los conceptos de dicha pirámide, se estableció un conjunto de procesos que cuentan con una definición, objetivos y actividades principales para llevarlo a cabo. Cada proceso establece entradas y salidas y formas de poder medirlo.

El modelo de gobierno TI propuesto, contiene los conceptos e ideas principales para construirse. Establece su estructura de relaciones, niveles de dirección y control, dominios

de gobierno y los principios por los cuales se debe regir dicho gobierno TI, lo cual es el fundamento del gobierno TI propuesto.

No obstante lo anterior, es importante continuar en la labor de enriquecer dicho Gobierno TI. Es necesario, que exista un riguroso plan de implementación, de tal manera que los interesados encuentren en dicho Gobierno TI las ventajas que éste puede otorgar y que el negocio sea beneficiado en aspectos de eficiencia y ventaja competitiva en el manejo de las TI.

Por otra parte, esta propuesta no ofrece un modelo exhaustivo para medir la madurez de los procesos, y en consecuencia, el marco en general, ya que su enfoque principal se encuentra en asentar las bases y fundamentos de Gobierno TI. Sin embargo, una vez que se haya establecido una cultura de Gobierno TI en la organización y un modelo, será naturalmente necesario ampliar la construcción de éste incorporando estándares de medición eficaces reconocidos en la literatura.

Añadiendo a lo anterior, esta propuesta no contiene ninguna herramienta adicional que obligue a quienes son responsables a ejecutar el marco de gobierno, tal como un sistema que exija índices de avances en la ejecución de los procesos. En la medida que el Gobierno TI comience a ser parte de la empresa del caso estudio, será necesario contar con este tipo de herramientas, ya que permitirá un control exacto y detallado y un canal de comunicación entre los interesados.

Además de lo anterior, a medida que el modelo vaya madurando en la subgerencia de informática, será necesario hacer revisiones que incorporen mejoras al modelo. Lo anterior, puede significar agregar nuevos procesos, quitar o modificar los que ya existen. También puede incidir en los principios establecidos, en tanto que las demandas hacia las TI son dinámicas y la organización también va mudando en el tiempo. Estas revisiones siempre deben tener como input principal, la organización, su misión, visión, valores, estrategias, y cómo ésta se va desenvolviendo en su entorno. El proceso de mejora continua del Gobierno TI propuesto, también debe considerar el ambiente y los aportes en el marco teórico actual, ya que éste va considerando las tendencias y demandas del mercado que van surgiendo.

El modelo propuesto, tiene características propias de la empresa en estudio. Sin embargo, en la medida que otras empresas tengan una visión completa de las TI, quiere decir, que la hagan responsable de sus operaciones, administración y además, la consideren un aliado estratégico del negocio, este marco de trabajo puede ser adoptado. En este caso, debe adaptar las áreas de servicio del negocio a las que la propia compañía tenga, ya que en ese sentido, cada una cuenta con una estructura particular.

9. REFERENCIAS

- Andrade, A., & Rossetti, J. P. (2004). *Governança corporativa: fundamentos, desenvolvimento e tendências*. São Paulo: Atlas.
- Ayala, J. B. (jun de 2014). Aplicación de las tecnologías de la información (TI) a la mejora de la inteligencia en las organizaciones. *Inteligencia y Seguridad: Revista de Análisis y Prospectiva.*, 2014(15), 45-76.
- Ballester, M. (mayo de 2009). ISO/IEC 38500, La norma para el Gobierno de las TIC. *revistadintel*, 126-128.
- Barriga Jiménez, S., González Gabaldón, B., Cantero-Sánchez, F., León Rubio, J. M., Gómez Delgado, T., & Medina Anzano, S. (1998). *Psicología social : orientaciones teóricas y ejercicios prácticos*. Madrid: McGraw-Hill Interamericana de España.
- Bauset-Carbonell, M. C., & Rodenes-Adam, M. (sep/oct de 2012). La gestión de Servicios de TI: ITIL e ISO/IEC 20000. *DYNA - Ingeniería e Industria*, 87(5), 492-495.
- Blair, M. M. (1995). *Ownership and control : rethinking corporate governance for the twenty-first century*. Washington, D. C.: Brookings Institute.
- Bowen, P., Cheung, M.-Y., & Rohde, F. (2007). Enhancing IT governance practices: a model and case study of an organization's efforts. *Accounting Information Systems*, 8(3), 191-221.
- Cano, J. J. (2006). Arte y Ciencia del Gobierno de TI. *Sistemas*, 54-64.
- Ceballos, C. (10 de 11 de 2014). Funcionamiento Departamento de Soporte Corporativo SAP. (D. Firmani, Entrevistador)
- Ceballos, C. (10 de 11 de 2014). Funcionamiento Departamento de Soporte Corporativo SAP. (D. Firmani, Entrevistador)
- De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (Spring de 2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems.*, 27(1), p307-324.
- De Wit, B., & Meyer, R. (2005). Strategy Synthesis: Resolving Strategy Paradoxes to Create Competitive Advantage. *Academy of Management Learning & Education*, 4(4), 516 –527.
- Elbashit, M. Z., Collier, P. A., & Michael J., D. (2008). Measuring the effects of business intelligence systems: The relationship between business process and organizational performance. *International Journal of Accounting Information Systems*, 9(3), 135-153.
- Essbio. (10 de 11 de 2014). *Essbio*. Obtenido de <https://www.essbio.cl/nosotros/>

- Essbio. (23 de 10 de 2014). *Portal de Colaboración ESSBIO S.A.* Obtenido de <http://portal.aguas.local>
- Fernandes, A. A., & Abreu, V. F. (2008). *implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços* (Segunda ed.). Rio de Janeiro: Brasport.
- Flôres, E. A. (2004). *Governança corporativa no Brasil e o papel dos investidores institucionais*. Tesis (Doctorado), Pontificia Universidade Católica do Rio de Janeiro, Rio de Janeiro.
- Franco.IT-grc. (14 de 04 de 2012). *IT – Governance, Risk & Compliance*. Recuperado el 01 de 11 de 2014, de <https://francoitgrc.wordpress.com/2012/04/14/cobit-5-update-por-version-oficial-de-isaca/>
- Hamaker, S. (2003). Spotlight on Governance. *Information Systems Audit and Control Association*, 1.
- Hamaker, S., & Hutton, A. (2003). Principles of Governance. *Information Systems Audit and Control Association*, 3.
- Hamaker, S., & Hutton, A. (2004). Principles of IT Governance. *Information Systems Audit and Control Association*, 3.
- Hirschheim, R., Schwarz, A., & Todd, P. (2006). A marketing maturity model for IT: Building a customer-centric IT organization. *Ibm Systems Journal*, 45(1), 181-203.
- IBGC. (2006). *Guia de orientação para o gerenciamento de riscos corporativos*. São Paulo: Instituto Brasileiro de Governança Corporativa.
- Isaca. (2009). *The Risk IT Framework: Risk IT Based on COBIT*. Rolling Meadows, IL: ISACA.
- Isaca. (2010). *Enterprise Value: Governance of IT Investments. The Val IT Framework 2.0*. Rolling Meadows, IL: ISACA.
- Isaca. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: ISACA.
- ISO 27001:2005. (s.f.). *Sistemas de Gestión de Seguridad de la Información*.
- ISO/IEC. (2008). *ISO/IEC 38500 Corporate Governance of Information Technology*. Geneva, Switzerland.
- ISO27000.es. (24 de 12 de 2014). *ISO 27000.ES*. Obtenido de http://www.iso27000.es/sgsi_implantar.html
- ITGI. (2007). *COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute.
- ITGI. (2009). *An executive view of IT Governance*. Rolling Meadows, IL: IT Governance Institute.

- ITGI. (2011). *Board Briefing on IT Governance* (Segunda ed.). Rolling Meadows, IL: IT Governance Institute.
- Jaeger-Neto., J. I., Luciano, E. M., Becker, C. A., & Testa, M. G. (2009). The perception of operational managers on the impacts on work processes after the implementation of best practices in IT governance in the Regional Court of Santa Catarina (TRE/SC). *Revista de Administração Pública*, 8(1), 1-18.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: managerial behavior, agency costs. *Journal of Financial Economics*, 3(1), 305-360.
- Kaplan, R. S., & Norton, D. P. (1996). *The Balanced Scorecard: Translating Strategy Into Action*. Boston: Harvard Business Press.
- Lorente, J. J. (2011). ¿Qué es el gobierno de las TI? En A. Fernández, & F. Llorens, *Gobierno de las TI para universidades* (págs. 32-46). Madrid: Conferencia de Rectores de las Universidades Españolas (CRUE).
- Lunardi, G. L. (2008). *Um estudo empírico e analítico do impacto da governança de TI no desempenho*. Tesis (doctorado), Universidade Federal do Rio Grande do Sul, Porto Alegre.
- Martin, N. C., Dos Santos, L. R., & Dias, J. M. (2004). Governança empresarial, riscos e controles internos: a emergência de um novo modelo de controladoria. *Revista Contabilidade & Finanças*, 15(34), 7-22.
- Muñoz, H. (11 de 11 de 2014). Funcionamiento Departamento de Infraestructura TI. (D. Firmani, Entrevistador)
- Muñoz, M. (06 de 11 de 2014). Funcionamiento Departamento Gestión TI Procesos de Negocio. (D. Firmani, Entrevistador)
- Pelanda, M. L. (2006). *Modelos de governança de tecnologia da informação adotados no Brasil : um estudo de casos múltiplos*. Tesis Magíster, Universidade Metodista de São Paulo, São Paulo.
- Peterson, R. (2003). Integration Strategies and Tactics for Information Technology Governance. *Strategies for Information Technology Governance*, 37-80.
- Puente, A. (16 de 10 de 2014). Funcionamiento Subgerencia TI. (D. Firmani, Entrevistador)
- Ruiz, R. (12 de 11 de 2014). Funcionamiento Departamento de Operaciones. (D. Firmani, Entrevistador)
- Silveira, A. D. (2002). *Governança corporativa, desempenho e valor na empresa no*. Tesis (Magíster), Universidade de São Paulo, São Paulo.

- Simonsson, M., & Johnson, P. (2006). Defining IT governance-a consolidation of literature. *the 18th Conference on Advanced Information Systems Engineering*, 6.
- Smits, D., & Hillegersberg, J. v. (2013). The Continuing Mismatch Between IT Governance Theory and Practice: Results from a Delphi Study with CIO's. *AMCIS 2013*. Chicago.
- Souza N, J., & Ferreira N, A. N. (Sept/Dec de 2013). Metamodelo do framework COBIT de governança de TI. *Revista de Gestão da Tecnologia e Sistemas de Informação*, 10(3), 521-540.
- Van Grembergen, W. (2004). *Strategies for information technology governance*. Hershey • London: Idea Group Inc.
- Vera, M. (05 de 11 de 2014). Funcionamiento Oficial de Seguridad y Control de Calidad. (D. Firmani, Entrevistador)
- Weill, P., & Ross, W. J. (2006). *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores*. São Paulo: Makron.
- Weill, P., Broadbent, M., & Blosch, M. (Enero de 2003). How to Achieve Effective IT Governance. *Financial Times*.
- Wilkin, C. L., & Chenhall, R. H. (2010). A Review of IT Governance: A Taxonomy to Inform Accounting Information Systems. *Journal of Information Systems*, 24(2), 107-146.

10. ANEXO I: MAPEO PROCESOS DE TI A LOS PRINCIPIOS DE GOBIERNO TI

Tabla 62 Tabla de Mapeo de Procesos TI a los Principios de Gobierno TI

Código Proceso	Nombre Proceso	Principios Gobierno TI					
		Soluciones de Negocio	Alineación Estratégica	Responsabilidad	Adquisición	Unidad de Servicios de Negocio	Conformidad
E-D-M 01	Definir un Plan estratégico de TI	✓	✓✓	✓			
E-D-M 02	Definir la Arquitectura de la Información	✓	✓✓		✓	✓	
E-D-M 03	Monitorear y Evaluar el desempeño de TI		✓	✓		✓✓	✓
E-D-M 04	Definir Procesos, Organización y Relaciones de TI	✓	✓✓	✓		✓	✓
E-D-M 05	Administrar la Inversión en TI	✓	✓		✓✓		
E-D-M 06	Definir Cartera de Proyectos TI para la Compañía	✓✓	✓✓			✓	✓
Pl-Or 01	Administrar la Calidad	✓✓		✓	✓	✓✓	✓
Pl-Or 02	Definir Plan de Contingencia		✓✓	✓		✓✓	✓
Pl-Or 03	Establecer Framework de Administración de Programas y Proyectos	✓✓					
Co-Im 01	Administrar la Tecnología	✓	✓		✓✓		
Co-Im 02	Disponibilizar y Mantener Infraestructura Tecnológica	✓			✓	✓✓	
Co-Im 03	Administrar Cambios		✓		✓	✓	✓
Co-Im 04	Definir y Administrar el Catálogo de Servicios					✓✓	
En-DS 01	Garantizar la Seguridad de los SI/TI			✓		✓✓	✓
En-DS 02	Definir Modelo de Soporte SI/TI					✓✓	
En-DS 03	Administrar la Configuración					✓✓	✓
En-DS 04	Administrar Operaciones Tecnológicas					✓✓	
Su-Ev 01	Garantizar el cumplimiento Regulatorio	✓				✓	✓✓

11. ANEXO II: DESCRIPCIÓN DE PROCESOS COBIT 4.1

A continuación se da una breve descripción de cada proceso agrupadas según su dominio de COBIT 4.1 con el fin de tener una visión más amplia del framework.

a. Planear y Organizar (PO)

1. **Definir un Plan Estratégico de TI:** Este proceso es necesario para gestionar y dirigir todos los recursos de TI de tal manera que estén alineados con la estrategia y prioridades del negocio, que a su vez se deben reflejar en portafolios que se ejecutan por planes estratégicos de TI que especifican objetivos concisos, planes de acción y tareas entendidas por el negocio y por TI.

2. **Definir la Arquitectura de la Información:** La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad que garantice la integridad y consistencia de los datos.

3. **Determinar la Dirección Tecnológica:** Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias.

4. **Definir los Procesos, Organización y Relaciones de TI:** Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones.

5. **Administrar la Inversión en TI:** Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias.

6. **Comunicar las Aspiraciones y la Dirección de la Gerencia:** La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados

por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.

7. **Administrar Recursos Humanos de TI:** Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación.

8. **Administrar la Calidad:** Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables.

9. **Evaluar y Administrar los Riesgos de TI:** Crear y mantener un marco de trabajo de administración de riesgos que documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

10. **Administrar Proyectos:** Establecer un framework de administración de programas y proyectos para la gestión de todos los proyectos de TI establecidos que garantice la correcta asignación de prioridades y la coordinación de todos los proyectos. Debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan de pruebas, revisión de pruebas y post-implantación después de la instalación garantizando la gestión de riesgos del proyecto y la entrega de valor para el negocio.

b. Adquirir e Implementar (AI)

1. **Identificar soluciones automatizadas:** La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final.

2. **Adquirir y mantener software aplicativo:** Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares.

3. **Adquirir y mantener infraestructura tecnológica:** Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas.
4. **Facilitar la operación y el uso:** El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.
5. **Adquirir recursos de TI:** Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí.
6. **Administrar cambios:** Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación.
7. **Instalar y acreditar soluciones y cambios:** Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación.

c. Entregar y Dar Soporte (DS)

1. **Definir y administrar los niveles de servicio:** Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (stakeholders) sobre el cumplimiento de los niveles de servicio.
2. **Administrar los servicios de terceros:** La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.
3. **Administrar el desempeño y la capacidad:** La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso

incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias.

4. **Garantizar la continuidad del servicio:** La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad.

5. **Garantizar la seguridad de los sistemas:** La necesidad de mantener la integridad de la información y de proteger los activos de TI debe ser un proceso que incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. Se debe incluir la realización de monitoreo de seguridad y pruebas periódicas así como la realización de acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

6. **Identificar y asignar costos:** La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios.

7. **Educar y entrenar a los usuarios:** Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados.

8. **Administrar la mesa de servicio y los incidentes:** Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución.

9. **Administrar la configuración:** Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite.

10. **Administrar los problemas:** Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas.

11. **Administrar los datos:** Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información

también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios.

12. **Administrar el ambiente físico:** La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico.

13. **Administrar las operaciones:** Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware.

d. Monitorear y Evaluar (ME)

1. **Monitorear y Evaluar el Desempeño de TI:** El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones.

2. **Monitorear y Evaluar el Control Interno:** Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

3. **Garantizar el Cumplimiento Regulatorio:** Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.

4. **Proporcionar Gobierno de TI:** El establecimiento de un framework de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas con las estrategias y objetivos empresariales.

2. ANEXO III: ENTREVISTAS

10.1 Oficial de Seguridad y Control de Calidad

Cargo Entrevistado : Oficial de Seguridad y Control de Calidad

Antigüedad en el cargo: 2 años

Objetivo Entrevista : Profundizar en el quehacer del cargo para tener una visión más detallada de los servicios que presta la subgerencia de informática, cómo los presta y hacia dónde se están dirigiendo en la práctica.

Modalidad Entrevista: Abierta

PREGUNTAS

1. ¿Cuáles son las principales labores del cargo Oficial de Seguridad y Aseguramiento de Calidad?

R: El Oficial de Seguridad y Aseguramiento de Calidad tiene a cargo:

- Realización de documentación de políticas, procedimientos u otros documentos concernientes con la seguridad y aseguramiento de la calidad, por ejemplo procedimientos de solicitud de habilitación de cuentas, procedimientos de respaldo de datos, políticas de Seguridad de la Información, catálogo de acuerdos de servicios, etc.
- Revisión de la documentación de los procedimientos elaborados por otros departamentos de la subgerencia de TI con el objetivo de asegurar la calidad de los procedimientos.
- Habilitación y/o inhabilitación de cuentas de red con el propósito de asegurar la calidad de la prestación del servicio y el acceso a la información de la compañía.
- Habilitación y/o inhabilitación de cuentas de diversos sistemas de la compañía cuando un trabajador es contratado o desvinculado de la empresa con el fin de resguardar la seguridad del acceso a la información de la compañía.
- Ser el nexo oficial entre la subgerencia de informática y la Gerencia de auditoría de la Empresa.
- Generación de informes mensuales al subgerente que rinda cuentas de las dificultades que existen en alguna área, por ejemplo, porcentaje del cumplimiento de los niveles de acuerdo de servicio (SLA por sus siglas en inglés), eficiencia de ejecución, tickets fuera de estándar u otros.
- Dar fluidez al proceso de auditorías externas a la subgerencia de informática, por ejemplo, auditorías de las redes, sistemas, entre otras.

2. ¿En qué se basan para realizar la documentación de los procedimientos?

R: Los procedimientos se realizan de acuerdo a una plantilla estándar de la empresa. Luego, el contenido del procedimiento está basado en los acuerdos que haya tenido cada área para efectuar tal procedimiento.

3. ¿Hay alguna regulación legal que competa al cargo?

R. Regulaciones legales sanitarias, no. Sin embargo, sí existen aspectos legales concernientes a la información, por ejemplo, licenciamiento de software, acceso a la información privada de los trabajadores, etc.

4. ¿Cuáles son los procedimientos que ya se tienen?

R: Instructivos respecto gestión de cuentas a diferentes sistemas, políticas de seguridad de la información, procedimientos de custodia y manejo de medios de respaldo y recuperación de la información, ingreso de requerimientos, solicitud de mantención, solicitud de soporte, procedimientos concernientes al sistema SAP, etc.

5. ¿Qué procedimientos faltan?

R: La meta es documentar todos los procedimientos que se realizan en la subgerencia de informática, de tal manera que éstos sean estandarizados y posteriormente llegar a la mejora continua de estos procedimientos.

6. ¿Cuáles son los planes a futuro para el área de seguridad y control de calidad?

R: Generar un plan de seguridad y calidad que abarque todas las áreas de la subgerencia de informática, estableciendo estándares en los procedimientos y en la calidad de los servicios que presta dicha subgerencia. Además se incorporará el seguimiento de los contratos externos y de presupuestos, con el fin de verificar si se cumple con lo establecido en los acuerdos y/o procedimientos.

10.2 Gestión TI y procesos de Negocio

Cargo Entrevistado: Jefe de Gestión de Procesos de Negocio

Antigüedad en el cargo: 5 meses

Objetivo Entrevista: Profundizar en el quehacer del cargo para tener una visión más detallada de los servicios que presta la subgerencia de informática, cómo los presta y hacia dónde se están dirigiendo en la práctica.

Modalidad Entrevista: Abierta

1. ¿Cuál es el objetivo del área de gestión de procesos de negocio?

R: El área de gestión de procesos de negocio tiene como fin apoyar a todas las áreas del negocio para desarrollar soluciones que generen valor al negocio.

2. ¿Cómo se lleva a cabo el funcionamiento del área?

R: Cuando un usuario propone una iniciativa o idea de proyecto, ésta es recibida por esta área y estudiada en profundidad por los ingenieros de proceso, los cuales deben tener un conocimiento cabal de cómo opera el negocio para evaluar si es que efectivamente la iniciativa del usuario realmente es una iniciativa que debe tratarse como un proyecto nuevo o bien, como una mejora de algún sistema ya existente o, en su defecto, si no corresponde ninguna de las dos alternativas anteriores, comprobar si se necesita la corrección de alguna práctica que no amerita la construcción de algún sistema. Luego, si la iniciativa efectivamente corresponde a un proyecto, éste se someta a una evaluación por parte de un comité de TI que identifica si hay otras áreas que pudieran ser afectadas por el nuevo sistema, y si éste debiera considerar funcionalidades que pudieran potenciar la utilidad y la generación de valor al negocio, o si pudiese existir algún aspecto legal que potencie la

ejecución del proyecto o bien, cualquier otro factor que amplíe la utilidad del proyecto. Posteriormente se realizan cotizaciones a los proveedores, y dependiendo de la magnitud del proyecto se solicitan cotizaciones a proveedores de confianza (basado en experiencias anteriores con éstos, los cuales responden oportunamente y que entregan productos de calidad), o se realiza una licitación pública. Finalmente la propuesta de proyecto con sus respectivas cotizaciones y la proposición de trabajar con uno en particular, se lleva el proyecto al comité de inversión, el cual es el encargado de aprobar o posponer el proyecto.

3. Una vez que el proyecto entró a su fase de construcción, ¿Cómo son tratados los cambios?

R: Cuando el cambio es pequeño no es modificado y se propone un evolutivo una vez finalizado. No obstante, cuando el cambio es muy drástico, entonces se detiene su construcción para una reevaluación del mismo.

4. ¿Cuál es el criterio para la elección de un proveedor?

R: La experiencia anterior con los mismos, y el enfoque que tenga el proveedor versus lo que el proyecto amerita, por ejemplo, si el proyecto utiliza la tecnología de SharePoint, entonces se buscan proveedores que sean expertos en SharePoint, de tal manera que se asegure un producto de buena calidad.

5. ¿Cuál es el criterio para la evaluación de un proyecto?

R: Hay diferentes criterios para evaluar un proyecto, por ejemplo, la transversalidad, la utilidad que puede generar, pero en resumen, cuánto valor le aporta al negocio.

6. ¿Hay procedimientos formales y documentados en el área?

R: Sí. Estos son confeccionados por el área y revisados por el oficial de seguridad y control de calidad.

7. ¿Están basados en algún marco legal para realizar los procedimientos?

R: No, los procedimientos están basados en modelos propios y en la experticia de los profesionales.

10.3 Soporte Corporativo SAP

Cargo Entrevistado : Jefe de Soporte Corporativo SAP

Antigüedad en el cargo: 1 año y 6 meses.

Objetivo Entrevista : Profundizar en el quehacer del cargo para tener una visión más detallada de los servicios que presta la subgerencia de informática, cómo los presta y hacia dónde se están dirigiendo en la práctica.

Modalidad Entrevista: Abierta

1. ¿Cuáles son las principales labores de la unidad de Soporte Corporativo SAP?

R: Este departamento es responsable de estar siempre actualizado con la agenda SAP y mantenerse en constante investigación de los productos de SAP, con el fin de contribuir al negocio nuevas soluciones que están relacionadas con el sistema.

Trabajar también, en conjunto con el departamento de gestión TI y procesos y de negocio y con el departamento de operaciones.

Además de esto, por temas circunstanciales, la unidad tiene a cargo la cartera de iniciativas financieras, y para dichos casos, se trabaja bajo el alero de los procedimientos del departamento de gestión TI y procesos de negocios.

Asimismo, la unidad está a cargo de hacer gestión del conocimiento proponiendo estructuras y herramientas adecuada para éste.

2. ¿Cómo interactúa con las demás áreas de la subgerencia de TI

R: La unidad de Soporte se encuentra para dar apoyo al área de gestión TI y procesos de negocio y operaciones en los temas vinculados a SAP.

Apoya al área de gestión TI y procesos de negocio cuando se levanta una iniciativa, porque cuando ésta surge, entonces se estudia si puede ser cubierta por SAP, en ese caso, la iniciativa se trabaja en conjunto con los dos departamentos. En ese caso, la labor de la unidad consiste en dar consultoría de todos los temas relacionados a la iniciativa, negociar con el proveedor si es necesario.

Apoya al área de operaciones cuando hay necesidad de soporte que no ha podido ser resuelto por el departamento de operaciones. En tal escenario, los consultores senior del departamento de soporte corporativo prestan el servicio de soporte, y en el caso que no puede ser resuelto por la unidad se gestiona el soporte con consultores externos.

3. ¿Cuáles son los problemas más recurrentes en los aspectos de Soporte?

R: En este sentido no trabajamos con los problemas recurrentes, ya que éstos los ve directamente operaciones.

4. En el ámbito de Gestión del Conocimiento, ¿qué se está trabajando?

R: En este sentido, se están estableciendo las estructuras y herramientas para la gestión del conocimiento. Se planea establecer una base de datos (metadato) centralizada donde las otras bases de datos tengan acceso a ella, por ejemplo, la base de datos de finanzas, mantención, etc. De esta forma, toda la información se pueda compartir entre las distintas áreas y/o departamentos de la compañía.

10.4 Infraestructura TI

Cargo Entrevistado : Jefe de Infraestructura TI

Antigüedad en el cargo: 3 meses

Objetivo Entrevista : Profundizar en el quehacer del cargo para tener una visión más detallada de los servicios que presta la subgerencia de informática, cómo los presta y hacia dónde se están dirigiendo en la práctica.

Modalidad Entrevista: Abierta

1. ¿Cuáles son las principales labores del Departamento de Infraestructura?

R: El departamento está a cargo de los servidores y de los enlaces de comunicación de toda la compañía. Esto incluye: Almacenamiento de datos, software, correo electrónico, seguridad, telefonía (fija y móvil).

2. ¿Cómo se organiza la infraestructura de los datos de la compañía?

R: A través de Cloud Computing, con el cual se tiene un contrato de plataforma como servicio, contando con bases de datos para aplicaciones y con bases de datos como repositorios.

3. ¿Cómo se administra la seguridad con el acceso de extraños a las bases de datos?

R: El proveedor debe proveer seguridad a través de sus propios mecanismos. No obstante, no hay un procedimiento de auditoría interna para verificar dicha seguridad.

4. ¿Cómo se administra la seguridad para la disponibilidad de la información?

R: El proveedor debe proveer seguridad a través de sus propios mecanismos según los acuerdos de los SLA. No obstante, el administrador interno verifica dicha disponibilidad y registra cada incidencia ocurrida, generando informes que permitan las acciones correspondientes frente a la falta de los acuerdos convenidos.

5. ¿Cuáles son los problemas más frecuentes?

R: En el tema de servidores en este momento tiene que ver SAP, y se debe a una migración de la plataforma, la cual ha generado dificultades.

En el contrato de enlaces hay una plataforma bien estable.

10.5 Operaciones

Cargo Entrevistado : Jefe de Operaciones

Antigüedad en el cargo: 3 años

Objetivo Entrevista : Profundizar en el quehacer del cargo para tener una visión más detallada de los servicios que presta la subgerencia de informática, cómo los presta y hacia dónde se están dirigiendo en la práctica.

Modalidad Entrevista: Abierta

1. ¿En qué consiste y cómo opera el departamento de operaciones?

R: Este departamento es el encargado de:

- Entregar soporte a los sistemas: En este ámbito el departamento recibe, mediante el sistema de tickets ITS, una solicitud de soporte por algún sistema, el cual debe ser resuelto por el administrador de sistemas correspondiente, éste debe realizar un diagnóstico del ticket, entender el funcionamiento del proceso y del sistema. Si es un problema de configuración, entonces la solicitud la resuelve el mismo administrador, y si escapa dicho alcance, entonces se deriva la resolución del ticket mediante un proveedor externo.
- Administración de la mesa de ayuda: Esta área es la encargada de verificar los estados de los tickets y vela porque el cierre de éstos se efectúe en los plazos estipulados por los SLA.
- Administración de la plataforma de escritorio: Este proceso se encarga de monitorear los contratos de los computadores, notebooks e impresoras de la empresa y de realizar la renovación de éstos cuando la vida útil de estos implementos caduque.
- Licenciamiento de software

2. ¿Cuáles son las incidencias más recurrentes?

R: el 88% de los tickets corresponde al bloqueo de claves. Para esto, se está gestionando un sistema de desbloqueo de claves para sea efectuada por el usuario y se están haciendo las últimas validaciones correspondientes a políticas de la empresa, por ejemplo, que un

usuario con licencia médica no pueda efectuar el desbloqueo, ya que la empresa no permite que un trabajo con licencia médica ejecute trabajos.

3. ¿Los procesos más importantes están formalizados?

R: Hay algunos que están formalizados y otros que no han terminado su proceso, ya que éste debe pasar por tres etapas, escrito, revisado, publicado y difundido. Cuando es revisado debe estar coordinado con el área de auditoría de la empresa y además con temas legales, por lo tanto, algunos de ellos están en auditoría.

4. ¿Tienen algún modelo definido en la unidad?

R: Sí, pero no está formalizado. Básicamente se trata de que exista un canal único de contacto, el cual contenga compromisos bien definidos, bien impuestos por los SLA o los acordados con el usuario.

11. ANEXO IV: MARCOS COMPLEMENTARIOS DE GOBIERNO TI

11.1 ITIL

ITIL (Information Technology Infrastructure Library) es el conjunto de conceptos y mejores prácticas para la administración de servicios de TI (ITSM) para el desarrollo y las operaciones de TI establecido por la Oficina de Comercio del Gobierno del Reino Unido (OGC).

Originalmente se creó como una colección de libros, cada uno de los cuales cubría un área específica de prácticas de la administración de servicios de TI. ITIL se construyó utilizando el modelo de procesos de control y administración de las operaciones atribuido a Edwards en la década de 1950 Deming y a su ciclo Plan-Do-Check-Act (PDCA).



Figura 41 Ciclo de Vida del Servicio TI-ITIL

Publicado por primera vez en 1996 (v1) con más de treinta volúmenes, ITIL ha pasado por varios procesos de revisión, actualización y consolidación que lo llevaron a la versión 2 en 2000/2001, la versión 3 publicada en mayo de 2007, y la versión actual (2011).

El marco se basa principalmente en un modelo de procesos enfocados en el ciclo de vida para gestionar los servicios de TI. Como se puede apreciar en la Figura 41, el ciclo de vida mencionado se compone de cinco fases que se interrelaciona con el resto de fases del ciclo.

Las cinco fases del ciclo de vida de los servicios que propone ITIL 2011 son las

siguientes:

12. **Estrategia de servicio:** se ocupa del diseño, desarrollo e implantación de la gestión de servicios de TI como activo estratégico para la organización. El proceso de la estrategia de servicios comprende: la gestión de la cartera de servicios, la gestión financiera de TI y la gestión de la demanda.
13. **Diseño del servicio:** se encarga del diseño y desarrollo de los servicios y de los correspondientes procesos necesarios para apoyar dichos servicios. Entre los procesos del diseño de servicios figuran: la gestión del catálogo de servicios, la gestión de los niveles de servicio, la gestión de la disponibilidad, la gestión de la capacidad, la gestión de la continuidad de los servicios de TI, la gestión de la seguridad de la información y la gestión de proveedores.

14. **Transición del servicio:** se ocupa de la gestión y coordinación de los procesos, los sistemas y las funciones que se precisan para crear, comprobar e implantar servicios nuevos o modificados en las operaciones. Entre los procesos de transición del servicio figuran: la planificación y soporte de la transición, la gestión del cambio, la gestión de la configuración y los activos del servicio, la gestión del lanzamiento y el despliegue, la validación y comprobación del servicio, la evaluación y la gestión del conocimiento.
15. **Operaciones de servicio:** se ocupa de la coordinación, las actividades y los procesos necesarios para gestionar los servicios destinados a usuarios y clientes de empresas dentro de los niveles de servicio acordados. Los procesos de las operaciones de servicio son los siguientes: la gestión de eventos, el cumplimiento de peticiones, la gestión de incidencias, la gestión de problemas y la gestión del acceso.
16. **Mejora continua del servicio:** se ocupa de mejorar los servicios de forma constante para garantizar a las organizaciones que los servicios responden a las necesidades del negocio. La mejora continua trata sobre cómo mejorar el servicio, los procesos y las actividades de cada una de las fases del ciclo de vida.

La estrategia del servicio es el eje en torno al que giran todas las demás fases del ciclo de vida del servicio; es la fase de definición de políticas y objetivos. Solo la fase de mejora continua del servicio, que consiste en aprendizaje y mejora, abarca todas las fases del ciclo. Esta fase inicia los proyectos y programas de mejora, asignándoles prioridades en función de los objetivos estratégicos de la organización.

El patrón dominante en el ciclo de vida del servicio es el paso desde la estrategia del servicio al diseño del servicio, a la transición del servicio y a la operación del servicio hasta llegar a la mejora continua del servicio y volver a la estrategia del servicio, y así sucesivamente.

Existen 26 procesos oficiales a lo largo de todo el ciclo de vida del servicio. En la Tabla 63 se mencionan agrupados por la fase a la que pertenecen.

Tabla 63 Diagrama de Procesos de ITIL v2011. Fuente: Bauset-Carbonell & Rodenes-Adam (2012)

Estrategia del Servicio	Diseño del Servicio	Transición del Servicio	Operación del Servicio	Mejora Continua
1. Gestión Estratégica para los servicios de TI	1. Coordinación del Diseño	1. Planeación y Soporte a la Transición	1. Gestión de Eventos	1. Mejora de los 7 pasos
2. Gestión del Portafolio de Servicios	2. Gestión del Catálogo de Servicios	2. Gestión de Cambios	2. Gestión de Incidentes	
3. Gestión Financiera para Servicios de TI	3. Gestión de Niveles de Servicio	3. Gestión de Activos de Servicio Configuraciones	3. Cumplimiento de Solicitudes	
4. Gestión de la Demanda	4. Gestión de Disponibilidad	4. Gestión de Liberaciones e Implementaciones	4. Gestión de Problemas	
5. Gestión de Relaciones con el Negocio	5. Gestión de Capacidad	5. Validación y Pruebas del Servicio	5. Gestión de Accesos	
	6. Gestión de Continuidad de Servicios de TI	6. Evaluación del Cambio		
	7. Gestión de Seguridad de la Información	7. Gestión del Conocimiento		
	8. Gestión de Proveedores			

De cara al negocio, algunos de los beneficios de ITIL son mejorar la calidad del servicio y el soporte al negocio; aumentar la satisfacción del cliente, mediante la definición de los acuerdos de niveles de servicios prestados, SLA; y, formalizar los procesos de TI de manera que sean repetibles y sus resultados predecibles.

ITIL propone las mejores prácticas para desarrollar y desplegar políticas de seguridad que reflejen los objetivos del negocio y sus estrategias. En otras palabras ITIL propone cómo materializar el gobierno de TI partiendo de que su definición y aplicación efectiva son responsabilidad de la gerencia general de la empresa y de la dirección ejecutiva de la misma.

11.2 ISO 27001

Este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI). La adopción del SGSI debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa. La dinámica que implica su aplicación, ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un “proceso”. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Este estándar internacional adopta también el modelo “Plan-Do-Check-Act” (PDCA) (Ver Figura 42), el cual es aplicado a toda la estructura de procesos de SGSI, y significa lo siguiente (ISO 27001:2005)

Plan (Establecer el SGSI): Implica, establecer la política SGSI, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

Do (Implementar y operar el SGSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

Check (Monitorizar y revisar el SGSI): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

Act (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del SGSI

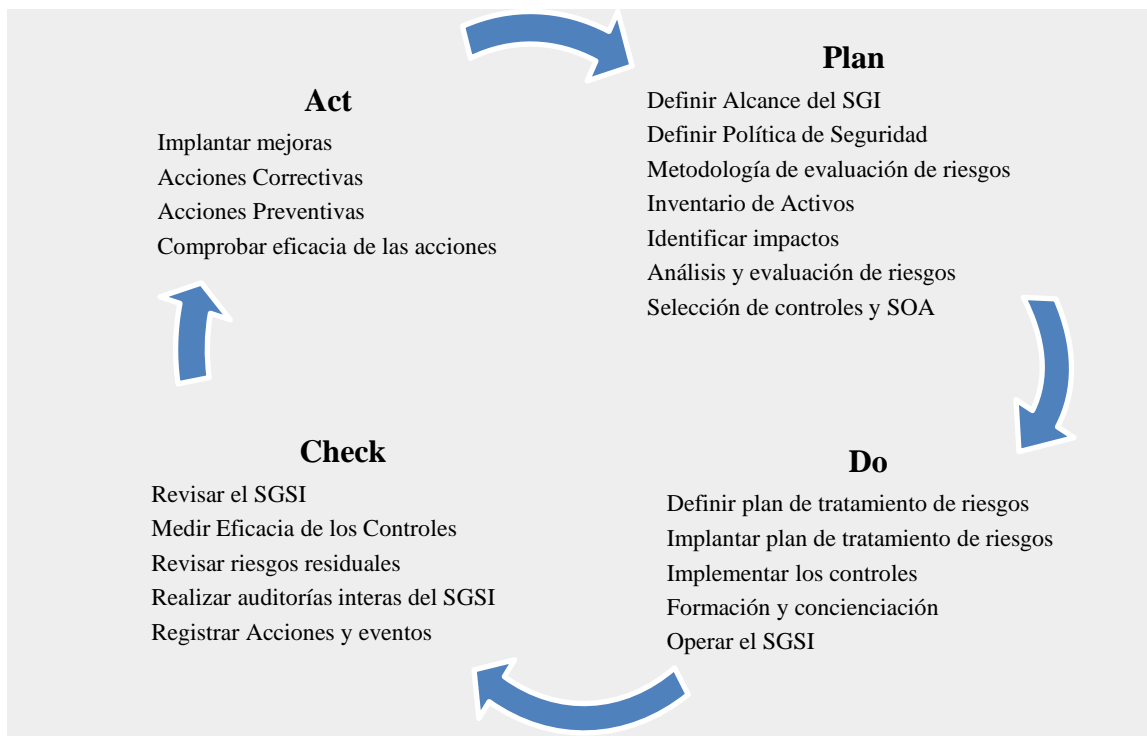


Figura 42 Ciclo Deming para un SGSI. Fuente: Elaboración Propia en Base a la Norma ISO 27001

Aplicación:

Los requerimientos establecidos en este estándar son genéricos y están diseñados para ser aplicados a todas las organizaciones, sin importar el tipo, tamaño o naturaleza. Incluye las siguientes cláusulas:

1. SGSI.
2. Responsabilidades de la Administración
3. Auditoría Interna del SGSI
4. Administración de las revisiones del SGSI
5. Mejoras del SGSI y Acciones correctivas.

SGSI: incluye las políticas, planes, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

Requerimientos generales:

La organización, establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documentado SGSI en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos. Para este propósito esta norma el proceso está basado en el modelo PDCA

Control de documentos: Todos los documentos requeridos por el SGSI serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- Aprobar documentos y prioridades o clasificación de empleo.
- Revisiones, actualizaciones y reprobaciones de documentos.
- Asegurar que los cambios y las revisiones de documentos sean identificados.
- Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
- Asegurar que los documentos permanezcan legibles y fácilmente identificables.
- Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- Asegurar que los documentos de origen externo sean identificados.
- Asegurar el control de la distribución de documentos.
- Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito

Responsabilidades de la administración: La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del SGSI a través de:

- Establecimiento de la política del SGSI.
- Asegurar el establecimiento de los objetivos y planes del SGSI
- Establecer roles y responsabilidades para la seguridad de la información
- Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto
- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el SGSI
- Decidir los criterios de aceptación de riesgos y los niveles del mismo
- Asegurar que las auditorías internas del SGSI, sean conducidas y a su vez conduzcan a la administración para la revisión del SGSI

Formación, preparación y competencia: La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el SGSI sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria

Auditoría interna del SGSI: La organización realizará auditorías internas al SGSI a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

Administración de las revisiones del SGSI: Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para

mejorar o cambiar el SGSI incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, serán claramente documentados.

Mejoras al SGSI: La organización deberá mejorar continuamente la eficiencia del SGSI a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración.

Acciones Correctivas: La organización llevará a cabo acciones para eliminar las causas que no estén en conformidad con los requerimientos del SGSI con el objetivo de evitar la recurrencia de los mismos.

12. ANEXO V: GLOSARIO

Alineamiento: Un estado en el que los elementos del gobierno y la gestión de TI empresa contribuyen a las metas y las estrategias de la empresa.

BPM: Gestión de Procesos de Negocio (por sus siglas en inglés Business Process Management)

BSC: Cuadro de Mando Integral (Por sus siglas en inglés Balanced Scorecard)

Capacidad: Contar con los atributos necesarios para realizar o lograr.

CEO: Director Ejecutivo (por sus siglas en inglés Chief Executive Officer)

CFO: Director Financiero (por sus siglas en inglés Chief Finance Officer)

CIO: Director de Información (por sus siglas en inglés Chief Information Officer)

Framework: Ver Marco de Trabajo

GEIT: Gobierno de TI de la Empresa (Por sus siglas en inglés Governance of Enterprise IT)

Gobierno: El método o marco de trabajo por el cual una organización es dirigida, administrada y/o controlada

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o reducción de la calidad de dicho servicio.

ITIL: Librería de Infraestructura de TI de la oficina de Gobierno Gubernamental del Reino Unido (OGC). Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

KGI: Indicador Clave de Resultado (por sus siglas en inglés Key Goal Indicator)

KPI: Indicador Clave de Desempeño (por sus siglas en inglés Key Performance Indicator)

Marco de Trabajo (framework): Herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Matriz RACI: Matriz que ilustra quién es responsable, quién debe rendir cuenta(s), a quién se le debe consultar y quién se le debe informar dentro de un conjunto de prácticas de un proceso.

Métrica: Estándar para medir el desempeño de un objetivo.

PMO: Oficina de Gestión de Proyectos (Por sus siglas en inglés Project Management Office)

Política: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos de jefatura del área que la implementa. Además del contenido de la política, ésta debe describir las consecuencias de la falta de

cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Portafolio: Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.

Práctica: Acción principal tomada para operar el proceso de gobierno TI.

Procedimiento: Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se sigue en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos. Manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Riesgo: El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daños a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

Riesgos Residuales: Riesgos que existen después de haberse considerado la eficacia y eficiencia de los controles.

SLA: Acuerdo de Niveles de Servicio (Services Level Agreement por sus siglas en inglés).

TI: Tecnología de la Información.