



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE CIENCIAS DE LA
COMPUTACIÓN**

CARRERA INGENIERÍA EN SISTEMAS E INFORMÁTICA

**TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SISTEMAS E INFORMÁTICA**

**TEMA: ESTUDIO ANALÍTICO DE LA COMPATIBILIDAD
ENTRE LA NORMA ISO 38500 Y COBIT 5 REFERENTE A
GOBERNANZA DE TI**

AUTORA: JENNY CUMANDÁ RAZO TAPIA

DIRECTOR: ING. MARIO RON MSc.

CODIRECTOR: ING. MAURICIO CAMPAÑA MSc.

SANGOLQUÍ, MARZO 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICADO

Ing. Mario Ron MSc. (DIRECTOR DE TESIS)
Ing. Mauricio Campaña MSc. (CODIRECTOR DE TESIS)

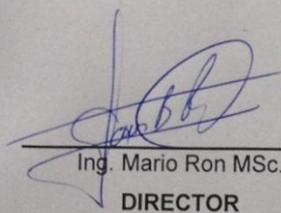
CERTIFICAN

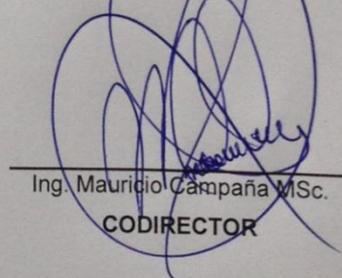
Que el trabajo titulado "ESTUDIO ANALÍTICO DE LA COMPATIBILIDAD ENTRE LA NORMA ISO 38500 Y COBIT 5 REFERENTE A GOBERNANZA DE TI", realizado en su totalidad por la Sra. Jenny Cumandá Razo Tapia ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento Estudiantes de la Universidad de las Fuerzas Armadas – ESPE.

Debido a que constituye un trabajo con excelente contenido científico, que coadyuvará a la aplicación de conocimientos y desarrollo profesional, se recomienda su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto al cual contiene los archivos en formato portátil de Acrobat (pdf). Se autoriza a la Sra. Jenny Cumandá Razo Tapia, que el material se entregue al Ing. Mauricio Campaña, en su calidad de Director de Carrera.

Sangolquí, Marzo del 2015.


Ing. Mario Ron MSc.
DIRECTOR


Ing. Mauricio Campaña MSc.
CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

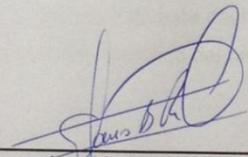
CERTIFICADO

Ing. Mario Ron MSc. (DIRECTOR DE TESIS)
Ing. Mauricio Campaña MSc. (CODIRECTOR DE TESIS)

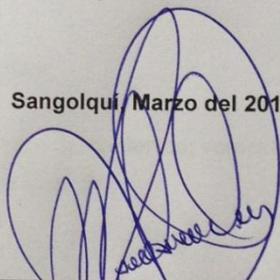
CERTIFICAN

Que el trabajo titulado "ESTUDIO ANALÍTICO DE LA COMPATIBILIDAD ENTRE LA NORMA ISO 38500 Y COBIT 5 REFERENTE A GOBERNANZA DE TI", fue realizado en su totalidad por la Sra. Jenny Cumandá Razo Tapia como requerimiento parcial a la obtención del título de Ingeniero en Sistemas e Informática.

Sangolquí, Marzo del 2015.



Ing. Mario Ron MSc.
DIRECTOR



Ing. Mauricio Campaña MSc.
CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DECLARACIÓN DE RESPONSABILIDAD

Jenny Cumandá Razo Tapia

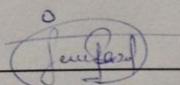
DECLARA QUE:

La presente tesis de grado titulada "ESTUDIO ANALÍTICO DE LA COMPATIBILIDAD ENTRE LA NORMA ISO 38500 Y COBIT 5 REFERENTE A GOBERNANZA DE TI", ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

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

Sangolquí, Marzo del 2015



Jenny Cumandá Razo Tapia

CC. 050187960-5

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

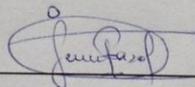
AUTORIZACIÓN DE PUBLICACIÓN

Jenny Cumandá Razo Tapia

AUTORIZA

A la UNIVERSIDAD DE LAS FUERZAS ARMADAS- ESPE la publicación en la Biblioteca Virtual de la Institución el trabajo "ESTUDIO ANALÍTICO DE LA COMPATIBILIDAD ENTRE LA NORMA ISO 38500 Y COBIT 5 REFERENTE A GOBERNANZA DE TI", cuyo contenido, ideas y criterio son de mi responsabilidad y autoría.

Sangolquí, Marzo del 2015



Jenny Cumandá Razo Tapia

CC. 0501879605

DEDICATORIA

A mi hija Jennifer que sin saberlo con toda su inocencia y ternura fue mi soporte, mi compañía y mi motivación; a mi esposo Ramiro por su apoyo incondicional, por su ejemplo, cariño y comprensión.

A mi madre Judith que ha sido durante toda mi vida mi ejemplo y el fuerte roble que siempre me brinda amor y apoyo. A mi familia por estar siempre dispuestos a brindarme su amor incondicional.

Jenny Cumandá Razo Tapia

AGRADECIMIENTOS

Agradezco a Dios que ha permitido que llegue a este momento, a mi hija Jennifer y mi esposo Ramiro que me acompañaron en el proceso del desarrollo del proyecto de culminación de mi carrera y me dieron fuerzas y ánimo.

Agradezco a mi madre Judith por su aporte con su infinito amor, paciencia y tiempo ha sabido ser mi compañera, mi amiga en mis tristezas y mis alegrías.

Agradezco a mi familia por haber creído siempre en mí, a todas y cada una de las personas que de una u otra manera ayudaron a la realización de este documento como a la finalización de mi carrera.

Agradezco de manera especial a mi Director de Tesis Ing. Mario Ron, a mi Codirector Ing. Mauricio Campaña por su apoyo, aporte, tiempo, conocimientos y paciencia que me brindaron durante todo este tiempo, mil gracias!

Mi agradecimiento para el Ing. Raúl Córdova auspiciante del tema de tesis, por su apoyo para que este proyecto haya culminado. Gracias.

Jenny Cumandá Razo Tapia

ÍNDICE DE CONTENIDO

CERTIFICADO	ii
CERTIFICADO	iii
DECLARACIÓN DE RESPONSABILIDAD	iv
AUTORIZACIÓN DE PUBLICACIÓN	v
DEDICATORIA	vi
AGRADECIMIENTOS	vii
ÍNDICE DE CONTENIDO	viii
ÍNDICE DE FIGURAS	xi
ÍNDICE DE TABLAS	xii
RESUMEN	xiii
ABSTRACT	xiv
CAPÍTULO 1	1
INTRODUCCIÓN	1
1.1. Planteamiento del Problema	1
1.2. Justificación	1
1.3. Objetivos.....	2
1.3.1. Objetivo General	2
1.3.2. Objetivos Específicos.....	2
1.4. Alcance	2
1.5. Metodología	2
1.6. Temario.....	3
1.7. Factibilidad.....	4
1.7.1. Factibilidad Operativa	4
1.7.2. Factibilidad Técnica	4
1.7.3. Factibilidad Económica	5
1.8. Cronograma.....	5

CAPÍTULO 2	6
MARCO TEÓRICO	6
2.1. Gobernanza de TI	6
2.1.1. Conceptos de Gobernanza de empresa, corporativa y de TI.....	7
2.1.2. Gobernanza de TI	9
2.1.3. Modelos de Gobernanza de TI	10
2.1.4. Principios para la gobernanza	13
2.2. ISO/IEC 38500:2008.....	15
2.2.1. Principios	16
2.2.2. Modelo	17
2.2.3. Relación principios/modelo ISO 38500.....	18
2.3. COBIT 5.....	19
2.3.1. Principios de COBIT.....	20
2.3.2. Dominios de COBIT	26
2.3.3. Distribución de los Dominios y Procesos de COBIT	26
2.4. Asignación de prioridades de medidas de prestaciones técnicas (Descripción de parámetros de prestaciones)	28
2.5. Matriz de Holmes o de prioridades.....	30
2.6. Principio de Pareto.....	33
CAPÍTULO 3	35
ESTUDIO ANALÍTICO ENTRE ISO 38500 Y COBIT 5	35
3.1. Descripción de parámetros de comparación	35
3.2. Selección de parámetros de comparación	47
3.3. Aplicación de parámetros.....	55
CAPÍTULO 4	56
RESULTADOS DEL ESTUDIO ANALÍTICO ENTRE ISO 38500 Y COBIT 5	56
4.1. Presentación de resultados.....	56
4.2. Discusión de resultados y análisis de compatibilidad	58
CAPÍTULO 5	69

CONCLUSIONES Y RECOMENDACIONES	x 69
5.1. Conclusiones	69
5.2. Recomendaciones	71
BIBLIOGRAFÍA	72

ÍNDICE DE FIGURAS

Figura 1.1 Cronograma propuesto.....	5
Figura 2.1 Gobernanza de TI, Gestión o administración de TI.....	9
Figura 2.2 Modelos de Gobernanza de TI	12
Figura 2.3 Modelo de Gobierno de TI propuesto por la norma ISO/IEC 38500.....	17
Figura 2.4 Principios COBIT.....	20
Figura 2.5 Cascada de objetivos COBIT 5	21
Figura 2.6 Componentes de un sistema de gobierno de TI según el modelo COBIT 5.....	22
Figura 2.7 Catalizadores de gobierno de TI según el modelo COBIT 5	23
Figura 2.8 Dimensiones comunes de los facilitadores de gobierno de TI según el modelo COBIT 5	25
Figura 2.9 Procesos de gobierno y gestión	26
Figura 2.10 Referencia de procesos y dominios según el modelo COBIT 5	27
Figura 3.1 Diagrama de Pareto para la selección de los parámetros.....	50
Figura 4.1 Integración COBIT e ISO 38500.....	61
Figura 4.2 COBIT, integración varias mejores prácticas.....	63
Figura 4.3 Procesos COBIT de gobierno de TI.....	64
Figura 4.4 Principios ISO 38500 y procesos COBIT	65
Figura 4.5 Trabajo conjunto entre ISO 38500 y COBIT	68

ÍNDICE DE TABLAS

Tabla 1.1 Costos desarrollo de proyecto.....	5
Tabla 2.1 Relación principios/modelo ISO 38500	18
Tabla 3.1 Matriz de Holmes parámetros de comparación	48
Tabla 3.2 Tabla principio de Pareto	49
Tabla 3.3 Resultados de principio de Pareto.	51
Tabla 3.4 Matriz de Holmes de parámetros seleccionados.....	52
Tabla 3.5 Tabla de métricas, rango y categorías.	54
Tabla 3.6 Resultados de aplicación de cada parámetro seleccionado a ISO 38500 y COBIT	55
Tabla 4.1 Resultados obtenidos	56

RESUMEN

Actualmente, abundan normas, marcos de trabajo, estándares, buenas prácticas referentes a la gobernanza de TI, las más reconocidas son el estándar ISO 38500 y el marco de trabajo COBIT 5. El presente artículo propone el análisis de la compatibilidad entre ISO 38500 y COBIT 5 respecto a la gobernanza de TI . El análisis se realizó adecuando los principios de Ingeniería de Software sobre TPM obteniendo un listado de parámetros o atributos deseables de una metodología para la gobernanza de TI, que fueron cuantificados y discriminados por su importancia respecto de la gobernanza de TI usando los conceptos de la matriz de Holmes y el principio de Pareto. Para cada parámetro se define una escala numérica de cumplimiento para establecer en qué medida ISO 38500 y COBIT 5 satisfacen dichos parámetros, éstos datos son cuantificados y multiplicados por un factor de ponderación obtenido usando los principios de métricas, para finalmente ser sumados y lograr un resultado global. Los resultados se enfocan en lo que ISO 38500 y COBIT 5 aportan a la gobernanza de TI y en la manera en que por ser compatibles pueden ser implementados en conjunto logrando el mejor “buen gobierno de TI”. El documento es una comparativa válida para los profesionales de TI que buscan gestionar a TI como un portafolio de negocios, integrando a TI con las estrategias del negocio y gestionando los riesgos e impactos estratégicos.

Palabras Clave:

- **GOBERNANZA DE TI**
- **ISO 38500**
- **COBIT 5**
- **ISO 38500 Y COBIT 5 JUNTOS.**

ABSTRACT

Currently, there are many standards, frameworks, best practices related to IT governance, the best known are the ISO 38500 standard and the COBIT 5 framework. This article proposes the analysis of the compatibility between ISO 38500 and COBIT 5 related to the IT governance. This analysis was performed by adapting the principles of software engineering on TPM obtaining a list of parameters or desirable attributes of a methodology for IT governance, which were quantified and discriminated against by their importance for the IT governance concepts using Holmes matrix and the Pareto principle. For each parameter a numerical scale of compliance was defined to establish the extent to which ISO 38500 and COBIT 5 fulfill these parameters, these data are quantified and multiplied with a weighting factor obtained using the principles of metrics, to be added and finally get a global result for each one. The results focus on what ISO 38500 and COBIT 5 contribute to the IT governance and how can be implemented in conjunction achieving the best "IT governance". The document is valid for IT professionals seeking to manage IT as a business portfolio, integrating IT with business strategies and managing risks and strategic impacts.

Keywords:

- **IT GOVERNANCE**
- **ISO 38500**
- **COBIT 5**
- **ISO 38500 AND COBIT 5 TOGETHER.**

CAPÍTULO 1

INTRODUCCIÓN

1.1. Planteamiento del Problema

En el escenario actual existe una abundancia de marcos, normas, guías y buenas prácticas que buscan establecer una buena gobernanza de TI, cada uno con un área limitada de aplicación, que se traslapan entre sí, pero en general no existe un marco global de gobernanza de TI que pueda usarse como referente estándar de aplicación. Tanto ISO/IEC 38500 como COBIT están basados en el mismo principio de gobernanza corporativa de TI, sin embargo ISO goza de más popularidad en el mundo corporativo, mientras COBIT está más orientado a la aplicación; para los líderes de TI, es cada vez más claro que ISO 38500 y COBIT pueden complementarse entre sí, si se aplica de la manera correcta.

1.2. Justificación

Esta investigación es relevante porque generará un conocimiento que podrá ser utilizado por los tomadores de decisión como referente para la gobernanza de tecnologías de la información.

Este problema de investigación podrá ser evaluada en varios niveles de la Organización y servirá de guía a los profesionales del sector de TI y a los líderes de las organizaciones como mecanismos de Gobernanza de TI. Se analizarán los beneficios y oportunidades de adoptar la Gobernanza como estrategia para alcanzar los objetivos y las metas, así también las desventajas económicas, técnicas e inclusive sociales de no hacerlo; a más de optimizar los niveles de riesgos y el uso de los recursos. La adopción de principios y la implementación del estándar ISO 38500 soportado por COBIT 5 facilitarán el uso y aplicación de las buenas prácticas.

1.3. Objetivos

1.3.1. Objetivo General

Realizar un estudio analítico de la compatibilidad de la norma ISO/IEC 38500 y COBIT 5 aplicado a la Gobernanza de TI.

1.3.2. Objetivos Específicos

- a. Describir la situación actual de la Gobernanza de TI
- b. Describir el estándar ISO 38500
- c. Describir el área de Gobernanza de TI de COBIT 5
- d. Definir los parámetros de integración entre ISO 38500 y COBIT 5
- e. Realizar el análisis comparativo de la compatibilidad entre ISO 38500 y COBIT 5
- f. Obtener los resultados del análisis comparativo

1.4. Alcance

En esta propuesta se realizará un estudio analítico de la compatibilidad de la norma ISO 38500 y COBIT 5 aplicado a la Gobernanza de TI.

1.5. Metodología

Para describir el estándar ISO 38500:2008, se usará la información disponible en distintos medios, también se utilizarán como referencia experiencias anteriores, y recursos de expertos en el tema que están publicados en internet.

De igual manera para la descripción del área de gobernanza de TI de COBIT, se usará la información disponible en libros o en medios electrónicos, también se busca apoyo en investigaciones realizadas sobre el tema, además de las experiencias recogidas de las personas líderes en el área de TI.

Para realizar el estudio analítico de compatibilidad entre de ISO 38500:2008 y COBIT, no existe un procedimiento definido, la investigación se centrará en elaborar un mecanismo que contemple los enfoques de ISO 38500 y COBIT y recoja los lineamientos de ambos y genere un comparativo.

1.6. Temario

CAPÍTULO 1. INTRODUCCIÓN

- 1.1 Planteamiento del Problema
- 1.2 Justificación
- 1.3 Objetivos
 - 1.3.1 Objetivo General
 - 1.3.2 Objetivos Específicos
- 1.4 Alcance
- 1.5 Metodología
- 1.6 Temario
- 1.7 Factibilidad
 - 1.7.1 Factibilidad Operativa
 - 1.7.2 Factibilidad Técnica
 - 1.7.3 Factibilidad Económica
- 1.8 Cronograma

CAPÍTULO 2. MARCO TEÓRICO

- 2.1 Gobernanza de TI
 - 2.1.1 Conceptos de Gobernanza de empresa, corporativa y de TI
 - 2.1.2 Gobernanza de TI
 - 2.1.3 Modelos de Gobernanza de TI
 - 2.1.4 Principios para la gobernanza
- 2.2 ISO/IEC 38500:2008
 - 2.2.1 Principios
 - 2.2.2 Modelo
 - 2.2.3 Relación principios/modelo ISO 38500
- 2.3 COBIT 5
 - 2.3.1 Principios de COBIT
 - 2.3.2 Dominios de COBIT
 - 2.3.3 Distribución de los dominios y procesos de COBIT
- 2.4 Asignación de prioridades de medidas de prestaciones técnicas (Descripción de parámetros de prestaciones)

2.5 Matriz de Holmes o de prioridades

2.6 Principio de Pareto

CAPÍTULO 3. ESTUDIO ANALÍTICO ENTRE ISO 38500 Y COBIT 5

3.1 Descripción de parámetros de comparación

3.2 Selección de parámetros de Comparación

3.3 Aplicación de Parámetros

CAPÍTULO 4. RESULTADOS DEL ESTUDIO ANALÍTICO ENTRE ISO 38500 Y COBIT 5

4.1 Presentación de resultados

4.2 Discusión de resultados y análisis de compatibilidad

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

5.2 Recomendaciones

BIBLIOGRAFÍA

1.7. Factibilidad

1.7.1. Factibilidad Operativa

Para el desarrollo de la presente propuesta se cuenta con los recursos informativos y bibliográficos necesarios para su desarrollo. También se tiene acceso a un conjunto de profesionales líderes con gran experiencia en gobernanza de TI.

1.7.2. Factibilidad Técnica

La Tecnología de la información se ha convertido en el recurso que hace posible importantes cambios en las organizaciones, y su uso inteligente y apropiado ha ocasionado una profunda transformación dentro y fuera de ellas llegando a influir inclusive en los mercados, de manera que la información se ha convertido en un activo cada vez más valorado, razón por

la cual hoy las organizaciones invierten para implementar una buena gobernanza y gestión de TI, mediante el uso de las mejores prácticas.

Los estándares, marcos y modelos existentes no siempre encajan el uno con el otro. Cada uno de ellos fue creado por personas u organizaciones diferentes, en distintos momentos, en lugares distintos y con propósitos distintos. Por ello, es de primordial importancia el saber elegir las mejores prácticas, procesos y estrategias entre todos estos modelos y poder generar a partir de ellas un modelo personalizado y adaptado totalmente para un tipo de organización en particular (Coello, 2008).

1.7.3. Factibilidad Económica

Los costos para la realización del presente trabajo de tesis serán cubiertos en su totalidad por la autora. La tabla 1 muestra el detalle.

Tabla 1.1
Costos desarrollo de proyecto

No.	Descripción	Valor Unitario	Total
1	Computador	\$1000,00	\$1000,00
1	Impresora a color	\$200,00	\$200,00
	Suministros de Oficina	\$300,00	\$300,00
	TOTAL		\$1500,00

1.8. Cronograma

El cronograma propuesto se muestra en la Figura 1.1.



Figura 1.1 Cronograma propuesto

CAPÍTULO 2

MARCO TEÓRICO

2.1. Gobernanza de TI

El término “gobernanza” es una traducción del término “governance” y tiene varias significaciones de acuerdo al área al que se refiera, en este caso, en términos empresariales se define como “El conjunto de procesos, costumbres, políticas, leyes e instituciones que afectan a cómo se dirige, administra o controla una empresa (corporación) (Wikipedia, Gobernanza).

También incluye las relaciones entre los muchos agentes implicados en ellas (desde la propiedad a la dirección, los controladores externos, acreedores, inversores, clientes, suministradores, empleados y el entorno y la sociedad entera)”. (Wikipedia, Gobernanza)

Gobernanza también se suele confundir con Gobernabilidad traducción literal de “governability”, que se define como “la situación en la que concurren un conjunto de condiciones favorables para la acción de gobierno, que se sitúan en su contorno o son intrínsecas a éste. Este concepto se enmarca en el ámbito de "la capacidad de gobierno". Éste se da siempre en un ámbito social tal en el que se registran demandas de los ciudadanos que son procesadas en menor o mayor medida por el sistema político (Wikipedia, Gobernabilidad).

También se confunde con el término “Gobierno” que en el ámbito empresarial su traducción es “Corporate Governance” y se define como “Los mecanismos, procesos y relaciones mediante el cual las empresas están controladas y dirigidas.

Las estructuras de gobierno a identificar la distribución de derechos y responsabilidades entre los diferentes participantes en la corporación (como la junta de directores, gerentes, accionistas, acreedores, auditores,

reguladores y otras partes interesadas) e incluye las normas y procedimientos para la toma de decisiones en los asuntos corporativos.” (Wikipedia, Corporate Governance).

“Lo importante es destacar que el gobierno corporativo no es un instrumento individual sino más bien un concepto que incluye el debate sobre las estructuras apropiadas de gestión y control de las empresas. También incluye las reglas que regulan las relaciones de poder entre los propietarios, el consejo de administración, la administración y, por último, pero no por ello menos importante, partes interesadas tales como los empleados, los proveedores, los clientes y el público en general” (Wikipedia, Gobierno Corporativo).

Si bien estos conceptos provienen de términos anglosajones y diferenciarlos implica un gran debate, siguiendo las definiciones enunciadas y en apego al tema del presente trabajo, se toma el término de gobernanza al conjunto de normas, marcos de trabajo, regulaciones, mejores prácticas que controlan el cómo se dirige, administra y controla una empresa. Gobierno implicaría el marco, norma, buena práctica específica seleccionada para formar parte de la gobernanza.

2.1.1. Conceptos de Gobernanza de empresa, corporativa y de TI

Gobernanza de TI se define como “Es una disciplina subconjunto de la gobernanza corporativa, centrada en Tecnología e Información (TI) y su gestión del rendimiento y riesgo. El interés en la gobernanza de TI se debe a la necesidad permanente dentro de las organizaciones para enfocar los esfuerzos de creación de valor en los objetivos estratégicos de la organización y para gestionar mejor el rendimiento de los responsables de la creación de este valor en el mejor interés de todas las partes interesadas” (Wikipedia, Corporate Governance of Information Technology).

Gartner define la gobernanza de TI como “Los procesos que garanticen el uso efectivo y eficiente de las TI para permitir que una organización logre sus objetivos” (Gartner).

Gobernanza de empresa es una traducción de “Enterprise Governance” y es más amplio que Gobernanza Corporativa (“Corporate Governance”), y se refiere no sólo a las empresas sino a otro tipo de organizaciones como agencias gubernamentales. Describe un marco de trabajo que cubre la gobernanza corporativa y la gobernanza de negocio (“Business Governance”).

La Gobernanza corporativa enfocada al aseguramiento de rendición de cuentas, y la gobernanza de negocio enfocada a la utilización de recursos para la creación de valor.

La gobernanza corporativa es el sistema por el cual las organizaciones son dirigidas y controladas. La dependencia de la empresa por la tecnología de la información se traduce en el hecho de que todas las cuestiones de gobernanza corporativa no pueden ser resueltas sin tener en cuenta a TI, y la gobernanza de negocio debe permitir y controlar las inversiones para TI.

La gobernanza corporativa conduce a la gobernanza de TI y a su vez, TI influye en las oportunidades estratégicas y puede proporcionar información crítica para los planes estratégicos, de esta manera la gobernanza de TI facilita a la empresa a tomar ventaja de su información, y puede ser considerado como un conductor para la gobernanza corporativa.

Por la estrecha relación entre gobernanza corporativa y gobernanza de TI, no pueden ser consideradas puramente distintas, y la gobernanza de TI debe ser integrada como parte de la gobernanza corporativa.

2.1.2. Gobernanza de TI

Dadas las definiciones anteriores sobre Gobernanza de TI, un tema importante y que queda en duda es el vínculo de TI con los objetivos presentes y futuros de la empresa. Esta diferenciación se visualiza en la figura 2.1.

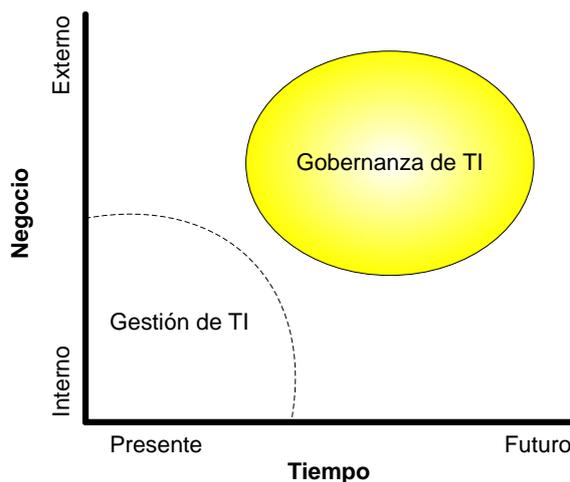


Figura 2.1 Gobernanza de TI, Gestión o administración de TI
Fuente: (ServiceXen, 2008)

La gestión o administración de TI (IT management) se enfoca en la provisión efectiva y eficiente de los servicios y productos de TI y la gestión de las operaciones de TI actuales (ServiceXen, 2008).

La gobernanza de TI es mucho más amplia y se centra en la transformación de los recursos de TI para satisfacer las demandas actuales y futuras de la empresa (enfoque interno) y los clientes del negocio (enfoque externo).

Sin hacer de menos a la importancia y complejidad de la gestión de TI (IT management), pero mientras que los elementos de la gestión de TI pueden ser tercerizados a algún proveedor, la gobernanza de TI es específica para la empresa, y la dirección y control no pueden ser delegados.

Los 3 objetivos de la gobernanza de TI son:

1. Asegurar que el uso de las tecnologías de la información generan valor para el negocio,
2. Supervisar el desempeño de la administración y
3. Mitigar los riesgos asociados con el uso de las tecnologías de la información.

Esto se logra a través del compromiso de la alta dirección, la implementación de una estructura organizacional con la rendición de cuentas bien definido para decisiones que incidan en el la consecución de los objetivos estratégicos e institucionalizar las buenas prácticas mediante la organización de actividades en procesos con salidas claramente definidas que vayan vinculadas a los objetivos estratégicos de la empresa.

La gobernanza de TI se podría traducir como el mejor “buen gobierno de TI”, y muchos autores de la definición coinciden en que se logra integrando estándares, marcos de trabajo, buenas prácticas de TI, así, la gobernanza de TI al ser una colección de las mejores prácticas, da un enfoque vigoroso de prácticas a seguir y base de certificación en esquemas de negocio de mejoramiento continuo en el uso y aprovechamiento de las TI en apoyo al logro de los objetivos del negocio (Wikipedia, Gestión de servicios de Tecnologías de la Información).

2.1.3. Modelos de Gobernanza de TI

Para lograr una buena gobernanza de TI, se debe apoyar en normas, marcos, estándares para garantizar que TI soporte los objetivos de negocio de la organización.

La gobernanza de TI al ser parte del gobierno corporativo, debe tener una estructura, procesos, roles y tecnología, todos estos recursos deben ser implementados a nivel estratégico (Consejo de Administración), táctico (Nivel

ejecutivo) y operativo (Gerentes de negocio, área de TI). La combinación específica de estos modelos se denomina modelo de Gobernanza de TI.

Según el ITGI (IT Governance Institute), las empresas no pueden hacer entrega efectiva de lo que demandan los requerimientos del negocio sin adoptar e implementar un marco de gobernanza de TI con los siguientes propósitos:

1. Enlazarse con los requerimientos del negocio
2. Hacer que el desempeño sea transparente a la luz de estos requerimientos
3. Organizar las actividades de TI dentro de un modelo de procesos generalmente aceptado
4. Identificar los principales recursos a controlar
5. Definir los objetivos de control de la administración a ser considerados

Por estas razones se encuentran referentes de gobernanza de TI que fueron diseñados para orientar la implementación de los distintos aspectos de gobierno de TI los cuales se complementan con los estándares y las mejores prácticas de gestión de TI.

Los modelos de gobernanza de TI que son mencionados en relación a gobernanza de TI son COBIT e ISO 38500, otro menos conocido es Calder-Moir. Cada uno de ellos por su propia naturaleza se centran en el nivel táctico y estratégico, y al momento de su aplicación, no todas las partes de los marcos pueden ser aplicables a todas las empresas, cada uno tiene partes comunes con los otros modelos y cada uno tiene ventajas y desventajas. La mejor manera de llevar a la práctica la gobernanza de TI puede ser la de tomar lo que se necesita de cada marco y adaptarla a las necesidades. La figura 2.2 muestra varios modelos aplicables de acuerdo al nivel de gestión.

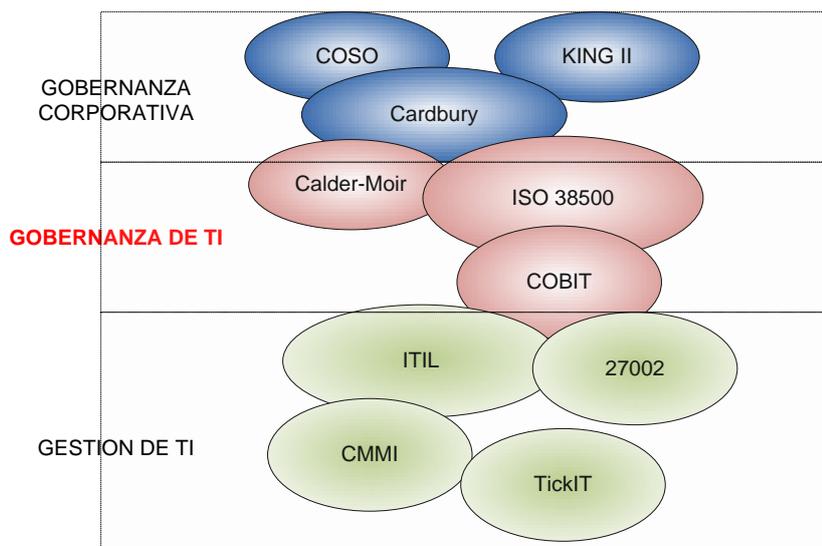


Figura 2.2 Modelos de Gobernanza de TI

La primera norma internacional que aborda el concepto de Gobernanza de TI es ISO/IEC 38500, que busca asesorar a quienes tienen las responsabilidades sobre el correcto funcionamiento de las organizaciones, en relación al papel que deben jugar respecto de las TI, definiendo, detallando los principios generales de gobernanza de TI: responsabilidad, estrategia, inversión, conformidad, rendimiento y comportamiento.

COBIT en su versión 5 es un marco de trabajo desarrollado a mediados de los 90 por ISACA, una organización independiente de profesionales interesados en la gobernanza y en gobierno de TI, inicialmente enfocado en reducir los riesgos técnicos en las organizaciones, en la versión 5 incluyó al alineamiento de TI con las metas estratégicas del negocio, es el marco de trabajo más ampliamente usado.

Calder-Moir es un meta-modelo para coordinar y organizar marcos de trabajo de gobernanza de TI, co escrito por Alan Calder, director de IT Governance (www.itgovernanceusa.com), está diseñado para maximizar el beneficio de varias normas, marcos, metodologías, marcos de trabajo integrados y superpuestos:

- COBIT
- ITIL
- ISO27001 / ISO27002
- ISO20000
- PRINCE2
- PMBOK
- TOGAF
- TI Cuadros de Mando
- Zachman Arquitectura Empresarial
- Gestión del Portafolio de TI

El objetivo del marco de trabajo Calder-Moir es actuar como ayuda para los profesionales relacionados con la gobernanza de TI y proporcionar un marco común cuando se trata de los problemas de TI en un alto nivel.

2.1.4. Principios para la gobernanza

Los principios de la gobernanza de TI son objetivos a largo plazo del uso de las TI, y deben responder al alineamiento de TI a los objetivos empresariales:

- a. ¿Cuál es el modelo operativo de la empresa?
- b. ¿Cómo contribuye la arquitectura de TI a dicho modelo operativo?
- c. ¿Cómo se financian las inversiones de TI?

Los principios deben intentar ser escalables a perfiles de empresas de diferentes tamaños, ámbitos, complejidades y riesgos y son consistentes con los principios de gobernanza de TI definidos por el ITGI:

- 1. Alineamiento estratégico:** Asegura que las iniciativas y estándares de TI apuntalan la estrategia y los objetivos de la empresa, esto implica:
 - Obtener apoyo de la dirección ejecutiva
 - Comprensión clara de las necesidades de la empresa
 - El desarrollo de la estrategia y los objetivos de TI

2. Entrega de valor: Asegura que se obtiene un valor a partir de la inversión en TI mediante la selección de las inversiones con prudencia y la gestión de los mismos a lo largo de su ciclo de vida. La entrega de valor eficaz asegura que las iniciativas de TI se completan a tiempo, dentro del presupuesto y cumpliendo las expectativas, esto implica:

- Identificación de los objetivos y recursos necesarios del portafolio de proyectos de la empresa
- Identificación de la prestación de servicios y metas
- Supervisar la gestión de proyectos y metas de entrega
- Facilitar la comunicación del valor de TI

3. Gestión de riesgos: Garantiza la salvaguarda de los activos de TI, recuperación de desastres y la continuidad de las operaciones, incluyendo la seguridad e integridad de la información (ITGI, 2008), esto implica:

- Configuración de la propensión al riesgo institucional, en relación con TI
- La determinación de las estrategias de gestión de riesgos de seguridad de la información y de TI
- Monitoreo de la aplicación de las estrategias de gestión de riesgos de TI
- Entendimiento cumplimiento y mandatos regulatorios
- Garantizar que la información se gestiona a través de prácticas eficaces de control de calidad
- Colaborar con las funciones y supervisores de auditoría de TI

4. Manejo de recursos: Asegura la optimización del uso y asignación de los recursos de TI, el cómo se gestiona y ofrece los recursos TI críticos, esto implica:

- Supervisar la asignación de recursos
- La gestión de los activos de hardware y software

- El mantenimiento de terceros proveedores de servicios y acuerdos de outsourcing
- Hacer cumplir las normas de arquitectura estandarizada

5. Gestión del rendimiento: Examina cómo el personal de TI supervisar la implementación de la estrategia de TI, cómo se determina el éxito de los proyectos, y si se ha mantenido un alto nivel de prestación de servicios, esto implica:

- Asegurar la satisfacción del cliente
- El mantenimiento de los niveles de servicio esperados
- Medir el valor del negocio en la prestación de servicios
- Fomentar iniciativas de mejora de procesos de TI

2.2.ISO/IEC 38500:2008

ISO/IEC 38500:2008 (Corporate governance of information technology) fue publicada en junio de 2008, es un estándar internacional para la gobernanza corporativa de las Tecnologías de la Información, fue publicada por la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission) tiene su antecesora en el estándar ISO 29382, que a su vez evolucionó a partir de la norma australiana AS8015:2005.

ISO 38500 proporciona un marco para la gobernanza efectiva de TI para ayudar a los que están en el más alto nivel de las organizaciones a entender y cumplir con sus obligaciones legales, regulatorios y éticos en relación con el uso de TI de sus organizaciones (Wikipedia, ISO/IEC 38500)

Para las empresas es un reto la optimización de la inversión de recursos en TI, y lograr que las decisiones de adquisiciones, tomadas se orienten a las estrategias, objetivos, prioridades y necesidades del negocio, tanto presentes como en el futuro, los directivos de la empresa debe asegurar el funcionamiento y control de los sistemas, y disponer de un plan para seguir

funcionando a futuro, y para soportar integraciones de nuevas tecnologías. ISO 38500 se aplica a entidades de todos los tamaños, sean públicas o privadas, entidades de gobierno, sin fines de lucro.

El objetivo de ISO 38500 es el uso de las tecnologías de la información de manera efectiva, óptima y eficiente en las organizaciones, con la finalidad de:

- a. Generar confianza en los stakeholders (empleados, clientes, proveedores, socios, accionistas, etc.) en el Gobierno Corporativo de TI en la Organización
- b. Informar y guiar al nivel directivo sobre gobernanza de TI en su organización
- c. Proveer de bases para la evaluación objetiva del Gobierno Corporativo de TI

2.2.1. Principios

ISO 38500 establece los siguientes principios para lograr un buen gobierno corporativo de TI:

- 1. Responsabilidad:** Todos deben aceptar y comprender sus responsabilidades sobre la demanda y oferta de TI.
- 2. Estrategia:** Las estrategias de la empresa toma en cuenta las posibilidades de desarrollo de TI. TI cumple con las expectativas del negocio tanto a corto plazo como a largo plazo
- 3. Inversión:** Las adquisiciones de TI se hacen en base a un análisis apropiado, y es claro y transparente, se logran buenos beneficios, oportunidades, costos y riesgos.
- 4. Rendimiento (Rendición de resultados):** Garantía de unas TI que funcionen bien y cuando son requeridas.

5. **Cumplimiento:** Garantía de unas TI que cumplen (y ayudan a cumplir) con la legislación y normas establecidas, las políticas están definidas, debidamente implementadas y exigidas.
6. **Comportamiento (Recursos humanos):** Las políticas garantizan el respeto a los factores humanos.

2.2.2. Modelo

El modelo de gobernanza de ISO 38500 debe realizar tres tareas sobre cada uno de los principios descritos:

- a. Evaluar el uso actual y futuro de las TI, se incluyen las estrategias, propuestas y procedimientos para lograr y mantener las ventajas competitivas
- b. Dirigir los planes y políticas para asegurar que el uso de las TI estén alineadas a los objetivos del negocio
- c. Monitorizar en rendimiento de las TI usando métricas adecuadas.

La figura 2.3 muestra el modelo de gobernanza de TI en el ciclo evaluar, dirigir, monitorizar.

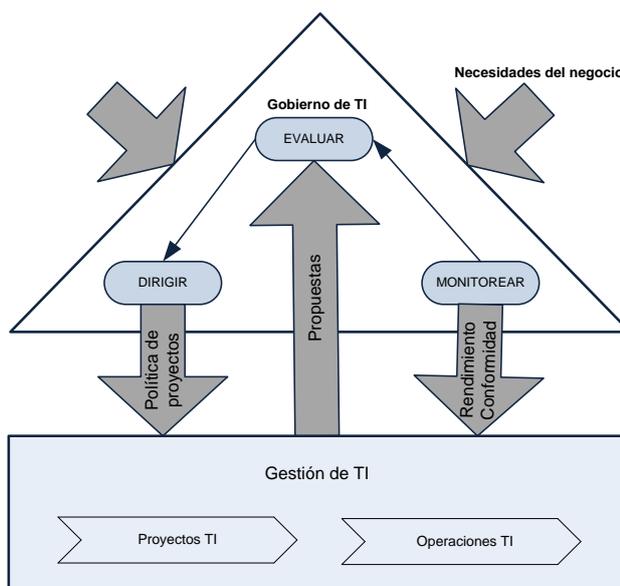


Figura 2.3 Modelo de Gobierno de TI propuesto por la norma ISO/IEC 38500
Fuente: ISO/IEC 38500

La dirección ejecutiva de la empresa, debe evaluar el uso de las TI por la organización frente a las presiones y necesidades del negocio existentes en el entorno, detectando amenazas existentes y debe desarrollar los planes necesarios para mitigar las amenazas identificadas.

La dirección de TI debe ejecutar dichos planes y dar seguimiento a los resultados y nuevamente tomar las acciones necesarias para asegurar los beneficios asociados.

2.2.3. Relación principios/modelo ISO 38500

La tabla 2.1 muestra las actividades (Evaluar, Dirigir y Monitorear) para cada principio de ISO 38500.

Tabla 2.1

Relación principios/modelo ISO 38500

Principios	Dirigir	Monitorizar	Evaluar
Responsabilidad	<ul style="list-style-type: none"> - Planes con Responsabilidad Asignada - Recibir información y rendir cuentas 	<ul style="list-style-type: none"> - Mecanismos establecidos Gobierno TI - Asignación Responsabilidades (entendimiento) - Desempeño responsables Gobierno de TI 	<ul style="list-style-type: none"> - Asignación Responsabilidades - Competencias responsables
Estrategia	<ul style="list-style-type: none"> - Creación y uso de planes y políticas - Asegurarse beneficios TI en el negocio - Alentar propuestas innovadoras 	<ul style="list-style-type: none"> - Supervisar el progreso de las propuestas aprobadas - Alcanzar objetivos en plazos establecidos - Utilizar recursos asignados - Uso de TI, alcanzando beneficios esperados 	<ul style="list-style-type: none"> - Evaluar el progreso propuestas aprobadas - Evaluar actividades TI y alineamiento - Mejores practicas - Satisfacción interesados - Valoración y evaluación de Riesgos
Adquisición	<ul style="list-style-type: none"> - Activos de TI se adquieren de manera apropiada - Documentos Capacidad Requerida - Acuerdos de Suministro respalden necesidades negocio 	<ul style="list-style-type: none"> - Inversiones y capacidades requeridas - Entendimiento Interno/Externo necesidades Negocio 	<ul style="list-style-type: none"> - Alternativas propuestas - Propuestas aprobadas - Análisis de riesgo / valor - Inversiones
Rendimiento	<ul style="list-style-type: none"> - Asignación Recursos Suficientes - Asignar prioridades y Restricciones - Satisfacer Necesidades de Negocio - Datos correctos, actualizados, protegidos 	<ul style="list-style-type: none"> - Grado TI Sustenta Negocio - Recursos e Inversiones Priorizados Necesidades Negocio - Política Precisión Datos (fiabilidad, exactitud e Integridad) - Política uso eficiente TI 	<ul style="list-style-type: none"> - TI sustenta procesos de negocio. Dimensionado y Capacidad - Riesgos: continuidad operaciones - Riesgos: integridad información, protección activos - Decisiones uso TI. Apoyo al negocio - Eficacia y desempeño Gobierno TI
Cumplimiento	<ul style="list-style-type: none"> - TI cumple obligaciones, normas y directrices - Establecer y aplicar políticas (uso TI interno) - Personal TI cumple directrices, desarrollo y conducta - Ética rige acciones relacionadas TI 	<ul style="list-style-type: none"> - Cumplimiento y Conformidad (Auditorías/Informes) - Oportunos, Completo, Adecuados (Necesidades Negocio) - Actividades TI 	<ul style="list-style-type: none"> - TI cumple Obligaciones, Normas y Directrices - Conformidad Gobierno TI
Factor Humano	<ul style="list-style-type: none"> - Actividades TI compatibles con Factor Humano - Informar por cualquier individuo (riesgos, problemas) - Administración riesgos según políticas y procedimientos - Escalado a los decisores 	<ul style="list-style-type: none"> - Identificar, prestar atención a las actividades TI - Practicas de trabajo son consistentes con el uso apropiado de TI 	<ul style="list-style-type: none"> - Se identifican actividades TI, que aseguran que los RRHH están identificados y considerados adecuadamente.

Fuente: (IEDGE - The European Business School, 2011)

2.3. COBIT 5

COBIT 5 (Control Objectives for Information and related Technology) fue lanzada en abril del 2012, es un marco de trabajo reconocido a nivel mundial, desarrollado por ISACA (Information Systems Audit and Control Association, actualmente mantenida por ITGI) busca ayudar a las organizaciones a cumplir los retos empresariales en las áreas de cumplimiento normativo, gestión de riesgos y alinear la estrategia de TI con los objetivos empresariales (Gobernanza de TI), integra los mecanismos de control de COBIT 4.1, los estándares para la gestión de riesgos de Risk IT, las inversiones Val IT, la gestión de servicios de ITIL (Information Technology Infrastructure Library) y la norma de gobernanza de TI ISO 38500, además de otros esquemas proporcionados por ITGI.

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para uso del día a día de los gestores de negocios (también directivos) y auditores". Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información (Wikipedia, Objetivos de control para la información y tecnologías relacionadas).

Una de las características de COBIT es su orientación al negocio, vinculando los objetivos del negocio con los objetivos de TI, y para medir los avances utiliza métricas y modelos de madurez, para esto asocia propietarios a los procesos del negocio y de TI.

Es enfocado a procesos, usando un modelo que subdivide TI en 37 procesos, en 4 áreas de responsabilidad, que siguen el ciclo de Deming (Plan (Planear), Do (Hacer), Check (Verificar), Act (Actuar)). La orientación

de COBIT hacia el negocio y hacia TI, el enlace que logra entre ambos, definiendo un lenguaje común que permite entender el valor estratégico de TI, y a los responsables de TI lo importante de aportar un valor al negocio, ha hecho de COBIT tenga el éxito del que goza.

COBIT 5 busca mantener un equilibrio entre los beneficios del uso de las TI, el uso de los recursos y el riesgo asociado al uso de las TI. Permite que TI sea gobernada y administrada o gestionada de manera integral, abarcando todas las áreas funcionales, tomando en cuenta los intereses de los stakeholders tanto internos como externos. Cuenta con 5 principios y 5 facilitadores genéricos aplicables a empresas comerciales o sin fines de lucro, de cualquier tamaño y para el sector público.

2.3.1. Principios de COBIT

Los principios son acciones que las empresas pueden realizar para gobernar y administrar efectivamente las TI. Entender y aplicar los 5 principios ayudan a las empresas a hacer mejores inversiones, tomar mejores decisiones de TI, y generar más valor a partir de la información y de sus activos tecnológicos. La figura 2.4 muestra los 5 principios COBIT:

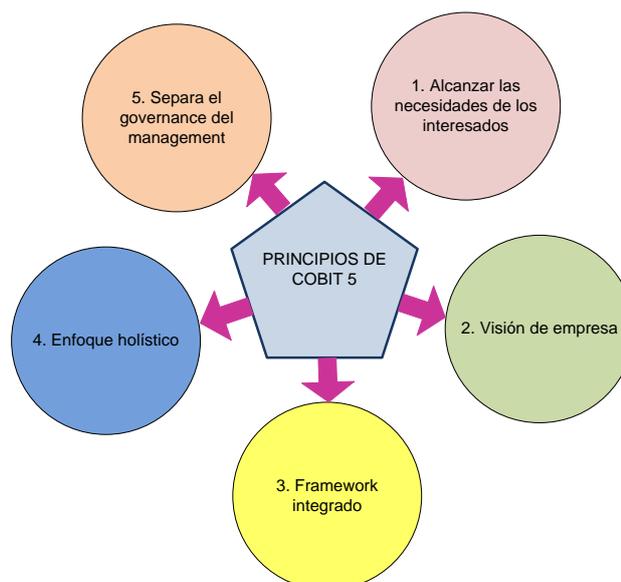


Figura 2.4 Principios COBIT
Fuente: (ISACA, 2012)

1. Alcanzar las necesidades de los stakeholders

Generar confianza en los stakeholders, y garantizar el ROI (Return of Investment) de la inversión en TI, y de su uso. COBIT es flexible, configurable proporciona las estructuras y herramientas que los ejecutivos requieren para dar valor al negocio. Ayuda a los ejecutivos a obtener más ventajas de los sistemas de información con un enfoque simplificado e integral para governance y management.

COBIT usa la herramienta “cascada de objetivos” para traducir los objetivos estratégicos en acciones concretas, la figura 2.5 grafica esta herramienta.

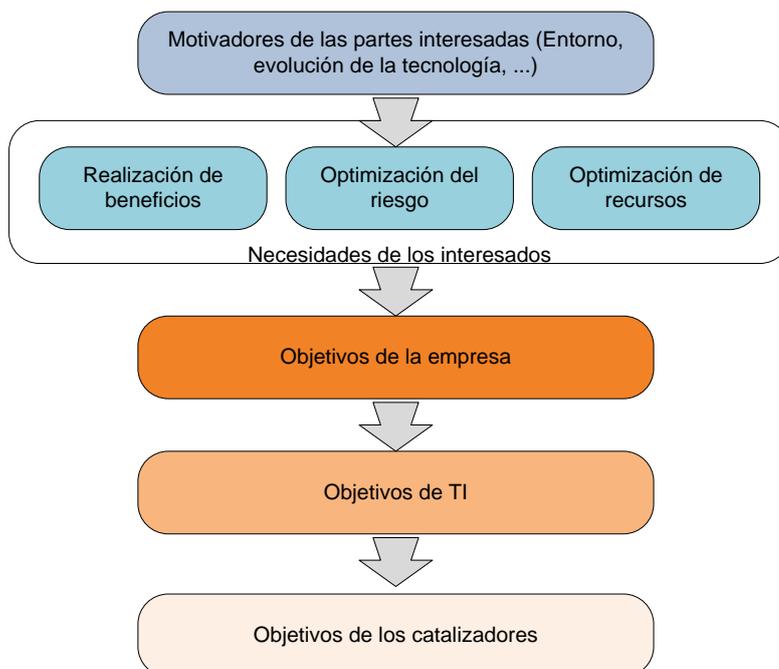


Figura 2.5 Cascada de objetivos COBIT 5
Fuente: (ISACA, 2012)

2. Visión de empresa

La parte de gobernanza ayuda a los ejecutivos a convertir los objetivos estratégicos en metas de TI, concretas, medibles y relevantes. COBIT entiende la empresa de extremo a extremo respecto a TI, provee <lineamientos para tomar las mejores decisiones enfocadas en los proyectos críticos.

Consta de 3 componentes principales del gobierno de TI:

1. Los facilitadores de gobierno de TI,
2. El alcance y los roles y
3. Las actividades y las relaciones.

La figura 2.6 muestra los componentes clave del sistema de gobierno.

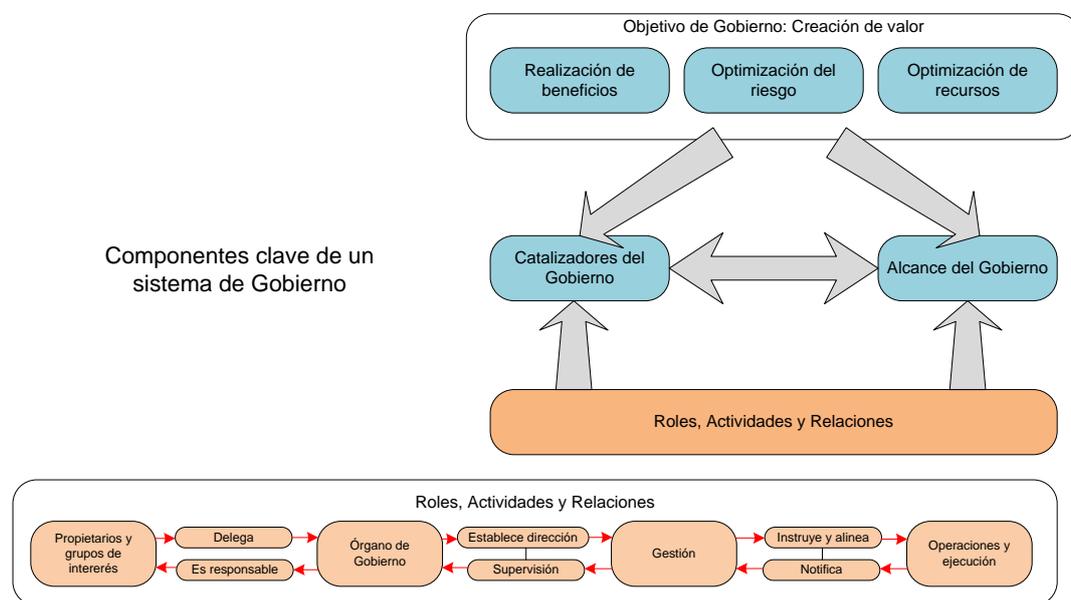


Figura 2.6 Componentes de un sistema de gobierno de TI según el modelo COBIT 5
Fuente: (ISACA, 2012)

Los **facilitadores** de gobierno de TI son los recursos de la organización tales como marcos, principios, estructuras, procesos y las mejores prácticas, mediante los cuales se dirige la acción y se logran los objetivos.

El **Ámbito** de aplicación del gobierno de TI (alcance) indica el nivel de aplicabilidad: toda la empresa, un área, un activo tangible o intangible, etc., es decir, es posible definir los diferentes puntos de vista de la empresa a la que la gobernanza se aplica (ISACA, 2012).

Los roles, actividades y relaciones, definen quién participa en el gobierno de TI, la forma en que son involucrados, lo que hacen y cómo interactúan.

3. Framework integrado

Existen muchos estándares, normas, marcos de trabajo, buenas prácticas relacionadas con TI, cada uno enfocado en un subconjunto de procesos o actividades de TI. COBIT se alinea con otros estándares, normas, marcos, y sirve de marco general para la gobernanza y gestión de TI. Está relacionado con:

1. Nivel Corporativo: ISO 9001, ISO 38500, COSO
2. Nivel TI: ITIL, ISO 31000, ISO 27000, ISO 22301, PMI PMBOK, CMMI, PRINCE 2

4. Enfoque Holístico

Los catalizadores de procesos son factores que individual o colectivamente influyen para que algo funcione, en este caso el gobierno y la gestión de TI. Son impulsados por la cascada de objetivos para garantizar que éstos se puedan cumplir. La figura 2.7 muestra los 7 catalizadores.

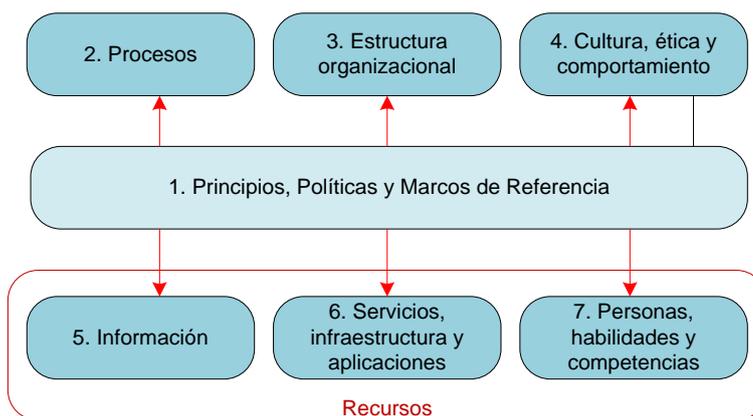


Figura 2.7 Catalizadores de gobierno de TI según el modelo COBIT 5
Fuente: (ISACA, 2012)

1. **Los Procesos** traducen los objetivos de la organización en actividades que reciben insumos de entrada, lo transforman y producen una salida.

2. **Las Estructuras Organizativas** es la estructuración de la organización, donde debe estar claramente definido cuáles niveles toman decisiones.
3. **La Cultura, Ética y Comportamiento** implica la actitud, los principios y la conducta individual y colectiva de las personas dentro de la empresa.
4. **Los Principios, Políticas y Marcos de Referencia** se encarga de traducir las directrices generales de la empresa en normativa a aplicarse a todo nivel. Los principios deben ser pocos, sencillos y claros. Las políticas se derivan de los principios y son más detallados.
5. **La Información** es el activo que produce o requiere la empresa, y gestionarla una actividad crítica.
6. **Los Servicios, Infraestructuras y Aplicaciones** se refiere a las directrices para el uso de los recursos relacionados con TI.
7. **Las Personas, Habilidades y Competencias** está relacionado con las aptitudes y conocimientos que debe tener las personas para cumplir con sus cargos, y la definición de las habilidades conocimientos que debe cumplir la persona que ocupa cierto cargo.

Para alcanzar los objetivos estratégicos, se debe considerar un conjunto interconectado de catalizadores, quiere decir que requiere del input de otro(s) catalizador(es) para lograr ser efectivo, y entrega un output a otro(s) catalizador(es).

Todos los catalizadores tienen un conjunto común de dimensiones, la figura 2.8 muestra las dimensiones comunes de gobierno de TI.

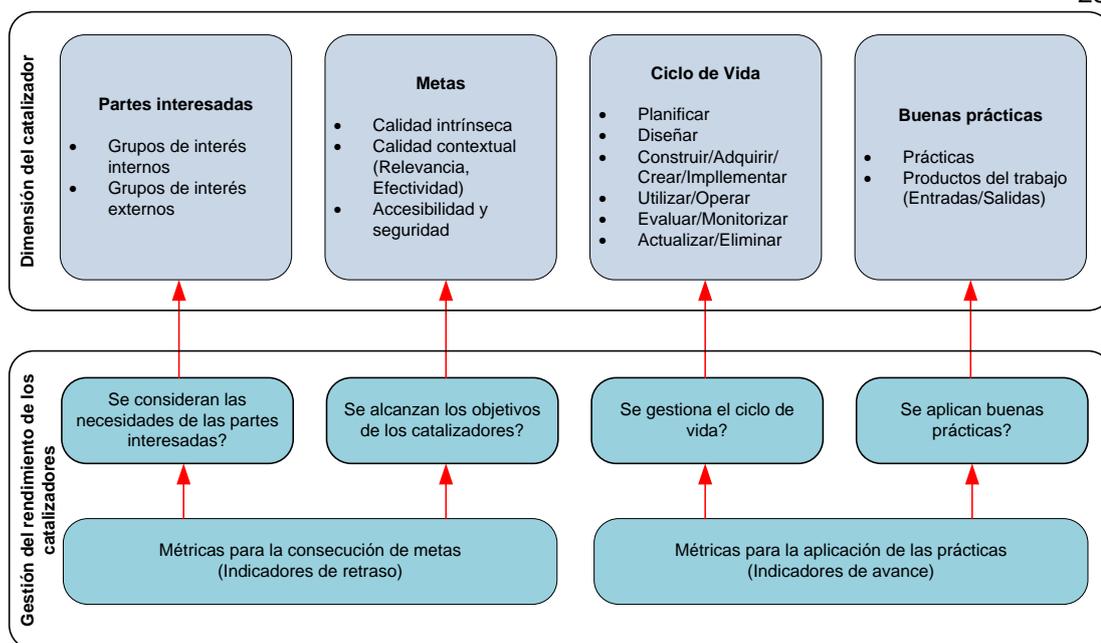


Figura 2.8 Dimensiones comunes de los facilitadores de gobierno de TI según el modelo COBIT 5
Fuente: (ISACA, 2012)

5. Separa el governance del management

Los términos gobernanza y gestión implican diferentes actividades, requieren de diferentes estructuras organizacionales, y tienen propósitos específicos. COBIT hace una clara diferenciación entre governance y management, provee las herramientas para simplificar los aspectos complejos y desarrollar buenas prácticas acordes a la realidad de la empresa.

Para COBIT, el gobierno es responsabilidad del Consejo de Dirección, en tanto que la gestión es responsabilidad de los ejecutivos de mandos medios.

La figura 2.9 muestra los procesos de gobierno y de gestión de manera que cubren las áreas clave.

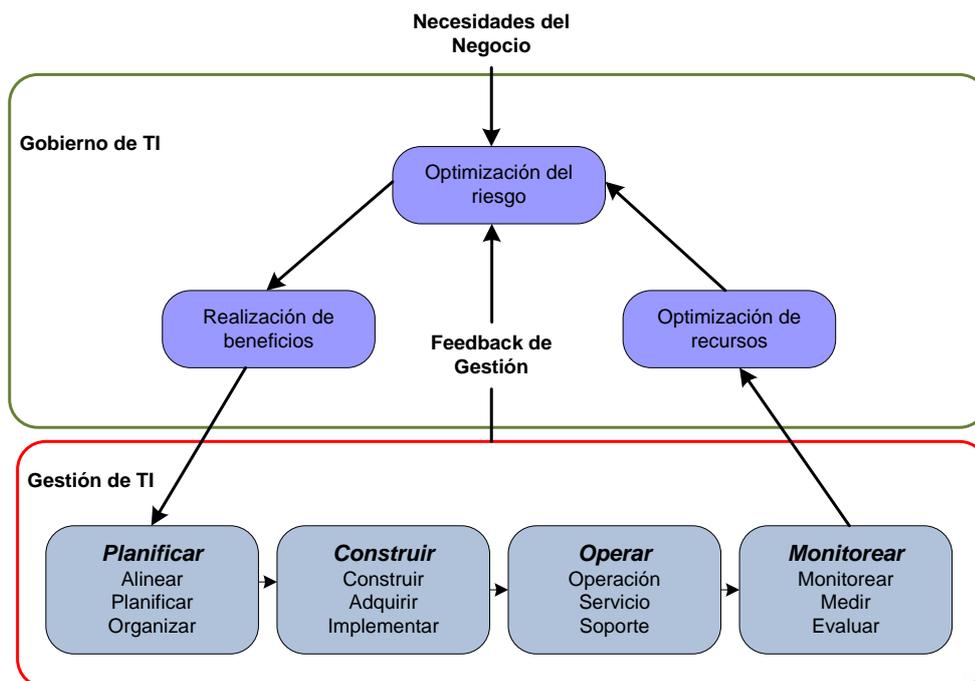


Figura 2.9 Procesos de gobierno y gestión
Fuente: (ISACA, 2012)

A este conjunto de procesos COBIT denomina Dominios que son aplicados a los niveles de gestión y de gobierno de la empresa.

2.3.2. Dominios de COBIT

COBIT divide a TI en dos procesos principales:

1. Gobierno. Contiene 5 procesos de gobierno de TI y se definen para cada uno de ellos las actividades de Dirigir, Supervisar y Evaluar: A este ciclo se lo denomina EDM.
2. Gestión. Contiene 4 dominios para las áreas de responsabilidad en los que se definen las actividades planear, construir, operar y monitorear a este conjunto se denomina PBRMI.

2.3.3. Distribución de los Dominios y Procesos de COBIT

En la figura 2.10 se muestra el grupo de procesos para cada uno de los dominios ya mencionados:

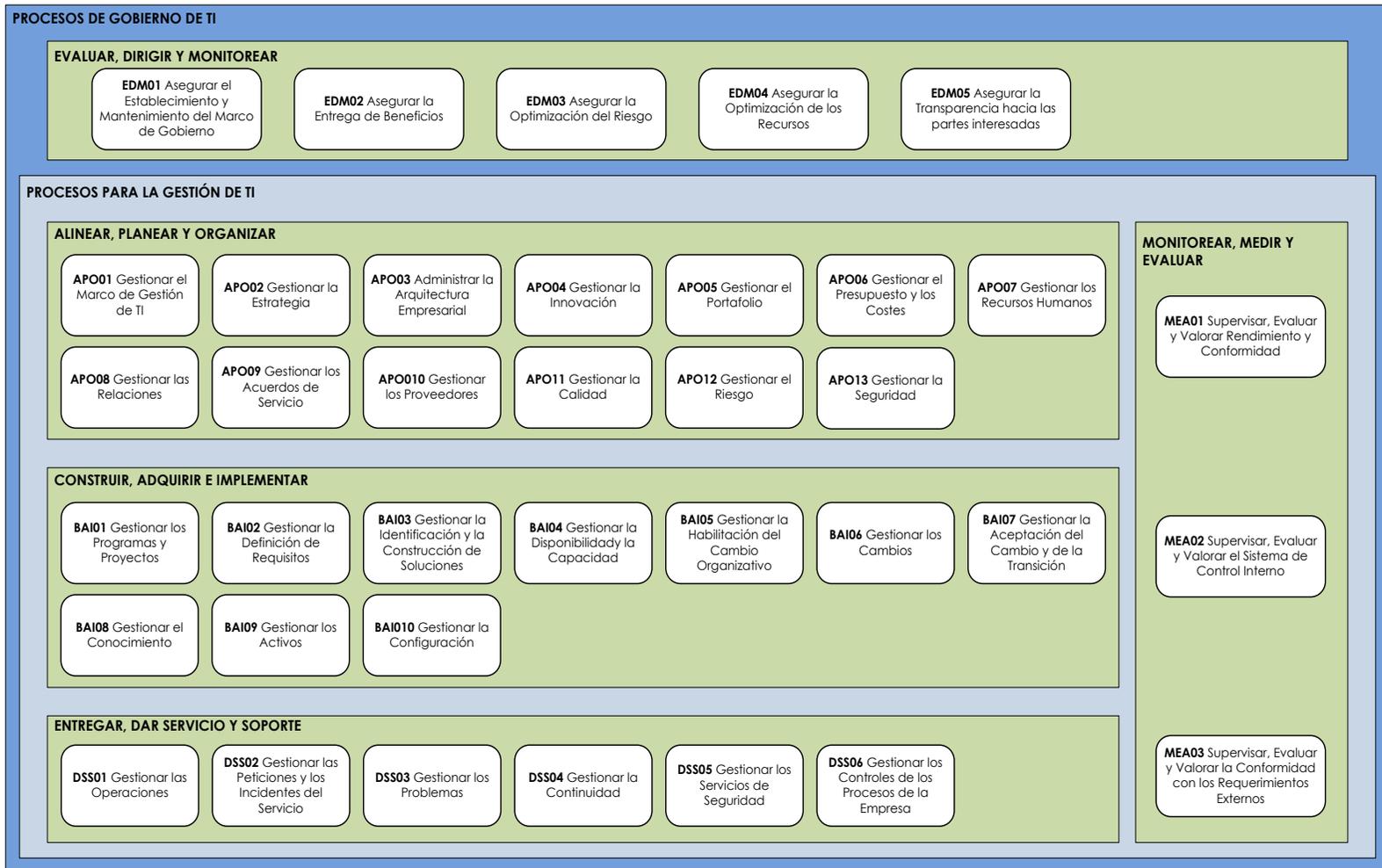


Figura 2.10 Referencia de procesos y dominios según el modelo COBIT 5
Fuente: (ISACA, 2012)

2.4. Asignación de prioridades de medidas de prestaciones técnicas (Descripción de parámetros de prestaciones)

Las normas, marcos de trabajo, modelos que definen la gobernanza de TI fueron creadas por personas u organizaciones diferentes, en distintos modelos, en distintos lugares y con diferentes enfoques, por lo que para poder realizar el análisis de compatibilidad entre ISO 38500 y COBIT se hace necesario seleccionar los parámetros adecuados de prestaciones.

Para este propósito, se toma la descripción de parámetros de prestaciones definida para Ingeniería de Sistemas, descrita por Benjamín Blanchard, que puede definirse como: “La aplicación de técnicas científicas y de ingeniería para:

1. Transformar una necesidad operativa en la descripción de los parámetros de prestaciones de un sistema y en su configuración mediante la utilización de un proceso iterativo de definición, síntesis, análisis, diseño, prueba y evaluación;
2. Integrar los parámetros técnicos relacionados y asegurar la compatibilidad de todas las interrelaciones físicas, funcionales y del programa de forma que se consiga la mejor definición y diseño del sistema completo; y
3. Integrar los aspectos de fiabilidad, mantenibilidad, seguridad, supervivencia, de personal y otros similares en el proceso global de ingeniería para conseguir los objetivos técnicos, de coste y de calendario fijados” (Blanchard, 1995)

En esta ámbito, prestaciones se puede definir como las características operativas, funcionales básicas de un sistema, entre ellos se puede mencionar: alcance, precisión, tasa, capacidad, volumen procesado, potencia de salida, dimensiones, peso, es decir cualquier característica

explícita o implícita que sea importante al momento de evaluar el rendimiento, la usabilidad de un sistema en función de la satisfacción total del producto obtenido, estos parámetros cambian de acuerdo a la naturaleza, a los objetivos y al propósito que vaya enfocado el sistema en estudio.

Se debe tener en cuenta que de todos los parámetros que se puedan definir, existen los parámetros críticos de prestación que se enfocan en el cumplimiento de la misión del sistema de acuerdo a los diferentes puntos de vista de cada interesado.

La descripción de parámetros de prestaciones se aplica a cualquier tipo de proyecto o sistema y puede ser analizado mediante Ingeniería de Sistemas, éste análisis inicia con la definición de los requisitos funcionales que son los que definen las funciones que el sistema necesita desarrollar, también se pueden definir los requisitos físicos, modos de operación, características, etc. Generalmente también se deben identificar los requisitos derivados que son los requisitos no establecidos directamente sino que son el producto del desarrollo propio del sistema.

Una vez definidas los requisitos, se definen los requisitos de prestaciones del sistema o parámetros de comportamiento de cada uno de los requisitos funcionales, es decir una vez definido que se debe hacer, sigue definir que tan bien debe hacerse, y finalmente se definen los requisitos de verificación, que permiten cumplir lo más fielmente los requerimientos iniciales.

La validación del total de los requisitos identificados se realiza por grupos clasificados de acuerdo a un nivel de prioridad (requisitos críticos, mandatorios, importantes, deseables) mediante el uso de las medidas de prestaciones técnicas (Technical Performance Measure, TPM) que no es

más que un margen de valores o un valor al que se puede calificar como aceptable cierta prestación.

Dentro del desarrollo del sistema o ejecución del proyecto, todas estas especificaciones deben ser incluidas como parte de la documentación y entregables que generalmente están asociados a los hitos de evaluación o pruebas.

2.5. Matriz de Holmes o de prioridades

La matriz de Holmes es una herramienta que permite comparar y priorizar parámetros de similares características que tratan sobre un tema en particular. Una matriz de criterios o priorización, es una herramienta para evaluar opciones basándose en una determinada serie de criterios explícitos que el grupo ha decidido que es importante para tomar una decisión adecuada y aceptable (Carrasco & Arasa, 2010).

La matriz de Holmes requiere de obtener una serie de opciones o parámetros que sean de complejos de evaluar y se requiere de priorizar estos parámetros buscando tomar una decisión. La matriz de Holmes permite clasificar los parámetros de acuerdo a su importancia respecto de algún criterio de comparación mediante la cuantificación de los parámetros, que facilita la toma de decisiones.

Para elaborar una matriz de Holmes se requiere de:

4. Definir un objetivo claro y explícito sobre el cual se definirá la matriz de Holmes
5. Identificar y elaborar una lista de parámetros respecto del objetivo que van a ser evaluados y priorizados
6. Con el listado de parámetros realizar una matriz que tanto en su eje vertical y horizontal contengan todos los parámetros a comparar.

7. Con la matriz definida, en la diagonal se llena con valores de 0,5 y en la parte superior de la diagonal se pondera cada parámetro respecto de los demás, determinando su grado de importancia respecto del otro, calificando con un 1 si el parámetro es más importante que el otro y con 0 si el parámetro es menos importante que el otro, sin perder de vista que la importancia es respecto del objetivo sobre el cual se está tratando. En la parte inferior de la diagonal se completa con valores de 0 ó 1 según corresponda a la celda opuesta correspondiente de la parte superior de la diagonal, al final se obtiene una matriz tipo L.
8. Se suma la horizontal de los resultados obtenidos para cada parámetro y se obtiene una calificación total que se ubica al extremo derecho de la matriz L.
9. Con la suma total obtenida para cada parámetro se obtiene un listado que cuantifica la importancia de cada parámetro, y que al ser ordenado permite una visualización clara de los parámetros más importantes. Con este listado se puede realizar cualquier otro tipo de análisis o tratamiento de la información obtenida.

En el caso particular del presente trabajo se busca evaluar a ISO 38500 y COBIT respecto de un conjunto de parámetros objetivo de la gobernanza de TI, la información obtenida de la matriz tipo L, se debe evaluar además respecto de ISO 38500 y de COBIT, y luego obtener una cuantificación total de cada parámetro tanto para ISO 38500 como para COBIT, para obtenerlo se realizará lo siguiente:

10. Una vez obtenida la lista de parámetros ordenada descendientemente, se discriminará usando el Principio de Pareto, descrito más adelante, para analizar únicamente los parámetros más importantes o más críticos respecto de la gobernanza de TI.

11. Se vuelve a aplicar el proceso descrito para la elaboración de la matriz de Holmes a los parámetros seleccionados como más importantes.
12. Además de obtener la suma total de calificación de cada parámetro, se obtiene una suma global de todas las calificaciones obtenidas y se ubica al final de la vertical de las sumas de cada parámetro.
13. Se busca obtener el grado de aportación de cada parámetro respecto del total global, a esta medida se la denomina factor de ponderación o simplemente ponderación y se obtiene dividiendo la suma total obtenida para cada parámetro dividida para el total global determinada en el punto 9. El factor de ponderación será usado como un factor de relación entre ISO 38500 y COBIT respecto de cada parámetro evaluado, y se ubica al lado de la suma total de cada parámetro.

Los parámetros más importantes seguramente son de naturalezas heterogéneas y difíciles de comparar entre sí, por lo que se usara los conceptos usados en Ingeniería de Software respecto de mediciones que aporten consistencia a los resultados obtenidos.

La medición de los parámetros permite comprender mejor los atributos de los modelos, evaluar su calidad y obtener una métrica asociada. Una métrica es la definición de un método de medición o su cálculo y el rango asociado.

Definir un método de medición puede buscar tener resultados objetivos (cálculos en base a fórmulas) o subjetivos (apreciación u observación), el rango son los valores extremos posibles que se puede obtener como resultado del método de medición como ejemplo: 1 el valor mínimo y 100 el valor máximo.

La propiedad más importante del rango es la escala, puede ser categórica o numérica y depende de la naturaleza de lo que está siendo evaluado como ejemplo: -40 muy malo, -20 malo, 20 bueno, 40 muy bueno. Para proporcionarle consistencia al análisis de los parámetros se usará una escala numérica

Para medir cada parámetro se definirá un rango y una escala que será descrito por el grado o nivel de cumplimiento del parámetro respecto de la gobernanza de TI.

14. El análisis final será someter a ISO 38500 y COBIT a una calificación de su cumplimiento de cada parámetro usando el método de medición descrito, obteniendo una matriz donde en el eje vertical estará ISO 38500 y COBIT y en el eje derecho los parámetros seleccionados como más importantes.
15. Se añadirá una fila donde se ubicará los factores de ponderación de cada parámetro obtenidos de acuerdo al punto 10.
16. Para obtener un resultado global se multiplica cada calificación obtenida por ISO 38500 y por COBIT multiplicada por el factor de ponderación de cada parámetro y se suma estos resultados en horizontal. Este cálculo permite hacer una relación justa entre los parámetros, su grado de cumplimiento respecto a la gobernanza de TI y las metodologías evaluadas.

2.6. Principio de Pareto

El principio de Pareto es también conocido como la regla del 80-20 y recibe este nombre en honor a Vilfredo Pareto, quien lo enunció por primera vez. En el mundo de la ingeniería del software el principio de Pareto puede ser enunciado de diferentes formas:

- Cuando se habla de los costes de desarrollo se puede decir que "el 80 % del esfuerzo de desarrollo (en tiempo y recursos) produce el 20 % del código, mientras que el 80 % restante es producido con tan solo un 20 % del esfuerzo".
- Si se habla de pruebas de software, el principio dice que "el 80% de los fallos de un software es generado por un 20% del código de dicho software, mientras que el otro 80% genera tan solo un 20% de los fallos" (Wikipedia, Principio de Pareto).

El principio de Pareto afirma que de un grupo de factores que buscan el mismo objetivo, únicamente unos pocos aportan la mayor parte para conseguir dicho objetivo (Fundibeq, 2009). Analiza cuantitativamente estos elementos y los clasifica en los "pocos vitales" y los "muchos triviales". Es aplicable a cualquier tipo de problemas donde se busca evaluar qué factores influyen más que otros a la consecución de un objetivo o resultado, es útil para discriminar y enfocar análisis o estrategias únicamente a lo más importante. Puede usarse en conjunto con otras metodologías de análisis, pero Pareto es la forma más sencilla de discriminar factores.

CAPÍTULO 3

ESTUDIO ANALÍTICO ENTRE ISO 38500 Y COBIT 5

3.1. Descripción de parámetros de comparación

Gobernanza de TI involucra una forma de evaluación directa del uso de las TI para apoyar y controlar el uso que se hace de TI buscando alinearse a los objetivos empresariales, para ello necesita incluir estrategias y políticas dentro de la organización.

La gobernanza de TI debe integrar el marco necesario para la toma de decisiones y rendición de cuentas, buscando fomentar el buen uso de las TI, y la capacidad organizacional de los directivos buscando controlar la implementación de la estrategia de TI integrándola con el negocio (Nugroho, Conceptual model of IT governance for higher education based on COBIT 5 framework, 2014).

ISO 38500 se encarga de definir la estrategia para que TI genere valor para el negocio, define el que hacer, mientras que COBIT se enfoca en entregar servicios y productos de valor, de llevar las estrategias de TI a planeación, desarrollo, implementación y evaluación, define cómo hacerlo, quien lo va a hacer y cuando hacerlo.

Una estrategia completa para gobernanza de TI debería contemplar las áreas de gobierno y de gestión, con éste propósito se establece y define un conjunto de parámetros de comparación:

1. Utilidad

Utilidad es cualidad o propiedad de valor útil que se le otorga a una acción o un objeto de útil. El término 'utilidad' también significa provecho, conveniencia, interés fruto o ganancia que se obtiene de algo (Definicion.de).

Algo es útil si satisface las necesidades de quien lo solicita, y si ese algo le sirve para realizar una tarea específica o cumplir un objetivo. Para TI la utilidad significa que el servicio que brinda TI sea en la cantidad apropiada, que sea relevante, que sea comprensible, que se pueda interpretar y que sea objetivo (ISACA, 2012).

2. Eficacia.

Es la capacidad de lograr un efecto deseado, esperado o anhelado (Wikipedia, Efectividad). Para TI eficacia se refiere a que la información que entregue TI sea relevante y pertinente para el negocio, además que debe ser entregada de manera oportuna, correcta, consistente y utilizable (Wikipedia, Information Criteria).

La eficacia se relaciona con el logro de las metas estratégicas y mejoras al negocio mediante el uso adecuado de las TI. El logro de las mencionadas metas está ligado a las métricas o la evidencia que se pueda obtener usando una variedad de fuentes de información, métodos y métricas que puedan sostener la calidad de que algo es eficiente.

3. Eficiencia.

Se trata de proveer información a través de la utilización óptima de los recursos (más productivo y económico) (Wikipedia, Information Criteria). Además funcione de forma eficiente y con costes competitivos, debe ser una fuente muy importante para la mejora de la productividad de la organización, de forma que incida directamente en la mejora de la rentabilidad (Cuesta, 2014).

La eficiencia trata de entregar la misma o mejor calidad de servicios más rápido y/o más barato, siempre tratando de aportar al negocio. Las organizaciones actualmente presionan para que sus departamentos sean más eficientes, TI debe estar constantemente buscando las maneras de lograrlo, con estrategias que aporten a este objetivo.

4. Confidencialidad.

La confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado (Wikipedia, Confidencialidad). Se refiere a la exactitud y completitud de la información como su validez en concordancia con los valores y expectativas del negocio (Ríos & Plazas, 2009).

La confidencialidad se relaciona con las características de protección de acceso, protección de privacidad, información de propietario e integridad que debe mantener la información y las directivas y acciones necesarias que deben ser garantizadas para lograrlo.

5. Integridad.

La integridad se refiere a la exactitud y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio (Wikipedia, Information Criteria). La integridad es un concepto complejo que tiene diferentes interpretaciones en los diferentes niveles de TI, como ejemplo en referencia a la seguridad, la integridad de los datos se define como la imposibilidad de que alguien modifique los datos sin ser descubierto (Gelbstein, 2011).

En referencia a la administración de base de datos integridad depende de que los datos introducidos en una base de datos sean precisos, válidos y coherentes. Integridad es la cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de éstos datos (Gelbstein, 2011).

La integridad se logra cuando se implementa los mecanismos necesarios para impedir eficazmente la inserción, modificación, o destrucción no autorizada sea accidental o no accidental de la información (Gelbstein, 2011). La integridad incumbe a la seguridad de la información, la calidad de software, al networking, a la capacidad del personal que genera esa información, y es uno de los parámetros que menos métricas tiene por lo complejo de su manejo.

6. Disponibilidad.

El concepto de disponibilidad se utiliza en diversos ámbitos y esferas para hacer referencia a la posibilidad de que algo, un producto o un fenómeno, esté disponible de ser realizado, encontrado o utilizado (Definicionabc).

Se refiere a que la información esté disponible cuando sea requerida por cualquier proceso del negocio sea ahora o en el futuro. También se refiere a la protección de los recursos necesarios y las capacidades asociadas (Wikipedia, Information Criteria).

La disponibilidad de los servicios que entrega TI es fácilmente visible y medible, la no disponibilidad se traduce en tiempo improductivo (downtime) que generalmente afecta al giro del negocio, se debe garantizar la disponibilidad de la información necesaria para dar soporte a los requerimientos del negocio.

7. Confiabilidad.

Hace referencia al grado de consistencia y estabilidad de las puntuaciones obtenidas a lo largo de sucesivos procesos de medición con un mismo instrumento (Wikipedia, Fiabilidad). Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento (Fernández & Llorens, 2011).

Los errores y caídas de algún servicio que proporciona TI, genera incomodidades sea de clientes internos o externos al negocio, y su costo se traduce en la pérdida de confiabilidad, es necesario asegurar que a lo largo del tiempo los servicios estén siempre disponibles y con la calidad e integridad requerida al punto de que puedan ser utilizados para responder a requerimientos fiscales y de obligaciones.

Se debe tener claro que la confiabilidad es en parte una percepción de que se pueda confiar en la información o servicios que se recibe de TI, confiabilidad implica que si la norma es seguida de manera adecuada los stakeholders pueden confiar en la gobernanza de TI.

8. Cumplimiento.

La oferta de cumplir con las leyes reglamentos y acuerdos contractuales a los que el proceso de negocio está sujeto, es decir, los criterios de negocio impuestos externamente, así como las políticas internas (Wikipedia, Information Criteria). Los controles que deben garantizar el cumplimiento de las políticas internas y con los requerimientos legales y regulatorios externos (Batch, 2012).

Todos los servicios que entrega TI deben cumplir y estar enmarcados dentro de la normativa, leyes o regulaciones tanto internas como externas a las que está sujeto el negocio. Son normativas que hereda del negocio y que debe ser cuidadosamente regulada y que garanticen el funcionamiento de TI en estricto apego. Junto con la confiabilidad y efectividad, proporcionan el respaldo que da la sensación de solvencia para TI respecto de sus servicios.

9. Alcance.

Distancia a la que llega la acción o influencia de alguien o algo (Wordreference). Normalmente las decisiones se clasifican en función de

su horizonte temporal en decisiones de corto y largo plazo. En ocasiones existe una relación entre el plazo temporal de la toma de decisión y el nivel al que es tomada.

Los altos ejecutivos y los CIOs suelen planificar y establecer objetivos estratégicos a largo plazo, mientras que el resto de la administración suelen estar autorizados sólo para tomar decisiones de inmediata aplicación. Además, las decisiones estratégicas necesitan de un mayor análisis y preparación que las decisiones tácticas (Fernández & Llorens, 2011).

El alcance se refiere al ámbito de acción, decisión e influencia que tiene la gobernanza de TI sobre la empresa, para el caso de estudio, sería el ámbito en el que se desenvuelve el modelo de gobernanza. El alcance del estándar es proporcionar los principios guía para los directivos sobre el uso efectivo, eficiente, y aceptable de las TI dentro de sus empresas.

10. Flexibilidad.

Por flexibilidad se entiende a la característica de flexible. Se trata de una palabra que permite resaltar la disposición de un individuo u objeto para ser doblado con facilidad, la condición de plegarse según la voluntad de otros y la susceptibilidad para adaptarse a los cambios de acuerdo a las circunstancias (Definicion.de).

La flexibilidad es la condición que tiene algo material o inmaterial de ser flexible, o sea lo contrario a lo rígido. Es lo que puede sufrir adaptaciones, es maleable, propenso a adaptarse a los cambios y a la movilidad (Deconceptos).

La flexibilidad está relacionada con la capacidad de adaptarse, para el caso sería la capacidad que tiene el modelo de gobernanza a adaptarse a las condiciones de la empresa, a su naturaleza, a su tamaño.

11. Objetividad.

Imparcialidad con que se trata o se considera un asunto prescindiendo de las consideraciones y los criterios personales o subjetivos (Thefreedictionary). La evaluación imparcial del gobierno de TI que el modelo hace a los procesos de gestión de las TI's en todo tipo de organizaciones que utilicen (hoy todas) las tecnologías de la información (Wikipedia, ISO/IEC 38500).

La evidencia práctica de que TI está cumpliendo sus objetivos son las métricas, que indican de manera imparcial y cuantificable el estado real de algún aspecto, el modelo de gobernanza debe facilitar, servir de base para hacer una evaluación imparcial de TI por parte de la alta dirección de la gestión de TI, esta evaluación puede dar con objetividad, sin prejuicios, y sin ambigüedades el estado real de TI.

12. Coherencia.

Relación lógica entre dos cosas o entre las partes o elementos de algo de modo que no se produce contradicción ni oposición entre ellas (Definicionabc). El concepto se utiliza para nombrar a algo que resulta lógico y consecuente respecto a un antecedente. La coherencia también se asocia a aquello que resulta entendible a partir de la lógica (Definicion.de, 2008).

La gobernanza de TI debe asegurarse de ser un marco coherente para garantizar que la dirección esa debidamente implicada en la gestión de TI en cualquier ámbito y alcance, que existe una buena articulación entre las medidas tomadas y la consecución de los objetivos, entre las estrategias planteadas y los resultados esperados.

13. Pertinencia.

Es la adecuación o el sentido de algo en un determinado contexto. Se trata de un adjetivo que hace mención a lo perteneciente o correspondiente a algo o a aquello que viene a propósito (Definicion.de).

Uno de los objetivos de TI es la alineación de sus objetivos con los de la empresa, para lograr este propósito, se deben utilizar diferentes estrategias, directrices contempladas en los modelos de gobierno de TI, se evalúa la pertinencia de estos modelos respecto al objetivo de alineación estratégica de TI.

14. Alineamiento estratégico.

El objetivo principal de la gobernanza de TI es conseguir la alineación de los recursos, capacidades, que posee o que podría adquirir a los objetivos actuales y futuros de la empresa. Esto significa que la estrategia de TI debe diseñarse de tal manera que apoye y apuntale la estrategia de la empresa, estableciendo las prioridades a los planes de TI con los objetivos estratégicos.

Una vez definidas las estrategias de TI la tarea de aterrizarlas a niveles de tareas, actividades y procesos con responsables, recursos, duración, también es parte del alineamiento estratégico. Las inversiones que se realicen deben estar enfocadas a soportar el negocio, crear infraestructura para crecimiento o para obtener ventaja competitiva.

Además se debe evaluar los beneficios obtenidos después de implementar los planes de TI.

15. Satisfacer las necesidades de los interesados.

Toda empresa busca generar valor para sus accionistas, por lo que uno de sus objetivos estratégicos será generar valor (valor o ganancia de

cualquier tipo) utilizando sus recursos, minimizando los costos de operación, y minimizando los riesgos.

Los beneficios que se buscan obtener, son conceptos diferentes para cada interesado, y es tarea del gobierno de TI considerar a todos los interesados y tomar decisiones evaluando los beneficios, la necesidad de recursos y los riesgos asociados, buscando el mejor equilibrio entre estos criterios.

16. Cubrir la organización de forma integral.

Se busca considerar a TI como una empresa, y que sus objetivos estratégicos heredados de los objetivos empresariales, se lleven a cabo desde el nivel estratégico, táctico y operacional.

Se debe contemplar todos los procesos y funciones necesarias para gobernar y administrar toda la organización, y en particular las TI, en esto debe incluir los servicios que presta TI internos como externos, además de los procesos de negocio internos y externos.

17. Transparencia financiera.

Debido a los costos que involucran las inversiones en TI, se busca que toda adquisición de TI, tenga un análisis apropiado, se hagan por razones válidas y que cumplan con un equilibrio entre costo, oportunidad y riesgo.

Si bien este tipo de análisis de cada adquisición de TI puede conllevar mucho tiempo y recursos, es válido al pensar que cada inversión en TI debe tener un retorno una generación de valor asociada en beneficio de la empresa, aparte de que debe contribuir a los objetivos estratégicos empresariales.

18. Estructuras organizativas.

Es importante definir responsabilidades relacionadas con el gobierno y la gestión de TI, para lograrlo se debe contar con una estructura organizacional bien definida, adecuadamente distribuida en los niveles estratégico, táctico y operacional, y con personal competente, esto junto a una empresa que cuente con procesos coordinados, asegura que los objetivos de gobernanza de TI se logren.

Una medida clave que se debería incluir es involucrar activamente al Consejo Administrativo, al Gerente (CEO - Chief Executive Officer) y al Gerente de TI (CIO – Chief Information Officer) como primeros responsables de la alineación de TI con el negocio.

19. Procesos de Gobernanza de TI

La gobernanza de TI se centra en la transformación de los recursos de TI para satisfacer las demandas actuales y futuras de la empresa y a los clientes del negocio.

Se debe incluir los procesos necesarios y adecuados para conseguir que la gobernanza de TI alcance sus 3 objetivos:

- 1) Que TI genere valor para el negocio,
- 2) Supervisar y controlar el rendimiento de la gestión de TI y
- 3) Mitigar los riesgos asociados al uso de las TI.

20. Gestión de riesgos.

TI debe analizar cómo proteger sus activos, conservar el valor del negocio, garantizar la continuidad de los servicios y una pronta recuperación en caso de un desastre.

Un adecuado manejo de los riesgos asociados al uso de las TI, permite detectar, prevenir y reaccionar ante eventos que puedan representar pérdidas de cualquiera de sus recursos y ponga en riesgo la disponibilidad de la información, el cumplimiento y la confiabilidad.

TI debe asegurar que los riesgos más importantes (estratégicos, operativos, información y cumplimiento) tengan políticas asociadas que permitan evitarlos, si bien la gestión de riesgos implica costos, una gestión adecuada puede significar una ventaja competitiva, y hacer que la empresa sea proactiva y reaccione rápidamente ante una situación de riesgo y/o pueda recuperarse lo más rápido posible.

21. Medir el rendimiento.

Evaluar valor generado por las TI, constituye una medida importante para la empresa, se busca controlar regularmente la ejecución de los proyectos, medir su rendimiento o desempeño y cuantificar la relación costo/beneficio.

La medición del rendimiento debe usar técnicas que se ajusten a la naturaleza de TI (servicios intangibles o mejora de servicios), pues muy probablemente medir a TI en términos económicos o monetarios no resulte apropiado. La medición del rendimiento proporciona información valiosa para valorar a TI, tomar decisiones y conocer el avance hacia los objetivos planteados.

22. Gestión de recursos.

Está enfocada al manejo adecuado y óptimo de los recursos disponibles y de los que se vaya a adquirir clasifica los recursos TI como:

- **Datos**, elementos de datos en su más amplio sentido, estructurados y no estructurados, gráficos, sonido, etc.
- **Aplicaciones**, que son la suma de procedimientos manuales y programados;
- **Tecnología**, hardware, software, sistemas operativos, sistemas de administración de bases de datos, etc.;

- **Instalaciones**, recursos para alojar y dar soporte a los sistemas de información; y
- **Personal**, habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y controlar servicios y sistemas de información (Fernández & Llorens, 2011).

TI debe manejar sus recursos de manera que coadyuven a un buen gobierno de TI, las estrategias, herramientas análisis que se hagan al respecto se denomina gestión de los recursos.

23. Gestión de Personas.

Las habilidades, actitudes y aptitudes de las personas (colaboradores) influyen en el éxito de una empresa. Para esto cada persona involucrada debe tener claro su rol dentro de TI, cada rol requiere de un conjunto de habilidades que debe ser documentado, y para su correcto desenvolvimiento se debe asegurar la capacitación, educación, conocimientos técnicos necesarios para que pueda ejecutar su trabajo.

Del lado de cada colaborador, su experiencia, habilidades, conocimiento, conducta, actitud le proporcionan a la empresa un valor agregado, una calidad que aporta al valor que TI entrega para el logro de los objetivos estratégicos.

24. Alinearse con las principales normas y estándares

La empresa se constituye por varias áreas, cada una para buscar su mejor funcionamiento puede adoptar seguir los lineamientos de normas, marcos de trabajo, buenas prácticas que mejor se adapten a su realidad, pero al mismo tiempo todos estos modelos deben integrarse, articularse de tal manera que se logre el máximo beneficio de todos ellos, lo

importante es lograr que todos los modelos aplicados coexistan juntos y se logre un modelo integral para la empresa.

TI, al seleccionar algún marco de trabajo o estándar en el cual apoyarse debe también tomar en cuenta que el modelo seleccionado debe tener la facilidad de combinarse con los diferentes marcos de trabajo de las otras áreas de la empresa con las que se TI se relaciona, esto con la premisa de que de manera general todos los marcos de trabajo no son mutuamente excluyentes y generalmente usan lenguajes similares.

25. Integra otras normas, marcos y/o estándares

Los marcos de trabajo, estándares, buenas prácticas tienen un ciclo de desarrollo, es decir inician con una visión y enfocados a solucionar una necesidad, pero conforme se van implementando, van incorporando nuevas funcionalidades, van adquiriendo madurez, en este contexto, los modelos también incorporan o recogen lo mejor de otros modelos o marcos, buscando mejorar sus funcionalidades o ampliar su enfoque.

3.2. Selección de parámetros de comparación

La selección de los parámetros de comparación consiste en discriminar al grupo de parámetros más importantes del total de los parámetros descritos, para lograrlo se realiza la matriz de Holmes comparando cada uno de los parámetros con respecto al resto y determinado cual es más importante en referencia a la gobernanza de TI, al final la de suma obtenida para cada parámetro, esto se muestra en la tabla 3.1.

Tabla 3.1
Matriz de Holmes parámetros de comparación

Parámetros de comparación	Utilidad	Eficacia	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Cumplimiento	Alcance	Flexibilidad	Objetividad	Coherencia	Pertinencia	Alineamiento estratégico	Satisfacer las necesidades de los interesados	Cubrir la organización de forma integral	Transparencia financiera	Estructuras organizativas	Procesos de Gobernanza de TI	Gestión de riesgos	Medir el rendimiento	Gestión de recursos	Gestión de Personas	Alinearse con las principales normas y estándares	Integra otras normas, marcos y/o estándares	Suma
Utilidad	0,5	0	0	0	0	0	0	0	1	1	0	1	0	0	0	1	0	1	0	0	1	1	1	0	1	9,5
Eficacia	1	0,5	1	1	1	1	1	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	1	1	15,5
Eficiencia	1	0	0,5	0	0	0	0	0	0	1	0	1	1	0	0	1	1	1	0	0	1	1	1	1	0	11,5
Confidencialidad	1	0	1	0,5	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	7,5
Integridad	1	0	1	0	0,5	1	0	0	0	1	0	1	0	0	0	1	1	1	1	1	0	1	1	1	1	14,5
Disponibilidad	1	0	1	1	0	0,5	0	0	0	1	1	0	0	0	0	1	1	1	1	0	0	1	0	1	1	12,5
Confiabilidad	1	0	1	1	1	1	0,5	0	1	1	0	1	1	1	0	1	1	1	0	0	1	0	1	0	0	15,5
Cumplimiento	1	0	1	1	1	1	1	0,5	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	21,5
Alcance	0	1	1	0	1	1	0	0	0,5	1	0	0	0	0	0	1	1	1	0	1	0	1	1	1	1	13,5
Flexibilidad	0	0	0	1	0	0	0	0	0	0,5	0	0	1	1	1	0	1	1	0	0	0	1	1	0	0	8,5
Objetividad	1	1	1	1	1	0	1	0	1	1	0,5	0	1	1	0	1	1	0	1	0	1	0	0	1	0	15,5
Coherencia	0	0	0	1	0	1	0	0	1	1	1	0,5	1	0	0	1	0	1	0	0	0	0	0	1	1	10,5
Pertinencia	1	0	0	1	1	1	0	1	1	0	0	0	0,5	0	0	1	1	1	0	0	0	0	0	1	1	11,5
Alineamiento estratégico	1	1	1	1	1	1	0	0	1	0	0	1	1	0,5	0	1	1	1	0	0	0	1	1	1	1	16,5
Satisfacer las necesidades de los interesados	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0,5	1	1	1	1	0	0	0	1	0	1	18,5
Cubrir la organización de forma integral	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0,5	1	0	0	1	1	1	1	0	0	7,5
Transparencia financiera	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0,5	1	0	0	0	0	0	1	1	6,5
Estructuras organizativas	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	0,5	1	0	0	0	0	0	0	5,5
Procesos de Gobernanza de TI	1	1	1	1	0	0	1	1	1	1	0	1	1	1	0	1	1	0	0,5	1	1	1	1	0	0	17,5
Gestión de riesgos	1	0	1	0	0	1	1	0	0	1	1	1	1	1	1	0	1	1	0	0,5	1	1	1	1	1	17,5
Medir el rendimiento	0	1	0	1	1	1	0	0	1	1	0	1	1	1	1	0	1	1	0	0	0,5	1	0	1	1	15,5
Gestión de recursos	0	1	0	1	0	0	1	0	0	0	1	1	1	0	1	0	1	1	0	0	0	0,5	0	1	0	10,5
Gestión de Personas	0	1	0	1	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	1	0,5	1	0	11,5
Alineación con las principales normas y	1	0	0	0	0	0	1	0	0	1	0	0	0	0	1	1	0	1	1	0	0	0	0	0,5	1	8,5
Integra otras normas, marcos y/o estándares	0	0	1	0	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0	1	1	0	0,5	9,5

Usando el principio de Pareto en la tabla 3.2 se muestran los parámetros ordenados por el total de la suma obtenida en la matriz de Holmes, el total acumulado, el porcentaje correspondiente del parámetro en referencia al total de la matriz, y el porcentaje acumulado de los parámetros.

Tabla 3.2
Tabla principio de Pareto

Parámetro	Suma	Acumulado	% del total	% acumulado del total
Cumplimiento	21,5	21,5	7%	7%
Satisfacer las necesidades de los interesados	18,5	40	6%	13%
Gestión de riesgos	17,5	57,5	6%	18%
Procesos de Gobernanza de TI	17,5	75	6%	24%
Alineamiento estratégico	16,5	91,5	5%	29%
Eficacia	15,5	107	5%	34%
Confiabilidad	15,5	122,5	5%	39%
Objetividad	15,5	138	5%	44%
Medir el rendimiento	15,5	153,5	5%	49%
Integridad	14,5	168	5%	54%
Alcance	13,5	181,5	4%	58%
Disponibilidad	12,5	194	4%	62%
Pertinencia	11,5	205,5	4%	66%
Gestión de Personas	11,5	217	4%	69%
Eficiencia	11,5	228,5	4%	73%
Gestión de recursos	10,5	239	3%	76%
Coherencia	10,5	249,5	3%	80%
Integra otras normas, marcos y/o estándares	9,5	259	3%	83%
Utilidad	9,5	268,5	3%	86%
Alineación con las principales normas y estándares	8,5	277	3%	89%
Flexibilidad	8,5	285,5	3%	91%
Cubrir la organización de forma integral	7,5	293	2%	94%
Confidencialidad	7,5	300,5	2%	96%
Transparencia financiera	6,5	307	2%	98%
Estructuras organizativas	5,5	312,5	2%	100%
Total	312,5			

Para hacer más visible la selección de los parámetros, aplicando el principio de Pareto la figura 3.1 muestran los totales de cada parámetro, contrastado con el porcentaje acumulado. Las líneas rojas punteadas muestran la división del 80% para el eje y derecho, y para el eje x, el cuadrante superior izquierdo concentra la mayor contribución de los parámetros y son llamados los “pocos vitales”, y el cuadrante inferior derecho los “muchos triviales”.

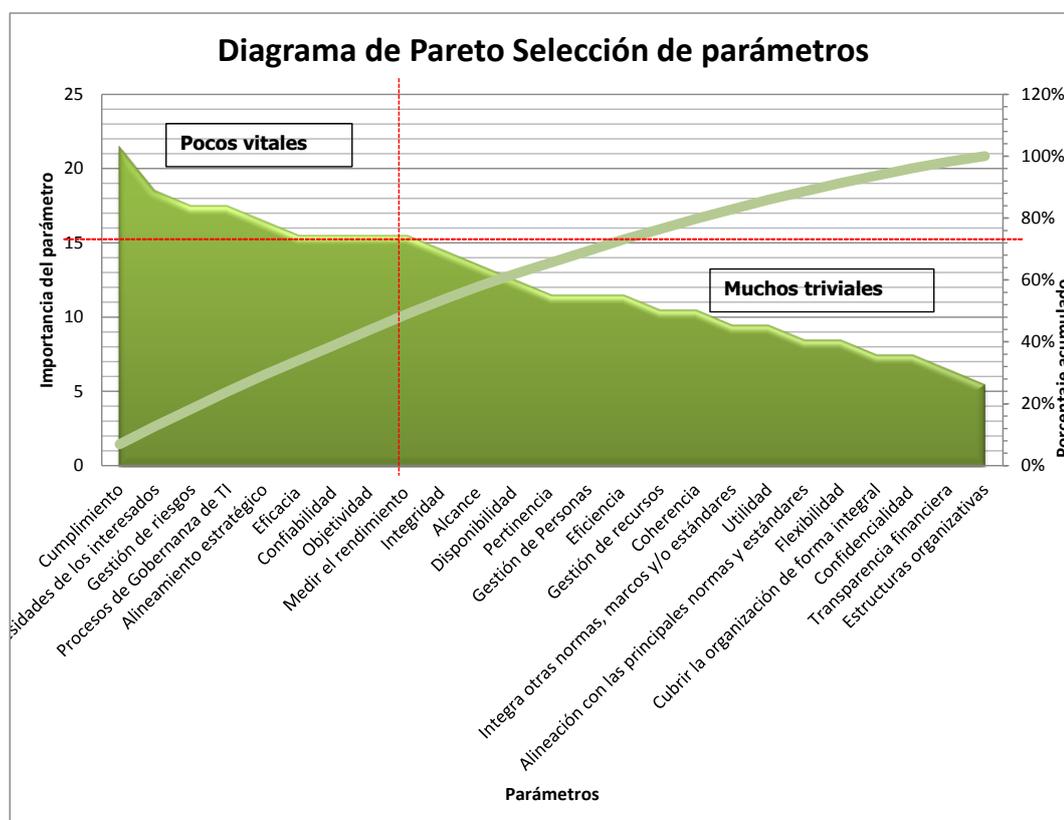


Figura 3.1 Diagrama de Pareto para la selección de los parámetros

Conforme con los resultados mostrados del principio de Pareto, los primeros parámetros mostrados en la tabla 3.3 son los de mayor contribución es decir son los criterios más importantes para gobernanza de TI.

Tabla 3.3
Resultados de principio de Pareto.

Parámetro	Suma
Cumplimiento	21,5
Satisfacer las necesidades de los interesados	18,5
Gestión de riesgos	17,5
Procesos de Gobernanza de TI	17,5
Alineamiento estratégico	16,5
Eficacia	15,5
Confiabilidad	15,5
Objetividad	15,5
Medir el rendimiento	15,5
Integridad	14,5
Alcance	13,5
Disponibilidad	12,5
Pertinencia	11,5
Gestión de Personas	11,5
Eficiencia	11,5
Gestión de recursos	10,5
Coherencia	10,5
Integra otras normas, marcos y/o estándares	9,5
Utilidad	9,5
Alineación con las principales normas y estándares	8,5
Flexibilidad	8,5
Cubrir la organización de forma integral	7,5
Confidencialidad	7,5
Transparencia financiera	6,5
Estructuras organizativas	5,5

Previo a comparar estos parámetros respecto a COBIT e ISO 38500, se evalúan mediante una matriz de Holmes, para obtener los pesos referenciales de cada parámetro, este valor luego es tomado en cuenta para evaluar el grado de cumplimiento del parámetro para ambos modelos. La tabla 3.4 muestra la matriz de Holmes aplicada a los parámetros de mayor contribución.

Tabla 3.4
Matriz de Holmes de parámetros seleccionados.

Parámetro	Cumplimiento	Satisfacer las necesidades de los interesados	Gestión de riesgos	Procesos de Gobernanza de TI	Alineamiento estratégico	Suma	Ponderación
Cumplimiento	0,5	1	1	0	1	3,5	0,28
Satisfacer las necesidades de los interesados	0	0,5	0	0	1	1,5	0,12
Gestión de riesgos	0	1	0,5	1	1	3,5	0,28
Procesos de Gobernanza de TI	1	1	0	0,5	1	3,5	0,28
Alineamiento estratégico	0	0	0	0	0,5	0,5	0,04
Total						12,5	

Los 5 criterios indicados son los atributos mínimos deseables de los modelos de Gobernanza de TI, queda evaluar en que “medida” ISO 38500 y COBIT cumplen con cada uno de estos atributos. Por la naturaleza compleja de los modelos ISO 38500 y COBIT realizar una medición de ellos se puede lograr amoldando los conceptos usados en Ingeniería de Software respecto a mediciones, esto aporta y resulta beneficioso en cuanto a la consistencia de los resultados obtenidos.

La medición de los parámetros permite comprender mejor los atributos de los modelos, evaluar su calidad y obtener una métrica asociada. Una métrica es la definición de un método de medición o su cálculo y el rango asociado.

El método de medición puede ser objetivo (cálculos en base a fórmulas) o subjetivo (apreciación u observación) y el rango son los valores extremos posibles que se puede obtener como resultado del método de medición. La propiedad más importante del rango es la escala, puede ser categórica o numérica y depende de la naturaleza de lo que está siendo evaluado.

Conforme estas definiciones, los métodos de medición de cada parámetro en una escala homogénea se definen de la siguiente manera:

- Para el parámetro de **cumplimiento**, se evalúa el nivel de facilidad que el estándar tiene para que TI se ajuste al cumplimiento de la normativa, leyes y regulaciones, se califica con 1 si el modelo no contempla el cumplimiento de la normativa, leyes y regulaciones, 2 si el modelo se ajusta a las regulaciones externas al negocio, 3 si el modelo se ajusta a las regulaciones externas e internas del negocio pero sin tener medidas si TI está estrictamente apegada a las normativas, y 4 si TI goza de una percepción de solvencia por su apego estricto y regulado a las normativa, leyes y reglamentos internos y externos al negocio.
- El parámetro de **satisfacer las necesidades de los interesados**, se evalúa si la norma contempla en sus lineamientos a los interesados y en qué medida son tomados en cuenta, dentro de los interesados están: inversores, accionistas, clientes, empleados, auditores, proveedores, financiadores, comunidad, gobierno, en total 9 interesados, la calificación sería 1 si no se hace referencia a los interesados, 2 si menciona a al menos 3 interesados y si existe indicaciones concretas respecto a la satisfacción de sus necesidades, 3 si menciona a al menos 6 de ellos, se contemplan medidas concretas y métricas de satisfacción de sus necesidades, y 4 si existen medidas concretas y métricas asociadas para todos los interesados.
- El parámetro **gestión de riesgos** evalúa las acciones de detección, seguimiento y control de los riesgos asociados a TI, su objetivo es aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad e impacto de los eventos negativos, se califica con 1 si el modelo no contempla nada sobre riesgos, 2 si identifica al menos dos riesgos, pero no existe ninguna medida asociada a ese riesgo, 3 si identifica riesgos y contempla alguna medida de mitigación de esos riesgos, 4 si existe un plan completo para detectar, prevenir y reaccionar ante un evento negativo.

- Para el parámetro **procesos de gobernanza de TI**, se evalúa si el modelo incluye los procesos necesarios para alcanzar los 3 objetivos de la gobernanza de TI. Se califica con 1 si no existe nada respecto a gobernanza de TI, 2 si se define procesos que apoyen a uno de los objetivos de la gobernanza de TI, 2 si se definen acciones que apoyen a dos de los objetivos de la gobernanza de TI y 4 si se definen acciones para los 3 objetivos de la gobernanza de TI.
- El parámetro de **alineamiento estratégico** evalúa que el modelo facilite el alineamiento estratégico de TI a los objetivos estratégicos de la empresa, se califica con 1 si el modelo no contempla el alineamiento con la estrategia de TI a la estrategia del negocio, 2 si el modelo contempla al menos una de las tres tareas de la gobernanza de TI (dirigir, evaluar y monitorear), 3 si el modelo facilita 2 de las tres tareas y facilita transformar las estrategias de TI en actividades, procesos acciones concretas a nivel de gestión de TI, y permite priorizar los proyectos de TI en pos del alineamiento estratégico corporativo, y 4 si el modelo contempla las 3 actividades, prioriza el portafolio de proyectos de TI, facilita transformar la estrategia de TI a acciones a nivel de gestión de TI, y permite medir el avance de la estrategia de TI.

La tabla 3.5 resume la calificación o métrica, el rango y las categorías definidos para cada parámetro.

Tabla 3.5
Tabla de métricas, rango y categorías.

Parámetro	Nivel de calificación			
	1	2	3	4
Cumplimiento	No facilitan el cumplimiento	Facilita un poco	Facilita medianamente	Facilita totalmente el cumplimiento
Satisfacer las necesidades de los interesados	No toma en cuenta a los interesados	Toma en cuenta unos pocos interesados	Toma en cuenta la mayoría de interesados	Toma en cuenta todos los interesados
Gestión de riesgos	No incluye gestión de riesgos	Menciona los posibles riesgos	Contempla actividades para mitigar riesgos puntuales	Cuenta con un plan de riesgos que cubre todas las áreas de TI
Procesos de Gobernanza de TI	No contempla procesos de gobierno	Menciona los procesos de gobierno	Tiene algunos procesos de gobierno de TI	Cuenta con todos los procesos de gobierno de TI
Alineamiento estratégico	No facilita el alineamiento estratégico	Facilita en pocos aspectos	Facilita en varios aspectos	Facilita totalmente el alineamiento estratégico

3.3. Aplicación de parámetros

La aplicación de parámetros consiste en evaluar cada parámetro de acuerdo a la tabla de métricas definida y obtener una calificación del cumplimiento de ISO 38500 y COBIT respecto a cada criterio, la tabla 3.6 muestra los resultados obtenidos de la calificación de cada parámetro.

Tabla 3.6
Resultados de aplicación de cada parámetro seleccionado a ISO 38500 y COBIT

Parámetro	Cumplimiento	Satisfacer las necesidades de los interesados	Gestión de riesgos	Procesos de Gobernanza de TI	Alineamiento estratégico
ISO 38500	2	2	2	4	4
COBIT	4	4	4	4	3

CAPÍTULO 4

RESULTADOS DEL ESTUDIO ANALÍTICO ENTRE ISO 38500 Y COBIT 5

4.1. Presentación de resultados

Un resultado global, se logra multiplicando cada calificación obtenida de la aplicación de los parámetros de comparación multiplicada por los factores de ponderación de la tabla 3.4. La tabla 4.1 muestra estos resultados.

Tabla 4.1
Resultados obtenidos

Parámetro	Cumplimiento	Satisfacer las necesidades de los interesados	Gestión de riesgos	Procesos de Gobernanza de TI	Alineamiento estratégico	Total
Factor de ponderacion	0,28	0,12	0,28	0,28	0,04	
ISO 38500	2	2	2	4	4	2,64
COBIT	4	4	4	4	3	3,96

Los resultados obtenidos ubican a COBIT e ISO 38500 respecto a la medida en que cumplen con estos atributos deseables de la gobernanza de TI.

ISO 38500 obtiene mejor resultado en el parámetro de **alineamiento estratégico**, por su enfoque al nivel estratégico cubre completamente las estrategias y tareas enfocadas a que TI cumpla con el alineamiento estratégico del negocio, COBIT en la versión 5 recoge para sí los principios y modelo de ISO 38500 e incrementa la visión de portafolio de productos y servicios competitivos, es decir COBIT facilita descender los objetivos

estratégicos del negocio al portafolio de proyectos que tiene TI, al mismo tiempo que busca proporcionarle valor a TI mediante la mejora o innovación de los productos y/o servicios que ofrece al negocio.

En el parámetro **cumplimiento** COBIT obtiene mejor resultado pues el apego estricto a las leyes, normativas, reglamentos tanto internos como externos que busca este parámetro, se aplica completamente con COBIT a nivel estratégico, táctico y operativo.

En cuanto a los **procesos de Gobierno de TI**, ISO 38500 y COBIT cumplen con tener acciones orientadas a cumplir con los 3 objetivos de la gobernanza de TI, con la diferencia que ISO 38500 cubre al nivel estratégico mientras que COBIT llega hasta el nivel táctico, ambos apalancan el logro de los mencionados objetivos.

El parámetro **satisfacer las necesidades de los interesados**, COBIT amplía más el cumplimiento de éste parámetro, pues a más de evaluar, dirigir y monitorear que las necesidades de los interesados sean cumplidas al igual que plantea ISO 38500, se asegura de medir que la inversión realizada en TI tenga un valor de retorno para el negocio, que las adquisiciones sean realizadas adecuadamente y respondan a una buena gestión. Esto debido a que COBIT integra a ValIT.

ValIT proporciona una fuente única, creíble y codificada para dar soporte a la creación de un valor de negocio real a partir de las inversiones posibilitadas por TI.

ValIT es relevante para todos los niveles de dirección a todo lo ancho tanto del negocio como de TI, desde el Director General y el consejo / directorio hasta todos aquellos involucrados directamente en los procesos de selección, aprovisionamiento, desarrollo, implementación, despliegue y

realización de beneficios. Val IT contiene guías esenciales para todos (Wikipedia, Val IT).

En el parámetro de **gestión de riesgos**, COBIT cumple a totalidad con lo que se espera de este parámetro, COBIT integra a Risk IT que brinda una vista completa de extremo a extremo de todos los riesgos relacionados con el uso de TI y un tratamiento similar a fondo de la gestión de riesgos, desde el tono y la cultura en la parte superior, a las cuestiones operativas (Wikipedia, Risk IT).

Con Risk IT se contemplan los riesgos de tipo estratégico, operativo, de información y de cumplimiento, Risk IT proporciona 3 dominios para la gestión del riesgo, la gobernanza del riesgo, la evaluación de los riesgos y la respuesta a los riesgos.

4.2. Discusión de resultados y análisis de compatibilidad

El cumplimiento de leyes, regulaciones, normativas es un atributo de primera importancia para la gobernanza de TI, COBIT utiliza las definiciones de COSO, que fueron ampliados no únicamente para las regulaciones financieras, sino para aquellas leyes, regulaciones, acuerdos contractuales a los que está sujeto el negocio, inclusive los externos.

ISO 38500 de su parte tiene como uno de sus principios al cumplimiento y dicta que Las TI deben cumplir con todas las leyes y normativas, Las políticas y los procedimientos internos deben estar claramente definidos, implementados y apoyados (Fernández & Llorens, 2011). El atributo de satisfacer las necesidades de los interesados para COBIT es uno de sus principios, clasifica las necesidades en:

- Obtención de beneficios
- Optimización de riesgos
- Optimización de recursos

Estas necesidades se deben transformar en estrategias que puedan lograrse, la cascada de metas de COBIT traduce las necesidades en prácticas específicas y metas personalizadas. Para ISO 38500 las necesidades de los interesados son parte de su modelo y en cada uno de los 6 principios se contempla implícitamente la satisfacción de las necesidades de los interesados.

El atributo de la gestión de riesgos en COBIT está completamente contemplado, con las definiciones de RiskIT, incluye un proceso completo de Gestión de los riesgos, que busca mitigar y enfrentar los posibles riesgos asociados a TI, COBIT define planes y medidas para cada riesgo. ISO 38500 se enfoca en el riesgo en cuanto al principio de adquisición, buscando que IT haga inversiones guardando equilibrio entre el beneficio, costo y riesgo asociado a las adquisiciones de TI.

Los procesos de gobernanza de TI, para COBIT los recoge en los 11 procesos que gestionan los elementos que giran alrededor de TI, pero no alcanzan el enfoque holístico más estratégico que logra ISO 38500, sin embargo ambos contemplan de manera adecuada lo necesario para la gobernanza de TI.

ISO 38500 respecto al alineamiento estratégico está enfocado totalmente al alineamiento estratégico con el negocio, las directrices de ISO 38500 son a nivel estratégico y directivo, su modelo de evaluar, dirigir y monitorear busca tener bajo control todas las operaciones de TI y que todas apuntalen a los objetivos estratégicos de la empresa. COBIT, recoge los lineamientos estratégicos del negocio y los transforma en acciones a nivel táctico y operativo, recoge métricas y permite evaluar el alineamiento estratégico.

Los resultados muestran que tanto ISO 38500 como COBIT tienen nichos específicos de acción, y cumplen en mayor o menor grado con los

atributos que debería contemplar un modelo de gobernanza de TI que sea aplicable a cualquier organización, elegir cuál de ellos implementar no supone ser una tarea sencilla y si se adopta uno solo de los modelos quedan algunos vacíos importantes. Tanto ISO 38500 como COBIT pueden integrarse, complementarse debido a su compatibilidad para convivir juntos de modo que sea cubierta en su totalidad los requerimientos de un buen gobierno corporativo de TI o un modelo de gobernanza de TI.

ISO 38500 goza de mayor difusión y aceptación por ser un estándar de aceptación internacional, COBIT al ser un marco de trabajo desarrollado por profesionales independientes ha logrado mejoras mediante la integración de otros estándares, modelos y mejores prácticas con lo que ha ganado ser un marco genérico de trabajo ampliamente aceptado. Mientras que COBIT gana terreno en el área de la gestión de TI, ISO 38500 se enfoca al nivel de gobierno de TI.

Para lograr un “mapeo” o integración entre COBIT e ISO 38500, se parte de la figura 4.1 que muestra el modelo de ISO 38500 y el modelo de COBIT. COBIT recoge de ISO 38500 las tareas de evaluar, dirigir y monitorear a nivel estratégico, y logra integrar con el nivel de gestión mediante los procesos de gobierno de TI. ISO 38500, únicamente dicta las políticas estratégicas que guiarán la actividad de TI, pero no llega al nivel de gestión, se asume que “alguien más” se encargaría de la ejecución de la estrategia a nivel operativo.

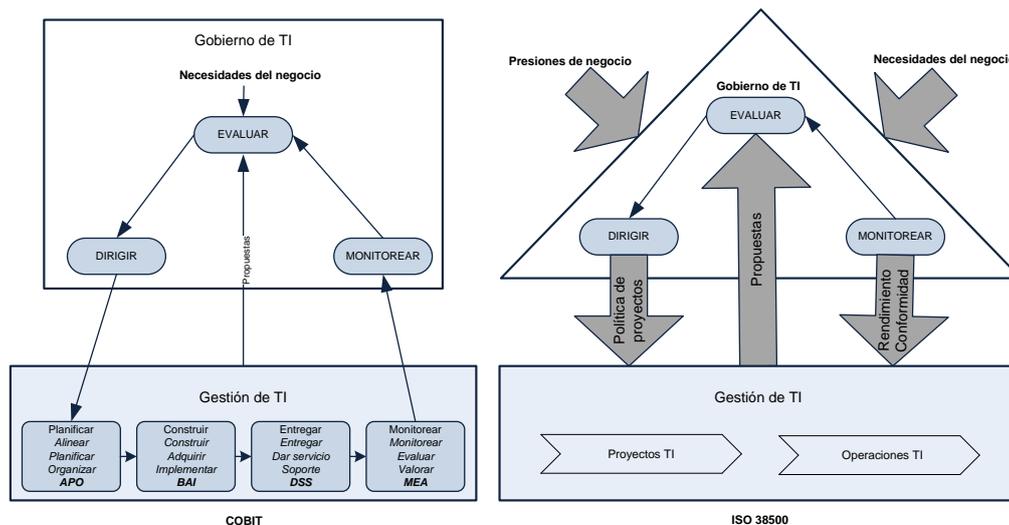


Figura 4.1 Integración COBIT e ISO 38500

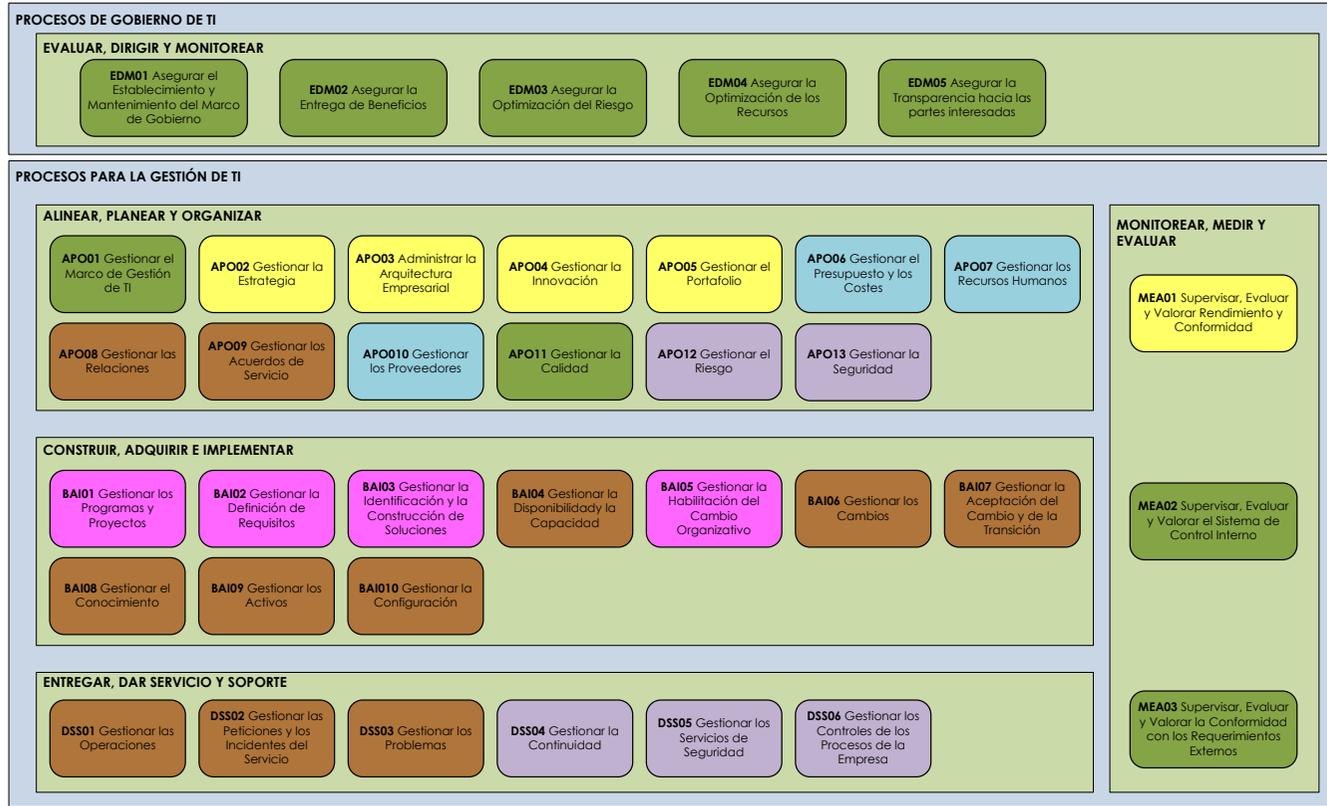
Durante la evolución de COBIT en sus diferentes versiones ha ido recogiendo y adoptando a otros modelos, normas, mejores prácticas logrando alinearse con todos ellos, integra además otros marcos ISACA dispersos, con ello ha logrado ser un marco de referencia integrado, la figura 4.2 muestra los enfoques en los que COBIT ha integrado otros estándares, marcos, mejores prácticas.

En la versión anterior de COBIT, se definieron los procesos de gestión de TI, y en la versión 5 se incluyeron los procesos de gobierno de TI, basados en las tareas de evaluar, dirigir y monitorear (EDM) definidos en ISO 38500. La figura 4.3 muestra en rojo los procesos de gobierno de TI.

Los procesos de gobierno de TI en COBIT son:

1. APO03 Gestionar la arquitectura empresarial
2. APO04 Gestionar la innovación
3. APO05 Gestionar el portafolio
4. APO06 Gestionar el presupuesto y los costes
5. APO08 Gestionar las relaciones
6. APO13 Gestionar la seguridad
7. BAI05 Gestionar la introducción de cambios organizativos
8. BAI08 Gestionar el conocimiento

9. BAI09 Gestionar los activos
10. DSS05 Gestionar los servicios de seguridad
11. DSS06 Gestionar los controles de los procesos del negocio



ENFOQUE	MARCOS DE REFERENCIA				
	COBIT 5	ISO 9001	ISO 38500	COSO	
GOBIERNO Y CALIDAD					
ESTRATEGIA	BSC	PMI Prf Mgn	TOGAF		
SERVICIOS	ISO 20000	ITIL			
DESARROLLO	CMMI	ISO 21500	PMI Prg Mgn	PMI PMBOK	PRINCE 2
PREVENCIÓN	ISO 31000	ISO 27000	ISO 22301		
RECURSOS	ITIL				

Figura 4.2 COBIT, integración varias mejores prácticas
Fuente: (Quintanilla, 2013)

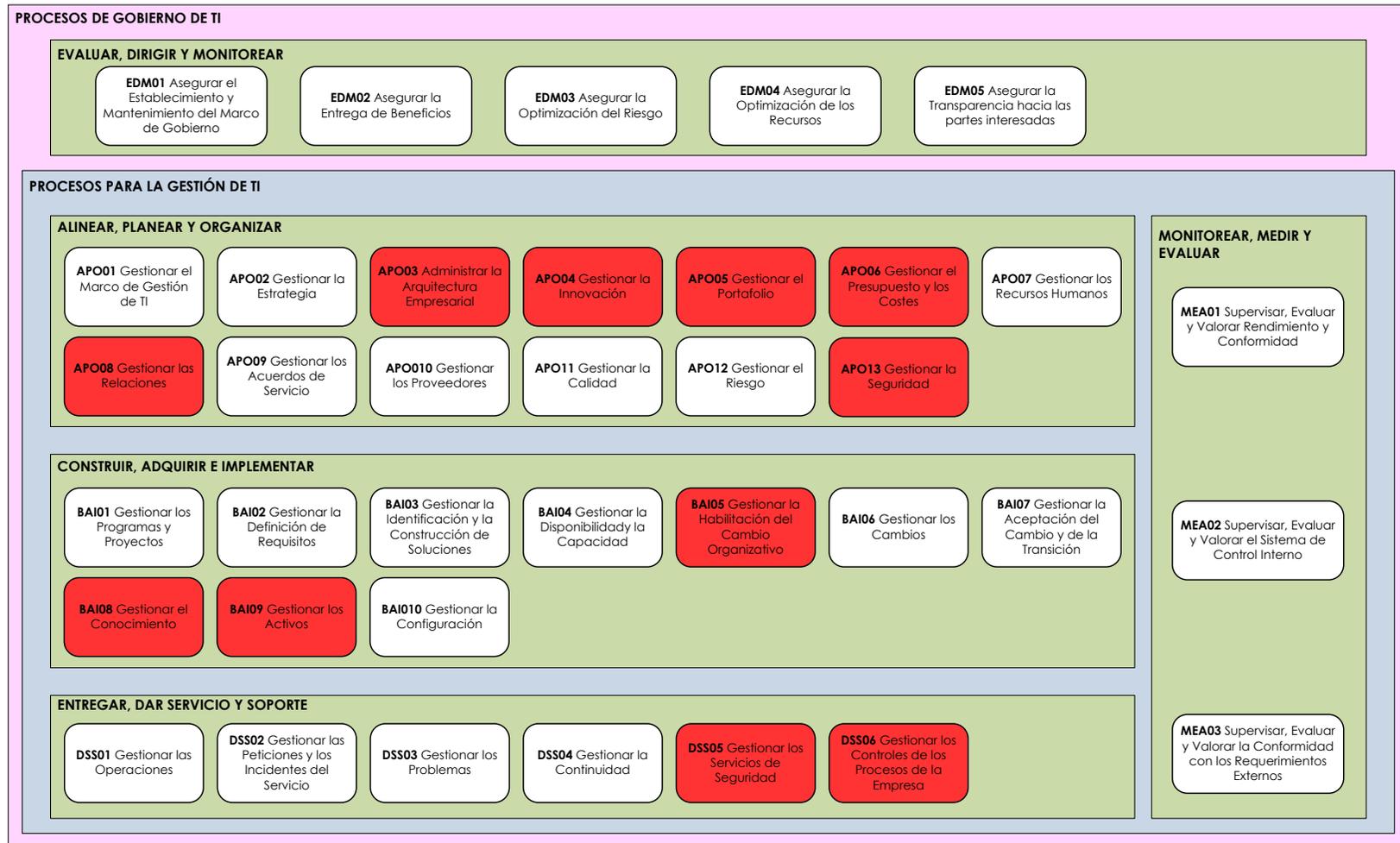


Figura 4.3 Procesos COBIT de gobierno de TI

Los principios que define ISO 38500 tienen compatibilidad con los procesos de COBIT, la figura 4.4 muestra los procesos COBIT que corresponden al cumplimiento de los principios de ISO 38500. Sin embargo, no se garantiza que COBIT cumpla completamente con esos procesos todo lo definido en los principios ISO 38500.

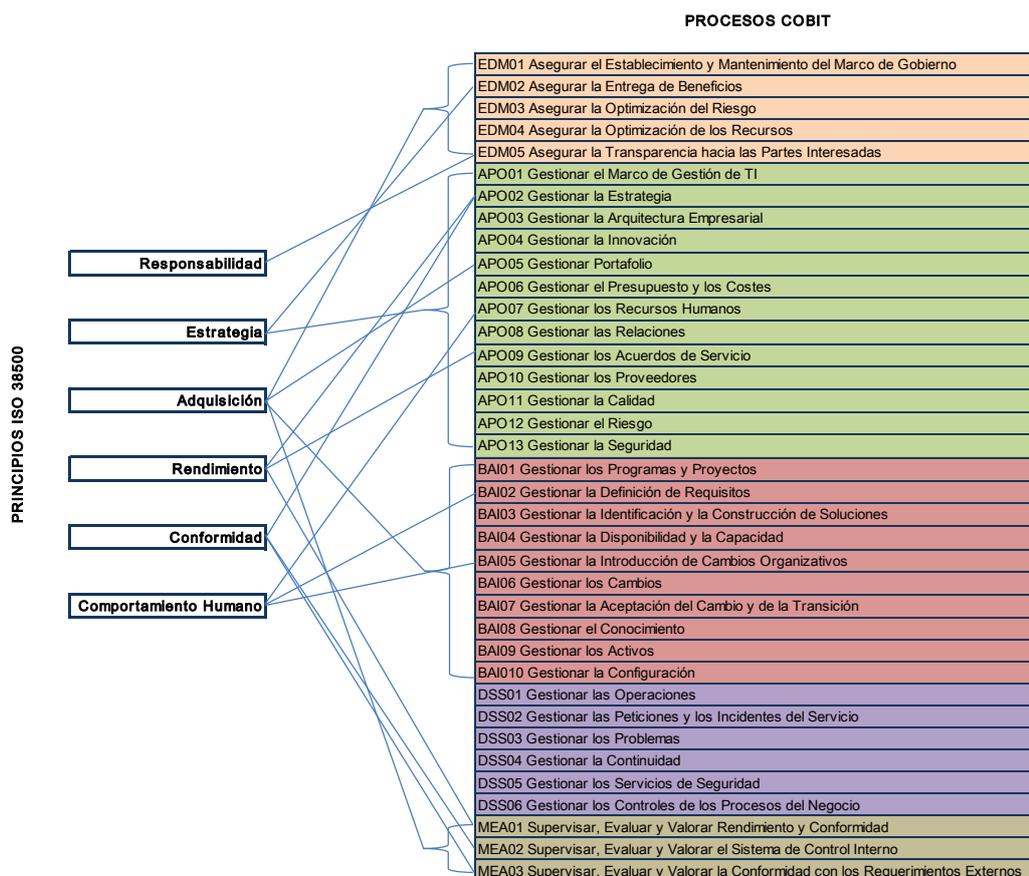


Figura 4.4 Principios ISO 38500 y procesos COBIT

Un aporte importante de COBIT al gobierno de TI es la incorporación de RiskIT y VallIT. Val IT (ITGI) es un framework de gobernabilidad que se puede utilizar para crear valor de negocio de las inversiones en TI.

Consiste en un conjunto de principios rectores y una serie de procesos y mejores prácticas que se los define como un conjunto de prácticas de gestión claves para apoyar y ayudar a la gerencia ejecutiva y juntas a nivel empresarial.

Val IT se centra en la decisión de invertir (¿estamos haciendo lo correcto?) y la realización de beneficios (¿estamos obteniendo beneficios?), mientras que COBIT está enfocado en la ejecución (¿lo estamos haciendo correctamente, y lo estamos logrando bien?) (Wikipedia, Val IT).

Risk IT (ISACA) brinda una visión completa y única de riesgos comerciales relacionados con la tecnología de la información, que pueden ocasionar a las compañías pérdidas anuales millonarias en ingresos y oportunidades. Los riesgos y el valor son dos lados de la misma moneda.

Los riesgos son inherentes a todas las empresas, pero se debe mantener cierto equilibrio para evitar la destrucción del valor y asegurar que las oportunidades para la creación de valores no se pierdan”, afirmó Brian Barnier, programador de TI, Certificado en Gobierno Empresarial de TI (Certified in the Governance of Enterprise Information Technology, CGEIT). “Risk IT ayuda a todos los niveles gerenciales en la administración de riesgos para obtener los mayores beneficios, y ayuda a detectar signos de advertencia con mayor anticipación” (Kessinger & Ketchum, 2009)

En cuanto a implementación la literatura de ISO 38500 proporciona el entorno adecuado para obtener el máximo provecho de las herramientas que brinda COBIT. COBIT dentro de su documentación de soporte incluye el IT Governance Implementation Guide (Guía de implementación de Gobierno de TI) que consiste de una metodología genérica y una hoja de ruta detallada que ayuda a la puesta en marcha, implementación, mantenimiento y mejora continua del ciclo de vida de gobierno de TI.

Se debe tener en cuenta que la orientación genérica que ofrece COBIT debe ser adaptada a las necesidades de cada organización y la hoja de ruta de la implementación debe diseñarse de acuerdo a estas necesidades.

Un modelo de trabajo de conjunto entre ISO 38500 y COBIT para la gobernanza de TI, sería básicamente construida basada en los 6 principios de ISO 38500, estos principios deberían funcionar bien para los procesos de gestión de TI: EDM, BAI, DSS APO y MEA. Estos procesos deberían responder a los 6 principios y a la vez cada principio debe ser cumplido por toda la estructura de TI.

La gobernanza de TI debería estar alineada con la Gobernanza de Empresa, y no ser de exclusiva responsabilidad del área de TI, debería ser responsabilidad de las personas involucradas con la gobernanza corporativa y con la gobernanza de negocio, asegurando que se cumpla la exigencia del gobierno corporativo relativo a cumplimiento y respecto al gobierno de negocio asegurar que se puede producir algo útil y rentable para la organización.

La implementación de los 6 principios en los procesos de gobernanza de TI aseguran que cada paso que se tome esté alineado con la misión y visión de las necesidades de los interesados. Las funciones de gobernanza se traducen en evaluar, dirigir y monitorear la consecución de los requerimientos del negocio y de los interesados y sean traducidos en planes de desarrollo en el área de gestión de TI.

En el área de gestión de TI, la dirección de la gobernanza de TI se traduce en planeación, desarrollo, implementación y evaluación interna, en la

figura 4.5 se puede ver este modelo sencillo de trabajo conjunto entre ISO 38500 y COBIT.

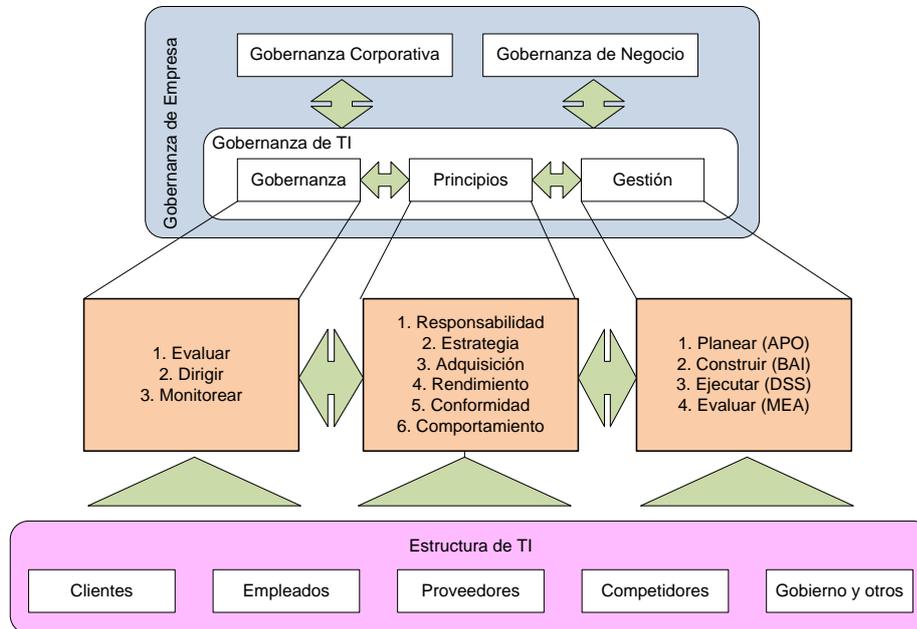


Figura 4.5 Trabajo conjunto entre ISO 38500 y COBIT

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Una vez concluido el presente estudio, los resultados obtenidos determinan que:

- Se ha logrado realizar satisfactoriamente el estudio analítico de la compatibilidad de la norma ISO IEC 38500 y COBIT 5 aplicado a la gobernanza de TI.
- La gobernanza de TI es un concepto muy debatido y disperso que busca aportar valor, manejo de riesgos y recursos, evaluación del rendimiento de TI dentro de la organización, que para su consecución se apoya en los estándares, buenas prácticas y regulaciones existentes que contengan lineamientos sobre gobernanza de TI.
- ISO IEC 38500 es un estándar formal para la gobernanza de TI desarrollado por la alianza ISO IEC que contempla definiciones adecuadas para gobernanza de TI, seis principios de un buen gobierno corporativo de TI y tres actividades que permiten gobernar TI. COBIT es un marco de trabajo desarrollado por ISACA que es un conjunto de buenas prácticas de gobierno y gestión de TI que incluye controles, medidas, modelos de madurez, indicadores y procesos para éstas dos áreas de TI, basado en cinco principios y siete facilitadores.
- Los parámetros de comparación se definen como los criterios aplicables esperados de un modelo de gobernanza de TI contemplados en un enfoque completo en las áreas estratégica, táctica y operativa de las organizaciones. El análisis comparativo de los parámetros más importantes somete a una evaluación cuantitativa del grado de cumplimiento de los mencionados parámetros respecto de ISO 38500 y COBIT.
- Los parámetros analizados como los más importantes: Cumplimiento, Satisfacer las necesidades de los interesados, Gestión de riesgos, Procesos de gobernanza de TI y Alineamiento estratégico, uno a uno y en conjunto se alinean al cumplimiento de los principios de la

gobernanza de TI definidos por el ITGI. La evaluación muestra que tanto ISO 38500 como COBIT cubren diferentes nichos de una buena gobernanza de TI, pero también tienen áreas e intereses comunes que son complementados e integrados por ambos. ISO 38500 establece “qué” se debe hacer mientras que COBIT establece “cómo”, “cuándo”, “por quién”, ISO 38500 proporciona el entorno necesario para obtener el máximo provecho de las buenas prácticas que ofrece COBIT, con ello obtener una ventaja competitiva perceptible.

- Una buena gobernanza de TI resultaría de la aplicación conjunta de ISO 38500 y de COBIT, del análisis de compatibilidad se desprende que se puede lograr un modelo completo de gobernanza de TI con la aplicación de ambos modelos expuestos para cualquier organización. Formalmente no existe un documento, una guía, una hoja de ruta (roadmap) para la implementación del modelo de gobernanza de TI basado en ISO 38500 y COBIT, el presente documento puede servir de pauta para los profesionales de TI que estén interesados en darle un valor estratégico al área de TI dentro de sus organizaciones mediante la implementación de un modelo de gobernanza de TI. Implementar e integrar en cualquier organización un modelo de gobernanza de TI, significa dirigir, gestionar y controlar las actividades de TI para alcanzar los objetivos de la organización mediante la adición de valor y el equilibrio entre el riesgo y el retorno sobre TI, pero también significa un ciclo continuo de trabajo, alto compromiso de todos los involucrados, fuerte conocimiento de la normativa a aplicar ISO 38500 y COBIT, una estructura organizativa bien definida y una correcta implementación de ISO 38500 y de COBIT.

5.2. Recomendaciones

- Realizar una guía genérica que sirva de modelo para la implementación de ISO 38500 y COBIT enfocados en la gobernanza de TI en cualquier organización.
- Desarrollar un comparativo entre la norma ISO 38500:2008 e ISO 38500:2015
- Lograr que los profesionales de las áreas de TI se empoderen de los conceptos de gobernanza, gobierno y gestión de TI que les permitan ser entes activos y participativos en las organizaciones para las que presten sus servicios, y que lleven a TI a una mejora de su realidad en cada organización. Lograr que los profesionales de Gestión de TI profundicen sus conocimientos sobre ValIT y RiskIT y su relación con la generación de valor y manejo de riesgos asociados al área de TI.
- Proponer un modelo de gobernanza de TI basado en los principios Gestión, Riesgo y Cumplimiento usando ISO 38500 y COBIT.
- Evaluar el impacto de los problemas a los que se podría enfrentar un proyecto de implementación de gobernanza de TI en una organización:
 - Falta de compromiso, involucramiento y apoyo de la alta dirección.
 - Personal del área de TI que no tenga los conocimientos y habilidades necesarias
 - Falta de aplicación de una metodología adecuada

BIBLIOGRAFÍA

- Arteaga Calispa, H. (13 de 4 de 2012). Desarrollo de un gobierno de TI para la empresa FIDUCIARIA Ecuador usando COBIT 4.1. *Facultad de Ingeniería de Sistemas - Escuela Politécnica Nacional*. Quito, Ecuador.
- Batch, L. (3 de 2012). *Accounting Information Systems Romney and Steinbart*. Recuperado el 28 de 10 de 2014, de lindabatchla2:lindabatchtla2portfolio.weebly.com/uploads/2/1/0/9/21092758/info_31878_deck_9_text_book_information_-_linda_batch.ppt
- Blanchard, B. (1995). *Ingeniería de Sistemas*. Madrid, España: ISDEFE.
- Carrasco, S., & Arasa, E. (8 de 7 de 2010). *Ministerio de la Protección Social*. Recuperado el 12 de 10 de 2014, de <http://mps1.minproteccionsocial.gov.co/evtmedica/linea%203.1/2.4matrices.html>
- Chaudhuri, A. (2011). *Enabling Effective IT Governance: Leveraging ISO/IEC 38500:2008 and COBIT to achieve business-IT alignment*. Recuperado el 17 de 10 de 2014, de Researchgate:
http://www.researchgate.net/publication/233468364_Enabling_Effective_IT_Governance_Leveraging_ISOIEC_385002008_and_COBIT_to_Achieve_BusinessIT_Alignment?ev=srch_pub&_sg=5qseL%2F1XLI22R0CljAFoHoF91efy7R29yU%2BQVP34GU5YduJ9LshN2JR3NmByfsr1_VlkVNYLjdCzUStfgB
- Coello, H. (8 de 12 de 2008). *ITIL, COBIT, CMMI, PMBOK: Cómo integrar y adoptar los estándares para un buen gobierno de TI*. Recuperado el 19 de 10 de 2014, de Wordpress: <https://helkyncoello.wordpress.com/2008/12/08/itil-cobit-cmmi-pmbok-como-integrar-y-adoptar-los-estandares-para-un-buen-gobierno-de-ti/>
- Cuesta, A. (4 de 2014). *Ibermática*. Recuperado el 15 de 10 de 2014, de <http://www.ibermatica.com/sala-de-prensa/opinion/como-medir-el-alineamiento-entre-ti-y-negocio-gobierno-ti-y-cobit-5>
- De Los Ríos, F. (2013). *Cobit 5 Introducción*. Recuperado el 6 de 11 de 2014, de slideshare: <http://es.slideshare.net/fernandelos/cobit5-introduccinv5.pdf>
- Deconceptos. (s.f.). *Flexibilidad*. Recuperado el 24 de 10 de 2014, de Deconceptos: <http://deconceptos.com/general/flexibilidad>
- Definicion.de. (2008). *Coherencia*. Recuperado el 24 de 10 de 2014, de Definicion.de: <http://definicion.de/coherencia/>

- Definicion.de. (s.f.). *Flexibilidad*. Recuperado el 24 de 10 de 2014, de Definicion.de:
<http://definicion.de/flexibilidad/>
- Definicion.de. (s.f.). *Pertinencia*. Recuperado el 26 de 10 de 2014, de Definicion.de:
<http://definicion.de/pertinencia/>
- Definicion.de. (s.f.). *Utilidad*. Recuperado el 15 de 10 de 2014, de Definicion.de:
<http://definicion.de/utilidad/>
- Definicionabc. (s.f.). *Coherencia*. Recuperado el 10 de 23 de 2014, de Definicionabc:
<http://www.definicionabc.com/general/coherencia.php>
- Definicionabc. (s.f.). *Disponibilidad*. Recuperado el 15 de 10 de 2014, de
<http://www.definicionabc.com/general/disponibilidad.php>
- Fernández Sánchez, C., & Piattini Velthuis, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*. Madrid: AENOR.
- Fernández, A., & Llorens, F. (10 de 2 de 2011). *Gobierno de las TI para Universidades*. Recuperado el 24 de 10 de 2014, de gti4u: <http://www.gti4u.es/pdf/gobierno-de-las-ti-para-universidades-imprimible.pdf>
- Fernández, A., Llorens, F., & De Andrés, J. (15 de 6 de 2011). *kTI, A Self-Assessment IT Governance System*. Recuperado el 2 de 10 de 2014, de Eunis:
http://www.eunis.ie/papers/kTI_AntonioFernandez_Paper.pdf
- Fundibeq. (22 de 1 de 2009). *Fundibeq*. Recuperado el 22 de 10 de 2014, de Diagrama de Pareto:
http://www.fundibeq.org/opencms/export/sites/default/PWF/downloads/gallery/methodology/tools/diagrama_de_pareto.pdf
- Gartner. (s.f.). *Gartner*. (Gartner, Ed.) Recuperado el 2 de 10 de 2014, de
<http://www.gartner.com/it-glossary/it-governance/>
- Gelbstein, E. (25 de 10 de 2011). *La integridad de los datos: el aspecto más relegado de la seguridad de la información*. Obtenido de www.isaca.org:
<http://www.isaca.org/Journal/Documents/11v6-Data-Integrity-Information-Security-Poor-Relation-spanish.pdf>
- IEDGE - The European Business School. (19 de 9 de 2011). *blog.iedge.eu*. Recuperado el 23 de 11 de 2014, de <http://blog.iedge.eu/wp-content/uploads/2011/09/IEDGE-SITI-12.jpg>
- ISACA. (4 de 12 de 2012). *Un marco de negocio para el gobierno y la gestión de las TI de la empresa*. Recuperado el 18 de 11 de 2014, de ISACA:
<http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf>

- ITGI. (2008). *Alineando COBIT 4.1, ITIL, e ISO/IEC 27002 en beneficio del negocio*. Recuperado el 20 de 11 de 2014, de ISACA: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf
- Kessinger, K., & Ketchum, M. (8 de 12 de 2009). *ISACA lanza Risk IT Framework para ayudar a organizaciones a equilibrar los riesgos con los beneficios*. Recuperado el 3 de 11 de 2014, de ISACA: <http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Launches-Risk-IT-Framework-to-Help-Organizations-Balance-Risk-with-Profit-Spanish.aspx>
- Lees, G. (6 de 2007). *Enterprise Governance*. Recuperado el 29 de 10 de 2014, de Cimaglobal: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_enterprise_governance__feb08.pdf.pdf
- Montaña Barón, A. (2013). Propuesta para la implementación de un esquema de gobierno de TI en ambientes tercerizados (Outsourcing) Caso de estudio: Universidad Nacional de Colombia. *Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial*. Bogotá, Colombia.
- Nugroho, H. (2013). *Proposed model of Vocational University Governance and measurement model by utilizing the ISO 38500 framework and COBIT 5 enabler*. Recuperado el 28 de 10 de 2014, de Researchgate: http://www.researchgate.net/publication/261489483_Proposed_model_of_Vocational_University_Governance_and_measurement_model_by_utilizing_the_ISO_38500_framework_and_COBIT_5_enabler
- Nugroho, H. (20 de 10 de 2014). *Conceptual model of IT governance for higher education based on COBIT 5 framework*. Recuperado el 14 de 10 de 2014, de JATIT: <http://www.jatit.org/volumes/Vol60No2/4Vol60No2.pdf>
- Quintanilla, G. (9 de 7 de 2013). *Introducción a COBIT 5*. Recuperado el 20 de 12 de 2014, de Software Guru: <http://sg.com.mx/sgce/2013/sessions/introducci%C3%B3n-cobit-5#.VWRpho6Qllw>
- Ríos, C., & Plazas, D. (4 de 3 de 2009). Recuperado el 16 de 10 de 2016, de <http://es.slideshare.net/cairiza/principios-de-cobit>
- Saull, R. (2006). *IT Governance a framework for performance and compliance*. Recuperado el 3 de 11 de 2014, de ITGI: <http://www.itgi.jp/conf200611/ronsauill.pdf>

ServiceXen. (1 de 6 de 2008). *IT Governance vs. Corporate Governance vs. IT Management*.

Recuperado el 10 de 10 de 2014, de ServiceXen:
<https://servicexen.wordpress.com/2008/06/01/it-governance-vs-corporate-governance-vs-it-management/>

Sunthonwutinun, W., & Chooprayoon, V. (8 de 8 de 2013). *A benchmarking study of standard frameworks for Information Technology Governance*. Recuperado el 20 de

11 de 2014, de SAKI:
http://saki.siit.tu.ac.th/acis2013/uploads_final/117__769dc388c40f9ef712c8dfe8e1de7513/acis2013_CameraReadyRvision_08.08.2013.pdf

Thefreedictionary. (s.f.). *Objetividad*. Recuperado el 24 de 10 de 2014, de
Thefreedictionary: <http://es.thefreedictionary.com/objetividad>

Wikipedia, C. d. (s.f.). *Confidencialidad*. Recuperado el 15 de 10 de 2014, de
<http://es.wikipedia.org/wiki/Confidencialidad>

Wikipedia, C. d. (s.f.). *Corporate Governance*. Recuperado el 12 de 10 de 2014, de
http://en.wikipedia.org/wiki/Corporate_governance

Wikipedia, C. d. (s.f.). *Corporate Governance of Information Technology*. Recuperado el 3 de
10 de 2014, de
http://en.wikipedia.org/wiki/Corporate_governance_of_information_technology

Wikipedia, C. d. (s.f.). *Efectividad*. Recuperado el 15 de 10 de 2014, de
<http://es.wikipedia.org/w/index.php?title=Especial:Citar&page=Efectividad&id=81747852>

Wikipedia, C. d. (s.f.). *Fiabilidad*. Recuperado el 20 de 10 de 2014, de
http://es.wikipedia.org/wiki/Fiabilidad_%28psicometr%C3%ADa%29

Wikipedia, C. d. (s.f.). *Gestión de servicios de Tecnologías de la Información*. Recuperado el
10 de 10 de 2014, de
http://es.wikipedia.org/w/index.php?title=Especial:Citar&page=Gesti%C3%B3n_de_servicios_de_tecnolog%C3%ADas_de_la_informaci%C3%B3n&id=82375789

Wikipedia, C. d. (s.f.). *Gobernabilidad*. Recuperado el 2 de 10 de 2014, de
<http://es.wikipedia.org/wiki/Gobernabilidad>

Wikipedia, C. d. (s.f.). *Gobernanza*. Recuperado el 2 de 10 de 2014, de
<http://es.wikipedia.org/wiki/Gobernanza>

Wikipedia, C. d. (s.f.). *Gobierno Corporativo*. Recuperado el 3 de 10 de 2014, de
http://es.wikipedia.org/wiki/Gobierno_corporativo

Wikipedia, C. d. (s.f.). *Information Criteria*. Recuperado el 15 de 10 de 2014, de http://en.wikipedia.org/wiki/Information_Criteria

Wikipedia, C. d. (s.f.). *ISO/IEC 38500*. Recuperado el 28 de 10 de 2014, de http://en.wikipedia.org/wiki/ISO/IEC_38500

Wikipedia, C. d. (s.f.). *Objetivos de control para la información y tecnologías relacionadas*. Recuperado el 24 de 10 de 2014, de http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas

Wikipedia, C. d. (s.f.). *Principio de Pareto*. Recuperado el 22 de 10 de 2014, de http://es.wikipedia.org/w/index.php?title=Especial:Citar&page=Principio_de_Pareto&id=82253059

Wikipedia, C. d. (s.f.). *Risk IT*. Recuperado el 28 de 10 de 2014, de http://en.wikipedia.org/wiki/Risk_IT

Wikipedia, C. d. (s.f.). *Val IT*. Recuperado el 28 de 10 de 2014, de http://es.wikipedia.org/wiki/Val_IT

Wordreference. (s.f.). *Alcance*. Recuperado el 26 de 10 de 2014, de Wordreference: <http://www.wordreference.com/definicion/alcance>

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR:

Jenny Cumandá Razo Tapia

**DIRECTOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS E
INFORMÁTICA**

Ing. Mauricio Campaña Ortega MSc.

Sangolquí, Marzo de 2015