Implementación integrada de marcos GTI

COBIT ® constituye la perspectiva Top Down del GTI o Gobierno de TI e ITIL V3 ®, ISO 27001 ®, PMBOK ® y otros la perspectiva Bottom Up. Este artículo describe un estilo de implementación integrada de los marcos de referencia que constituyen las perspectivas Top Down y Bottom Up del GTI.

Tania Barrera R.
Sergio Borja B.
Jorge Barrera N.

I. Modelo de perspectivas top down / bottom up del GTI

El modelo de perspectivas Top Down y Bottom Up del GTI o Gobierno de TI tratado en este artículo se deriva del alineamiento que COBIT 4.1 como marco sombrilla hace a los marcos de referencia ITIL V3 e ISO/IEC 27002. Este alineamiento es definido en [7] por el ITGI y la OGC.

Implementar el GTI implica definir y desarrollar sus Perspectivas Top Down y Bottom Up. La perspectiva Top Down la constituyen los 34 procesos COBIT y sus 210 Objetivos de Control [8], mientras que para definir la perspectiva Bottom Up es necesario:

- Un análisis del alineamiento definido por el ITGI y la OGC orientado a definir criterios claros de puesta en práctica del alineamiento.

- La definición de los marcos de trabajo que constituyen la perspectiva.

- La identificación de todos los elementos o entregables que constituyen la perspectiva.

La Figura 1 presenta el análisis del alineamiento, con una definición de casos propia del rol que juegan los marcos de referencia ITIL [13] e ISO [4] alineados.

ANÁLISIS DE CASOS EN EL ALINEAMIENTO DE COBIT 4.1 A ITIL V3 E ISO/IEC 27002 DEFINIDO POR EL ITGI Y LA OGC EN [7]				
EJEMPLO DE OBJETIVO DE CONTROL COBIT 4.1	CASO	INFORMACIÓN DE SOPORTE ITIL V3	INFORMACIÓN DE SOPORTE ISO/IEC 27002 - 2005	TOTAL
PO4.1 Marco de trabajo . . . de TI	1	**Primario** con elementos básicos ITIL V3	N.A.	29
PO4.5 Estructura organizacional . . .	2	**Primario** con elementos básicos ITIL V3	Secundario	40
PO1.4 Plan Estratégico de TI	3	**Primario** sin elementos básicos	N.A.	2
PO5.3 Proceso presupuestal	4	**Primario** sin elementos básicos	Secundario	3
DS4.5 Pruebas plan de continuidad	5	**Primario** con / sin elementos básicos.	**Primario**.	7
ME1.5 Reportes al Consejo Directivo	6	Secundario	N.A.	31
DS4.10 Revisión post reanudación	7	Secundario	Secundario	25
DS5.2 Plan de seguridad de TI	8	Secundario	**Primario**	19
ME3.5 Reportes Integrados	9	N.A	N.A.	18
DS5.11 Intercambio d datos sensitivos	10	N.A.	**Primario**	9
PO3.5 Consejo y Arquitectura de TI	11	N.A.	Secundario	27
			Total de Objetivos de Control COBIT	210
OBSERVACIONES:				
1. Los 104 Objetivos de Control COBIT que reciben aportes **Primarios** de elementos básicos ITIL V3 (**63**) y/o de Controles ISO/IEC 27002 (**112**) se implementan de ***manera indirecta*** mediante la implementación de los elementos y controles que los soportan. Casos 1, 2, 5, 8 y 10.				
2. Se implementan ***directamente*** los 63 elementos básicos ITIL V3 (4 Funciones, 30 Actividades y 29 Procesos) pues todos hacen aportes **Primarios**				
3. Se implementan de ***manera directa*** 112 controles ISO/IEC 27002 que hacen aportes **Primarios** a Objetivos de Control COBIT				
4. Se implementan de ***manera directa*** 106 Objetivos de Control COBIT que no reciben aportes **Primarios** ni de elementos básicos ITIL V3 ni de ISO/IEC 27002. Estas implementaciones aprovechan los correspondientes aportes *Secundarios* y **Primarios no básicos** de ITIL V3 y los *Secundarios* de 21 Controles ISO/IEC 27002. Entonces la suma de los casos 3, 4, 6, 7, 9 y 11 deberá ser 106.				

Figura 1. Análisis del alineamiento de COBIT 4.1 a ITIL V3 y a ISO/IEC 27002

La Figura 2 concreta el Modelo de Perspectivas Top Down Bottom Up propuesto por SGSISA [3]. En ella aparecen PMBOK [14] del PMI y la opción de incorporar otros marcos de referencia.

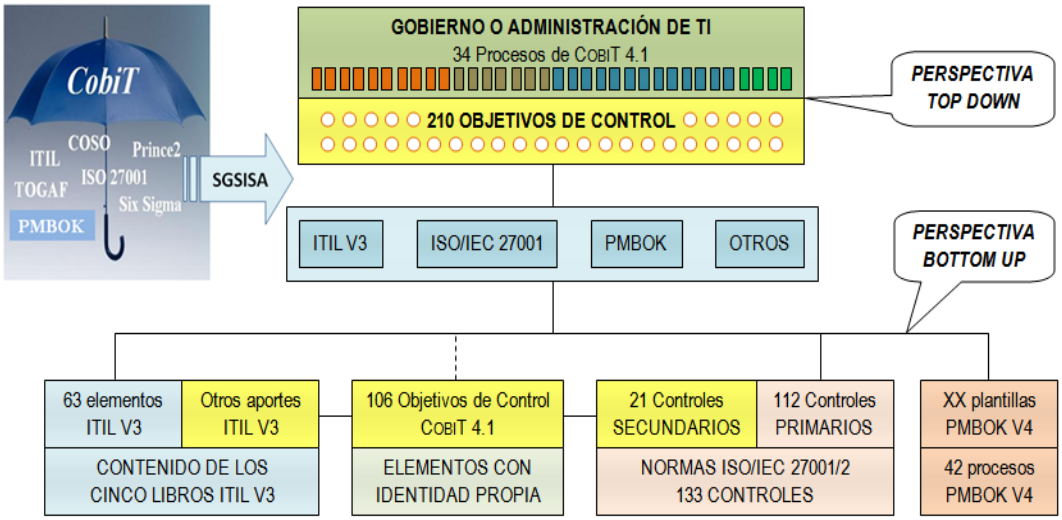

Figura 2. Modelo de Perspectivas basado en el alineamiento de COBIT a otros marcos de referencia

En la figura se observa que la Perspectiva Bottom Up comprende básicamente los siguientes elementos de los marcos de referencia allí identificados:

- 4 Funciones ITIL V3
- 30 Actividades ITIL V3
- 29 Procesos ITIL V3
- 112 Controles primarios ISO/IEC 27001
- 106 Objetivos de Control COBIT sin aportes primarios de ITIL ni de ISO
- XX Plantillas de Procesos y otros elementos PMBOK

Los elementos que conforman estos grupos se relacionan en un formulario como el ilustrado en la Figura 3.

ELEMENTOS A IMPLEMENTAR		MARCO DE TRABAJO					PRIORIZACION Y PLANES DE IMPLEMENTACION						
		ITIL V3			CTL ISO	COBIT OTRO	NIVEL DE PRIORIDAD 1 A 10				C / M / L PLAZO - MESES		
CODIGO	NOMBRE DESCRIPTIVO	F	A	P			CRE	Q.S.	S. B.	TOT.	1 a 6	7 a 12	13 a 24
	Se registran documentos de: • 4 Funciones ITIL V3 • 30 Actividades ITIL V3 • 29 Procesos ITIL V3 • 112 Controles IS/IEC 27001 • 106 Objetivos de Control COBIT • Otros												
OBSERVACIONES													
1. CRE significa Cumplimiento Regulatorio							3. SB Significa Security Base Line de COBIT						
2. QS significa Quick Start de COBIT							4. Los Criterios de Prioridad los adecúa cada organización						

Figura 3. Formulario Lista de elementos GTI y prioridad de implementación

La versión Quick Start se define en [10] y la Security Baseline en [11].

II. Implementación de la perspectiva bottom up

Los elementos identificados en la Figura 3 se desarrollan y ponen marcha como soporte de los Objetivos de Control COBIT que los alinean, según los casos definidos en la Figura 1, a los que apliquen. Para cada caso estos elementos deberán cumplir los siguientes requerimientos:

- ***Caso 1***. Los elementos básicos ITIL V3 asociados al Objetivo de Control COBIT serán su único soporte. Por tanto deberán integrar otros aportes **primarios** que haga ITIL V3 al Objetivo de Control COBIT.

- ***Caso 2***. Los elementos básicos ITIL V3 asociados al Objetivo de Control COBIT serán su único soporte. Por tanto deberán integrar los aportes *secundarios* que haga ISO/IEC 27002 al Objetivo de Control COBIT.

- ***Caso 3***. El Objetivo de Control deberá ser implementado con identidad propia y deberá integrar todos los aportes **primarios no básicos** que le hace ITIL.

- ***Caso 4***. El Objetivo de Control deberá ser implementado con identidad propia y deberá integrar todos los aportes **primarios no básicos** que le hace ITIL, si los hay, y además deberá integrar los aportes *secundarios* de ISO/IEC 27001.

- ***Caso 5***. Los elementos básicos ITIL V3 asociados al Objetivo de Control COBIT deberán integrar si los hay otros aportes **primarios** que haga ITIL V3. Los controles ISO/IEC asociados deberán hacer su aporte primario.

- ***Caso 6***. El Objetivo de Control deberá ser implementado con identidad propia y deberá integrar todos los aportes *secundarios* que le hace ITIL.

- ***Caso 7***. El Objetivo de Control deberá ser implementado con identidad propia y deberá integrar todos los aportes *secundarios* que le hace ITIL y además deberá integrar los aportes *secundarios* de ISO/IEC 27001.

- ***Caso 8***. Los controles ISO/IEC 27002 asociados al Objetivo de Control COBIT serán su único soporte. Por tanto deberán integrar los aportes *secundarios* que hace ITIL V3 al Objetivo de Control COBIT.

- ***Caso 9***. El Objetivo de Control deberá ser implementado con identidad propia sin aporte alguno por parte de ITIL V3 e ISO 27002. Se deberá entonces acudir a otros marcos de trabajo alineados, como PMBOK.

- ***Caso 10***. Los Controles ISO/IEC 27002 asociados al Objetivo de Control COBIT serán su único soporte.

- ***Caso 11***. El Objetivo de Control deberá ser implementado con identidad propia y deberá integrar todos los aportes *secundarios* que le hace ISO/IEC 27002.

Cada elemento básico ITIL V3 y cada control primario ISO 27001 puede ser soporte de varios Objetivos de Control COBIT a la vez. PMBOK [14] aplica al proceso PO10 de COBIT. Todos los casos 1 a 11 deberán tener en cuenta las Prácticas de Control de COBIT [9] y las Guías de Aseguramiento [12[.

III. Implementación de la perspectiva top down

El GTI como caso de negocio se define en [5]. La gestión de la perspectiva TOP DOWN comprende la gestión de cada uno de los 34 procesos COBIT 4.1 y la gestión de los 210 Objetivos de Control, temas tratados a continuación.

III.1 Gestión de los procesos COBIT

La Figura 4 muestra la tabla de contenido del formulario ***Hoja de Vida de un Proceso***, cuyo primer uso completo se da en el proceso GAP COBIT 4.1.

TABLA DE CONTENIDO		
	COMPONENTE DE LA HOJA DE VIDA DEL PROCESO COBIT 4.1	HOJA EN ESTE DOCUMENTO
1	Descripción del proceso	PAG_1_DESC
2	Propietario y entorno	PAG_2_PROP
3	Historia del documento	PAG_3_HDED
3.1	Compromiso de confidencialidad	
4	Tabla de contenido	PAG_4_TDEC
5	Declaración de aplicabilidad	PAG_5_ODEC
5.1	Elementos implementadores	
6	Evaluación de estado de las entradas al proceso	PAG_6_ENTR
7	Evaluación de estado de las salidas del proceso	PAG_7_SALI
8	Evaluación de estado de las actividades del proceso	PAG_8_ACTI
9	Evaluación del schedule o actividades del día a día generadas por el proceso	Integrado para todos los procesos
9.1	Sección 1/3 Registro de la operación generada por el Gobierno de TI	Integrado para todos los procesos
9.2	Sección 2/3 Descripción de las anomalías y plan de acción	Integrado para todos los procesos
9.3	Sección 3/3 Identificación y cronograma de las acciones preventivas y correctivas	Integrado para todos los procesos
10	Evaluación de los niveles de aplicación de las *prácticas de control* del proceso	PAG_10_PCPR
11	Evaluación de los niveles de aplicación de las *guías de aseguramiento*	PAG_11_GAPR
12	Evaluación de los niveles de las métricas del proceso	
12.1	Evaluación de las métricas de las actividades del proceso	PAG_12_MTRP
12.2	Evaluación de las métricas específicas del proceso	PAG_12_MTRP
12.3	Evaluación de las métricas TI asociadas al proceso	PAG_12_MTRP
13	Evaluación de las metas del negocio y TI asociadas al proceso	
13.1	Evaluación de las metas de las actividades del proceso	PAG_13_META
13.2	Evaluación de las metas específicas del proceso	PAG_13_META
13.3	Evaluación de las metas TI asociadas al proceso	PAG_13_META
13.4	Evaluación de las metas del negocio asociadas al proceso	PAG_13_META
14	Cálculo del nivel de madurez del proceso	PAG_14_CANM
15	Evolución del nivel de madurez del proceso	PAG_15_NMAD
16	Evaluación de las *guías de aseguramiento* de los controles genéricos	PAG_16_GAGE
17	Evaluación de las *prácticas de control* de los controles genéricos	PAG_17_PCGE
18	Evaluación para el proceso de los controles genéricos de procesos COBIT 4.1	PAG_18_CGEN

Figura 4. Tabla de Contenido de la Hoja de Vida de un Proceso COBIT

El registro oportuno de los elementos implementadores en la PAG_5_ODC y los procesos de las páginas de evaluación generan la *actualización en tiempo real* en la PAG_14_CANM del Nivel de Madurez del proceso.

III.2 Registro de implementación de Objetivos de Control COBIT

La Figura 5 corresponde a la PAG_5_ODC relacionada en la Figura 4. En ella se define la Declaración de Aplicabilidad del GTI y se registra a nivel Objetivo de Control el soporte provisto por los documentos identificados en la Figura 3.

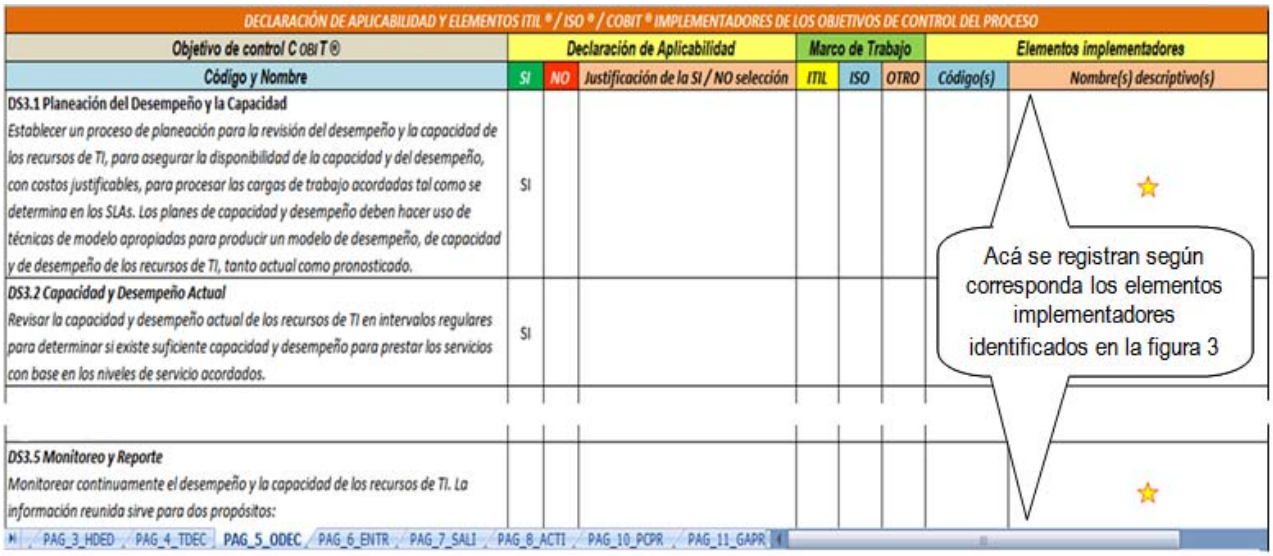

Figura 5. Registro de los elementos implementadores de los Objetivos de Control COBIT

El registro de elementos y la Declaración de Aplicabilidad deben ser acordes.

IV. Guías complementarias para la implementación del GTI

A continuación se ilustran otras buenas prácticas para implementar el GTI.

IV.1 Formulación de códigos de documentos - Ejemplos

La Figura 6 ilustra la asignación sugerida de códigos para elementos ITIL V3.

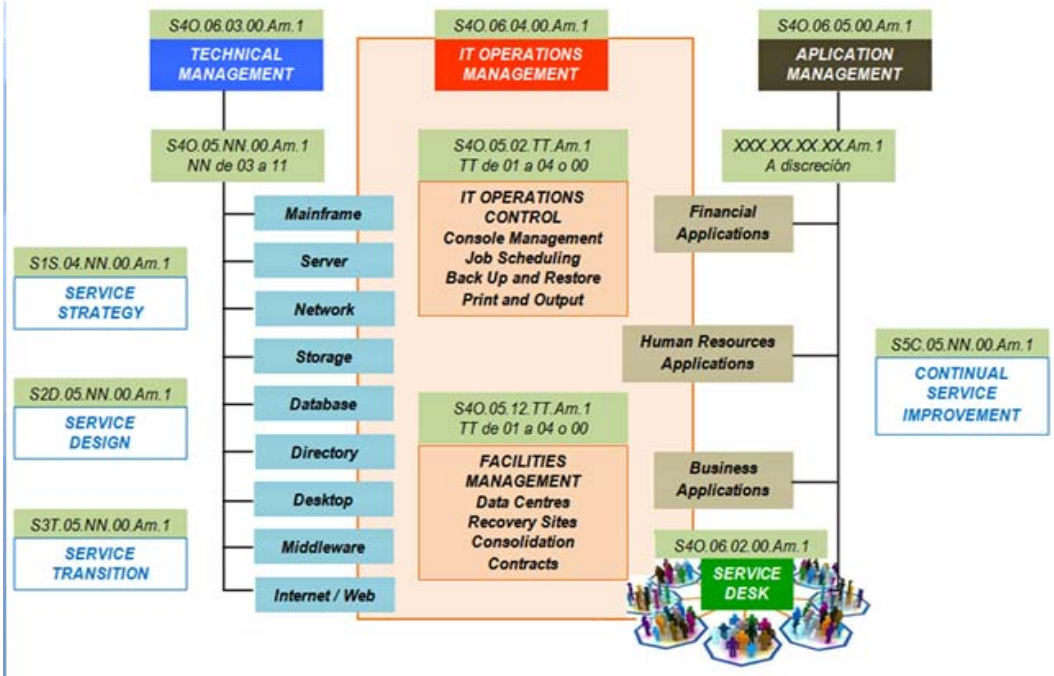

Figura 6. Formulación de códigos de las Funciones Actividades y Procesos ITIL V3

IV.2 Guías para la implementación de procesos ITIL V3 al estilo COBIT 4.1

La Figura 7 muestra la asignación de términos del glosario de ITIL a un proceso ITIL V3 [13]. SGSISA construye la matriz con soporte automatizado.

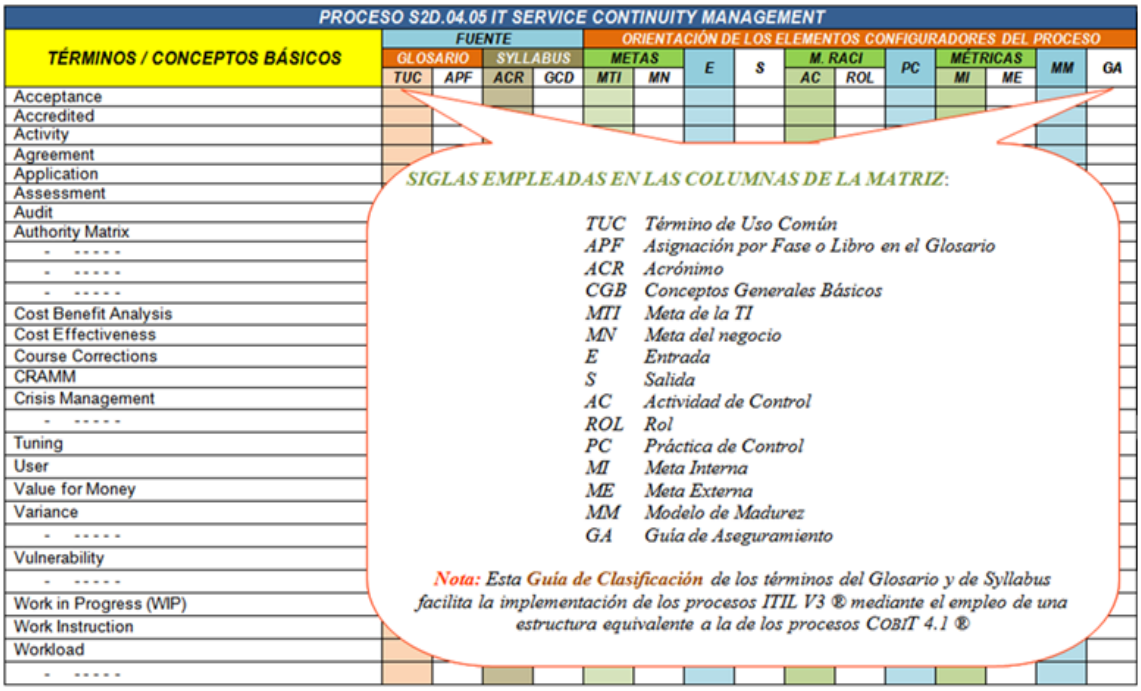

Figura 7. Fragmento de la asignación alineada de términos del glosario a un proceso ITIL V3

Esta asignación permite definir el proceso ITIL V3 en términos ITIL V3 con una estructura lógica análoga a la de los procesos COBIT, lo cual fortalece aún más el alineamiento entre estos dos marcos de trabajo.

IV.3 Guías para la implementación de elementos ISO/IEC 27002

La metodología de SGSISA [1] / [2] / [3] propone implementar cada Objetivo de Control ISO 27001 [4] con una estructura análoga a la propuesta para los procesos ITIL V3, es decir, alineada con la estructura de procesos COBIT [6]. Para cada Control ISO/IEC 27001 SGSISA define un conjunto de Actividades de Control a ser implementadas de manera individual o por grupos. La estructura del código identificador de documentos es clave en estos procesos.

V. Conclusiones y expectativas

Este artículo es eminentemente práctico. Para su comprensión no se requiere capacitación previa en los temas tratados.

La manera de entender estos temas es aplicar la ***Estrategia Aprender Haciendo***.

Esta estrategia aplica a otros marcos de trabajo relacionados tales como el PMBOK [14] del PMI para la gestión de proyectos.

Los datos de implementación de los marcos de referencia son parte de la Base de Datos del Conocimiento del GTI, que soporta la evolución a nuevas versiones, como la propuesta en [6] para COBIT 5.

Siglas empleadas

COBIT ® Control Objectives for Information and related Technology
CGEIT ® Certified in the Governance of Enterprise IT
CISA ® Certified Information Systems Auditor
CRISC ® Certified in Risk and Information Systems Control
ICONTEC ® Instituto Colombiano de Normas Técnicas y Certificación
IEC ® International Electrotechnical Commission
ISACA ® Information System Audit and Control Association
ISO ® International Organization for Standardization
ITGI ® IT Governance Institute
ITIL ® IT Infrastructure Library
OGC ® Office of Government Commerce
PMBOK ® Project Management Body of Knowledge
PMI ® Project Management Institute
PMP ® Certified as Project Management Professional
SGSISA ® Sistema de Gestión de Servicios Informáticos Soporte Automatizado
WBS ® Work Breakdown Structure

Referencias

[1] Barrera N. Jorge, Computer-assisted Implementation of ITSM Using COBIT 4.1, COBIT Focus July, 2009, *http://www.isaca.org/cobitnewsletter*.

[2] Barrera N. Jorge, Metodología de Implementación Integrada con Soporte Automatizado de COBIT ® ITIL V3 ® ISO 27001/2 ® PMBOK ®, ISACA VI Jornadas Académicas Bogotá, Octubre de 2010, *http://www.isaca-bogota.net/Descargas*.

[3] Barrera R. Tania y Barrera N. Jorge, www.sgsisa.com, 2008.

[4] ICONTEC ®, Normas ISO 27001/X / ISO 20000 / ISO 38500.

[5] ISACA ®, Building the Business Case for COBIT ® and Val IT Executive Briefing.

[6] ISACA ®, COBIT 5 Design Paper Exposure Draft, 2010.

[7] ITGI ® & OGC ®, Alineando COBIT ® 4.1, ITIL ® V3 e ISO/IEC 27002 en Beneficio del Negocio. Un reporte para gestión del ITGI y la OGC, 2009.

[8] IT Governance Institute ®, COBIT ® 4.1, 2007.

[9] IT Governance Institute ®, COBIT ® Control Practices, 2nd Edition, 2007.

[10] IT Governance Institute ®, COBIT ® Quick Start, 2Nd Edition, 2007.

[11] IT Governance Institute ®, COBIT ® Security Baseline, 2007.

[12] IT Governance Institute ®, IT Assurance Guide Using COBIT ®, 2007.

[13] Office of Government Commerce ®, ITIL Version 3 Service Strategy / Service Design / Service Transition / Service Operation / Continual Service Improvement, 2007.

[14] PMI ® Project Management Institute ®, Guía de los Fundamentos para la Dirección de Proyectos, Cuarta Edición, 2009.

Tania Barrera R: *Ingeniera de Sistemas. Certificada PMP, ITIL V3 y COBIT Foundations. Adelanta Especialización en Gerencia de Proyectos. Líder de Proyecto en IBM y ahora en el IDEAM. Coautora de www.sgsisa.com.*

Sergio Borja B: *Ingeniero de Sistemas. Maestría en Ciencias de la Ingeniería. Certificación CISA (En proceso post aprobación examen), CRISC, ITIL V3, COBIT Foundations, ISO 27001 Auditor Interno. Auditor de Sistemas y Líder de Proyecto en Presidencia de la República y ahora asesor asociado al Proyecto SGSISA. Idiomas Inglés, Portugués, Coreano y Español.*

Jorge Barrera N: *Magister en Ingeniería de Sistemas. Certificación CISA (En proceso post aprobación examen), CGEIT, CRISC, COBIT Foundations y SAP R3 Auditor. Entrenado como Auditor ISO27001. Consultor en GTI adscrito a Digiware de Colombia. Coautor de www.sgsisa.com. Ex Profesor en Programas de Magíster.*