1.4.6. Objetivos de Control para la Información y la Tecnología relacionada (COBIT, Control Objectives for Information and related Technology)

Es una herramienta de las Tecnologías de la Información, lanzada en 1996, que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

El marco de trabajo COBIT se basa en el principio de la figura 1.4, proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información. El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio. (COBIT4.0, 2006)

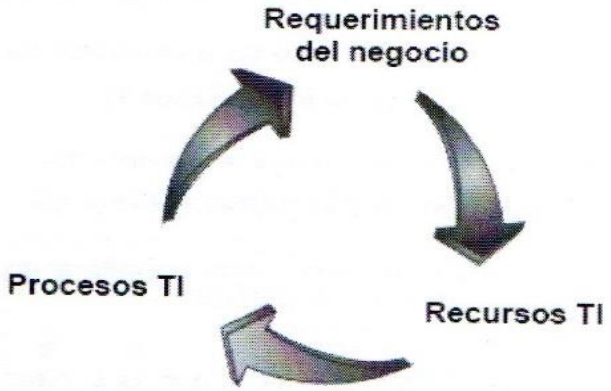

Figura 1.4: Principio de funcionamiento de COBIT. [Fuente: COBIT4.0, 2006]

A continuación se relacionan algunos elementos que describen y caracterizan a COBIT (COBIT4.0, 2006):

Usuarios

La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

Los Responsables de TI: para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Características

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

Recursos de TI necesarios para alcanzar los objetivos de negocio

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (ej., implementando una cadena de suministro) que genere el resultado deseado (ej., mayores ventas y beneficios financieros). (Colectivo, 2005)

Recursos de TI identificados en COBIT

- Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La información son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.
- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

Estructura

COBIT se divide en tres niveles:

- Dominios
- Procesos
- Actividades

Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control. Actividades: Acciones requeridas para lograr un resultado medible.

Dominios

1. *Planeación y Organización:* Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.
2. *Adquisición e Implementación:* Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
3. *Entrega y Soporte:* En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
4. *Monitoreo:* Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Medición del Desempeño

COBIT utiliza dos tipos de métrica: indicadores de metas e indicadores de desempeño. Los indicadores de metas de bajo nivel se convierten en indicadores de desempeño para los niveles altos. (Champlain 2003)

Se tiene que tener claro que COBIT ofrece un marco de referencia genérico para la gestión TI, pero no cubre en profundidad aspectos concretos de las TI como son la calidad, la seguridad de la información, la gestión de servicios o la gestión de proyectos. Para estos casos concretos se debe recurrir a metodologías específicas, pero tratando de que encajen, sin forzarlo, en el marco general de COBIT. (Sudhanshu, 2004)

Los beneficios de implementar COBIT como marco de referencia para la gestión de las TI incluyen:

- Mejor alineación, con base en su enfoque de negocios.

- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores.
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común.

Relación de COBIT con diferentes metodologías

A modo de orientación (Narbona 2, 2006) sugiere dónde pueden encajar las distintas metodologías, estándares y buenas prácticas, analizando los 4 dominios de COBIT. El Anexo 1 muestra la relación entre COBIT y otras metodologías (no se detallan los procesos correspondientes en las otras metodologías, sólo se indica que existe relación con algún proceso o control descrito en las otras metodologías) para cada proceso TI de COBIT. La relación indicada no implica que se pueda sustituir el proceso TI de COBIT por el de la metodología correspondiente, ni tampoco que la metodología correspondiente cubra completamente el proceso TI de COBIT con el que está relacionado.

Anexo 1: Relación de COBIT con otras metodologías. [Fuente: (Narbona 2, 2006)]

CD	DOMINIO		OTRAS METODOLOGÍAS, ESTÁNDARES Y BUENAS PRACTICAS
	CP	Proceso	
PO	PLANIFICACIÓN Y ORGANIZACIÓN		
	1.0	Definición del Plan Estratégico TI	IT BSC
	2.0	Definición de la Arquitectura de Información	
	3.0	Determinación de la Dirección Tecnológica	
	4.0	Definición de la Organización y de las Relaciones TI	
	5.0	Gestión de la Inversión TI	ITIL
	6.0	Comunicación de los Objetivos y Aspiraciones de la Gerencia	
	7.0	Gestión de Recursos Humanos	
	8.0	Gestión de Calidad	ISO 9000
	9.0	Análisis y Gestión de Riesgos TI	MAGERIT V2, ISO 17799, ISO 27001
	10.0	Gestión de Proyectos	PRINCE2
AI	ADQUISICIÓN E IMPLEMENTACIÓN		
	1.0	Identificación de Soluciones Automatizadas	CMMI
	2.0	Adquisición y Mantenimiento de Software de Aplicación	CMMI
	3.0	Adquisición y Mantenimiento de la Infraestructura Tecnológica	ITIL
	4.0	Habilitar la operación y el uso de los SI	CMMI
	5.0	Procurar los recursos TI	PRINCE2
	6.0	Gestión de Cambios	ITIL
	7.0	Instalación y Acreditación de Soluciones y Cambios	ITIL
DS	ENTREGA DE SERVICIOS Y SOPORTE		
	1.0	Definición y Gestión de Niveles de Servicio	ITIL
	2.0	Gestión de Servicios prestados por Terceros	
	3.0	Gestión del Desempeño y Capacidad	ITIL
	4.0	Aseguramiento de Servicio Continuo	ITIL
	5.0	Garantizar la Seguridad de Sistemas	ISO/IEC 17799
	6.0	Identificación y Asignación de Costos	ITIL
	7.0	Educación y Entrenamiento de Usuarios	
	8.0	Gestión del Service Desk y de los Incidentes	ITIL
	9.0	Gestión de la Configuración	ITIL
	10.0	Gestión de Problemas	ITIL
	11.0	Gestión de Datos	
	12.0	Gestión del Entorno Físico (Instalaciones)	
	13.0	Gestión de Operaciones	
ME	MONITORIZACIÓN Y EVALUACIÓN		
	1.0	Monitorización y Evaluación de la Ejecución	IT BSC
	2.0	Monitorización y Evaluación del Control Interno	
	3.0	Aseguramiento del Cumplimiento de la Normativa	
	4.0	Proveer el Gobierno TI	IT BSC
CD: Código de Dominio			CP: Código de Proceso