capítulo 9

COBIT

Manuel Ballester Fernández

Universidad de Deusto

9.1. Introducción

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- la creciente dependencia en información y en los sistemas que proporcionan dicha información
- la creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información (*information warfare*).
- la escala y el costo de las inversiones actuales y futuras en información y en tecnología de información;
- el potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos y críticos de la empresa.

Las organizaciones exitosas comprenden y administran los riesgos asociados con la implementación de nueva tecnología

Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos *Mainframe*. Por lo tanto, la administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega) al tiempo que demanda que esto se realice a un costo más bajo. Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

COBIT ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona "prácticas sanas" a través de un Marco Referencial de dominios y procesos y presenta actividades en una estructura manejable y lógica. Las mejores prácticas de COBIT representan el consenso de los expertos (le ayudarán a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo usted será evaluado si las cosas salen mal.

Las organizaciones deben cumplir con requerimientos de calidad, de reportes fiduciarios y de seguridad, tanto para su información, como para sus activos. La administración deberá obtener un balance adecuado en el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la administración deberá establecer un sistema adecuado de control interno. Por lo tanto, este sistema o marco referencial deberá existir para proporcionar soporte a los procesos de negocio y debe ser preciso en la forma en la que cada actividad individual de control satisface los requerimientos de información y puede impactar a los recursos de TI. El impacto en los recursos de TI es enfatizado en el Marco Referencial de COBIT conjuntamente a los requerimientos de información del negocio que deben ser alcanzados: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

La administración, mediante este gobierno corporativo (*corporate governance*), debe asegurar que la debida diligencia sea ejercitada por todos los individuos involucrados en la administración, empleo, diseño, desarrollo, mantenimiento u operación de sistemas de información.

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI.

Los recursos de TI deben ser administrados por un conjunto de procesos de TI, agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos

La orientación a negocios es el tema principal de COBIT. Esta diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, esta diseñado para ser utilizado como una lista de verificación (*check list*) detallada para los propietarios de los procesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y otorgamiento de autoridad (*Empowerment*) de los dueños de procesos para que estos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados. El Marco Referencial de COBIT proporciona herramientas al propietario de procesos de negocio que facilitan el cumplimiento de esta responsabilidad. El Marco Referencial comienza con una premisa simple y práctica: Los recursos de TI deben ser administrados por un conjunto de procesos de TI, agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos (Figura 9.1.).

Continúa con un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios: planificar y organizar, entregar y dar soporte y monitorizar y evaluar. Esta estructura cubre todos los aspectos de información y de la tecnología que la soporta. Dirigiendo estos 34 Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información. Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría o de aseguramiento que permite la revisión de los procesos de TI contra los 302 objetivos detallados de control recomendados por COBIT para proporcionar a la Gerencia la certeza de su cumplimiento y/o una recomendación para su mejora. COBIT contiene un conjunto de herramientas de implementación que proporciona lecciones aprendidas por empresas que rápida y exitosamente aplicaron COBIT en sus ambientes de trabajo. Incluye un Resumen Ejecutivo para el entendimiento y la sensibilización de la alta gerencia sobre los principios y conceptos fundamentales de COBIT. La guía de implementación cuenta con dos útiles herramientas (Diagnóstico de Sensibilización Gerencial – *Management Awareness Diagnostic*– y Diagnóstico de Control en TI – *IT Control Diagnostic* –) para proporcionar asistencia en el análisis del ambiente de control en una organización.

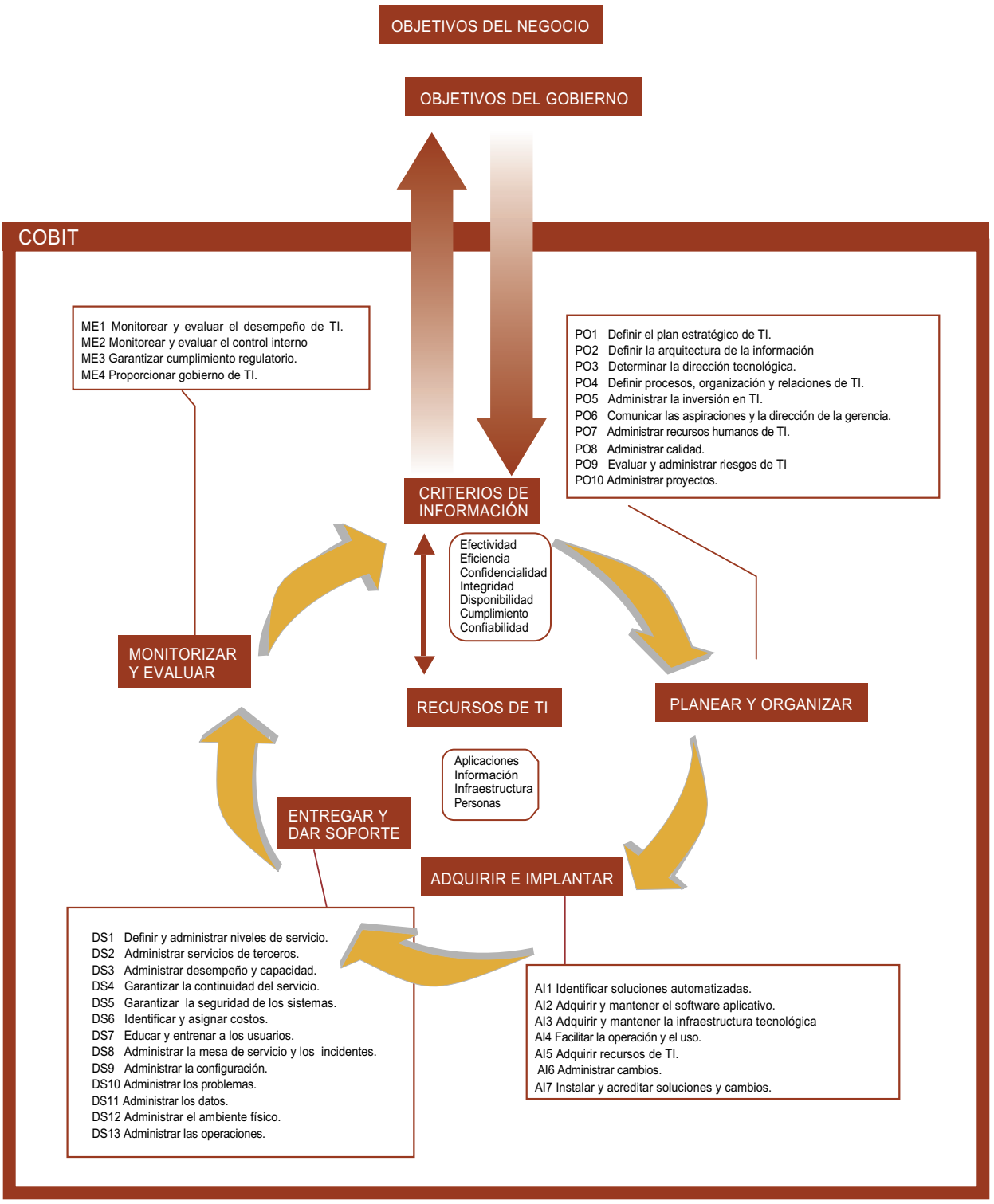
El Marco Referencial COBIT otorga especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el Marco Referencial proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con Tecnología de Información.

La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en TI para medir en forma comparativa (*Benchmark*) tanto su ambiente de TI existente, como su ambiente planeado. COBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio.

COBIT es una herramienta de gobierno de TI que ayuda a comprender y gestionar los riesgos asociados con las tecnologías de la información

COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de organizaciones, a nivel mundial. El objetivo de COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

Figura 9.1. Marco de referencia de COBIT



9.2. Desarrollo del Producto COBIT

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). –COBIT es la herramienta innovadora para el gobierno de TI (Governance. Término aplicado para definir un control total)–.

COBIT se fundamenta en los Objetivos de Control existentes de la *Information Systems Audit and Control Foundation* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicables y aceptados" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de *COBIT* ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

Se determinó que las mejoras a los *objetivos de control* originales debería consistir en:

- el desarrollo de un marco referencial para control en TI como fundamento para los objetivos de control en TI y como una guía para la investigación consistente en auditoría y control de TI;
- una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho; y
- una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en TI y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.) y
- una revisión crítica y actualización de las guías actuales para desarrollo de auditorías de sistemas de información.

Sin excluir ningún otro estándar aceptado en el campo del control de sistemas de información que pudiera emitirse durante la investigación, las fuentes han sido identificadas inicialmente como:

- **Estándares Técnicos** de ISO, EDIFACT, etc.
- **Códigos de Conducta** emitidos por el Council of Europe, OECD, ISACA, etc.;
- **Criterios de Calificación** para sistemas y procesos de TI: ITSEC, ISO9000, SPICE, IickIT, etc.;
- **Estándares Profesionales** para control interno y auditoría: reporte COSO, GAO, IFAC, IIA, ISACA, estándares CPA, etc.;
- **Prácticas y requerimientos de la Industria** de foros industriales (ESF, 14) y **plataformas patrocinadas** por el gobierno (IBAG, NIST, DTI); y
- **Nuevos requerimientos** específicos de la industria de la banca y manufactura de TI.

9.3. El Marco Referencial de COBIT

9.3.1. Orientación a objetivos de negocio

El objetivo principal de *COBIT* es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es el desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. Esto concuerda con la perspectiva COSO, que

Tabla 9.1. Definición de Control y Objetivo de Control

Control se define como	Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.
Objetivo de control en TI se define como	Una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

constituye el primer y mejor marco referencial para la administración en cuanto a controles internos. Posteriormente, los objetivos de control fueron desarrollados a partir de la perspectiva de los objetivos de auditoría (certificación de información financiera, certificación de medidas de control interno, eficiencia y efectividad, etc.)

Los Objetivos de Control muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoría. Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Se proporcionan consideraciones y guías para definir e implementar el Objetivo de Control de TI.

La clasificación de los dominios a los que se aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los requerimientos de negocio para la información en ese dominio, así como los recursos de TI que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el marco Referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 302 objetivos detallados de control. El Marco Referencial fue mostrado a la industria de TI y a los profesionales dedicados a la auditoría para abrir la posibilidad a revisiones, dudas y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

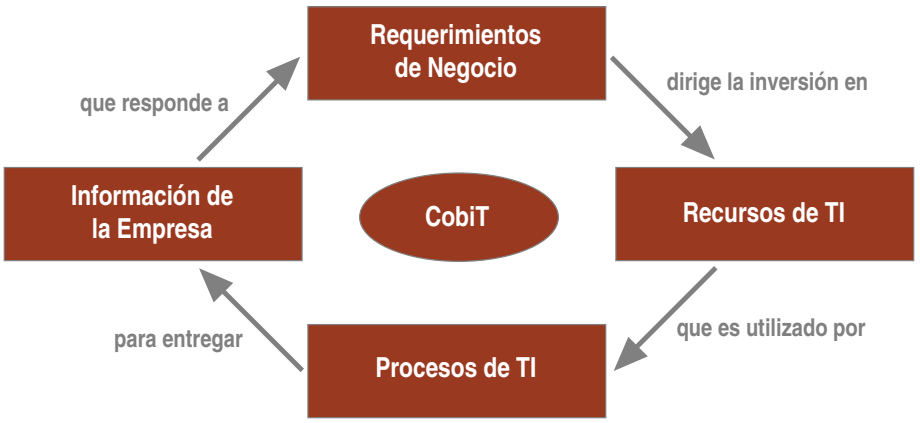
9.3.2. Definiciones

Para propósitos de este proyecto, se proporcionan las siguientes definiciones (Tabla 9.1.). La definición de "Control" está adaptada del reporte *COSO [Committee of Sponsoring Organisations of the Treadway Commission. Internal Control-Integrated Framework*, 1992 y la definición para "Objetivo de Control de TI" ha sido adaptada del reporte SAC (*Systems Auditability and Control Report). The Institute of Internal Auditors Research Foundation*, 1991 y 1994.

9.3.3. Principios del Marco Referencial

Existen dos clases distintas de modelos de control disponibles actualmente, aquéllos de la clase del "modelo de control de negocios" (por ejemplo COSO) y los "modelos más enfocados a TI" (por ejemplo, DTI). *COBIT* intenta cubrir la brecha que existe entre los dos. Debido a esto, COBIT se posiciona como una herramienta más completa para la Administración y para operar a un nivel superior que los estándares de tecnología para la administración de sistemas de información.

Figura 9.2. COBIT satisface los objetivos de negocio



Por lo tanto, COBIT es el modelo para el gobierno de TI.

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI (Figura 9.2.).

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como *requerimientos de negocio para la información*. Al establecer la lista de requerimientos, *COBIT* combina los principios contenidos en los modelos referenciales existentes y conocidos (Tabla 9.2.).

La Calidad ha sido considerada principalmente por su aspecto 'negativo' (no fallas, confiable, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo, atractivo, "ver y sentir –*look and fee*l–", desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la Calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega (de servicio) de la Calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el Costo es también considerado que queda cubierto por Eficiencia.

Para los requerimientos fiduciarios, COBIT no intentó reinventar le rueda –se utilizaron las definiciones de COSO para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones–. Sin embargo, confiabilidad de información fue ampliada para incluir toda la información –no solo información financiera.

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, fue descubierto que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas (Tabla 9.3.).

Los recursos de TI identificados en COBIT pueden identificarse/definirse como se muestra en la Tabla 9.4.

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización –y no la “jerga (*jargon*)” del auditor–. Por lo tanto, cuatro grandes

Tabla 9.2. Requerimientos de negocio para la información.

Requerimientos de calidad	Calidad Costo Entrega (de servicio)
Requerimientos Fiduciarios (COSO)	Efectividad & eficiencia de operaciones Confiabilidad de la información Cumplimiento de las leyes & regulaciones
Requerimientos de Seguridad	Confidencialidad Integridad Disponibilidad

Tabla 9.3. Criterios de calidad de la información de negocio

Efectividad	Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia	Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad	Se refiere a la protección de información sensible contra divulgación no autorizada.
Integridad	Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento	Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
Confiabilidad	de la información. 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.

Tabla 9.4. Recursos TI de COBIT

Datos	Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones	Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
Tecnología	La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones	Recursos para alojar y dar soporte a los sistemas de información.
Personal	Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Tabla 9.5. Dominios de COBIT

Planificar y Organizar	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.
Adquirir e Implementar	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.
Entregar y Dar 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.
Monitorizar y evaluar	Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitorizar y evaluar (Tabla 9.5.).

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos (Figura 9.3.).

Figura 9.3. Relación del mapa de procesos de COBIT con otras áreas.

		Áreas de enfoque de Gobierno TI					COSO					Recursos TI de CobiT				Criterios de Información de CobiT						
	IMPORTANCIA	Alineación estratégica	Entrega de valor	Administración de	Administración de	Medición del desempeño	Entorno de Control	Evaluación de riesgos	Actividades de control	Información y	Monitoreo	Aplicación	Información	Infraestructura	Personas	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar																						
PO1 Definir un plan estratégico de TI	A	P		S	S			P		S	S					P	S					
PO2 Definir la arquitectura de la información	B	P	S	P	S				P	P						S	P	S	P			
PO3 Determinar la dirección tecnológica	M	S	S	P	S			S	P	S						P	P					
PO4 Definir los procesos, organización y relaciones de TI	B	S		P	P		P			S	S					P	P					S
PO5 Administrar la inversión en TI	M	S	P	S		S		S	P							P	P					
PO6 Comunicar las aspiraciones y la dirección de la gerencia	M	P			P		P			P						P					S	
PO7 Administrar recursos humanos de TI	B	P		P	S	S	P			S						P	P					
PO8 Administrar la calidad	M	P	S		S		P		P	S	P					P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	A	P			P			P								S	S	P	P	P	S	S
PO10 Administrar proyectos	A	P	S	S	S	S	S	S	P		S					P	P					
Adquirir e implementar																						
AI1 Identificar soluciones automatizadas	M	P	P	S	S				P							P	S					
AI2 Adquirir y mantener software aplicativo	M	P	P		S				P							P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	B			P					P							S	P		S	S		
AI4 Facilitar la operación y el uso	B	S	P	S	S				P	S						P	P		S	S	S	S
AI5 Adquirir recursos de TI	M		S	P					P							S	P				S	
AI6 Administrar cambios	A		P	S				S	P		S					P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S					P	S		S	S		
Entregar y Dar Soporte																						
DS1 Definir y administrar los niveles de servicio	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	B		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3 Administrar el desempeño y la calidad	B	S	S	P	S	S			P		S					P	P			S		
DS4 Garantizar la continuidad del servicio	M	S	P	S	P	S	S		P	S						P	S			P		
DS5 Garantizar la seguridad de los sistemas	A				P				P	S	S							P	P	S	S	S
DS6 Identificar y asignar costos	B		S	P		S			P								P					P
DS7 Educar y entrenar a los usuarios	B	S	P	S	S		P			S						P	S					
DS8 Administrar la mesa de servicio y los incidentes	B		P			S	S			P	P					P	P					
DS9 Administrar la configuración	M		P	P	S				P							P	S			S		S
DS10 Administrar los problemas	M		P		S	S			P	S	S					P	P			S		
DS11 Administrar los datos	A		P	P	P				P										P			P
DS12 Administrar el ambiente físico	B			S	P			S	P										P	P		
DS13 Administrar las operaciones	B			P					P	S						P	P		S	S		
Monitorear y Evaluar																						
ME1 Monitorear y evaluar el desempeño de TI	A	S	S	S	S	P				S	P					P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	M		P		P						P					P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio	A	P			P				P	S	S										P	S
ME4 Proporcionar gobierno de TI	A	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

(P=Primario - S=Secundario)

9.4. Referencias

COSO (1994) *Control Interno—Marco de trabajo integrado*. Comité de organizaciones patrocinadoras de la Comisión Treadway.

COSO (2004) *Administración de riesgos empresariales—Marco de trabajo integrado*. Comité de organizaciones patrocinadoras de la Comisión Treadway.

ITIL (2004) *Biblioteca de infraestructura de TI® (ITIL®)*. Oficina de comercio gubernamental (OGC®).

ISO (2005) *ISO/IEC 17799:2005, Código de prácticas para la administración de la seguridad de la información*. Organización internacional para la estandarización.

CMM (1993) *SEI Modelo de madurez de la capacidad (CMM®)*. Instituto de Ingeniería de Software (SEI®).

CMMI (2000) *SEI Integración del modelo de madurez de la capacidad (CMMI®)*. Instituto de Ingeniería de Software (SEI®).

PMBOK (2000) *Cuerpo de conocimiento de administración de proyectos (PMBOK®)*. Instituto de administración de proyectos (PMI®).

ISF (2003) *El estándar de buenas prácticas para la seguridad de la información*. Foro de seguridad de información (ISF)

ISACA (2009) COBIT 4.1. ISACA.

ITGI (2009) *ITGI facilita la adopción de ISO38500*. Traducción al español por Cátedra de Buen Gobierno Universidad Deusto

sobre el Autor

Manuel BALLESTER FERNÁNDEZ
Universidad de Deusto

Actualmente

- Consejero Delegado de TEMANOVA Consulting
- Socio de ALINTEC International (Alianza Internacional de Buen Gobierno)
- Socio de AUREN
- Director de Postgrados de MAIN Escuela de Negocios de la Universidad de Deusto
- Director de la Cátedra de Buen Gobierno de la Universidad de Deusto
- Director del Máster de Buen Gobierno de la Universidad de Deusto, acreditado por ISACA.
- Miembro del SC7/GT 25 de AENOR.
- Vicepresidente del AEN/CTN 66/SC 1/GT 14
- Miembro del GCEIT Board Committee de ISACA
- Coeditor en el JTC1/WG6 IT-Governance (ISO 38500)
- Miembro del IEEE

- Doctor Ingeniero industrial Universidad Politécnica Valencia 1980
- MBA. IDE CESEM - 1994
- Posee las certificaciones CISA (Auditor Certificado en Sistemas de Información), CISM (Director Certificado en Seguridad de la Información), CGEIT (Corporate Governance Enterprise IT) y Cobit traineer acreditated de ISACA.
- Presidente Fundador del capítulo de ISACA Madrid.
- Cuenta con más de 30 años de experiencia. Es consejero de diversas organismos públicos y privados en cuestiones relacionadas con la implantación y el desarrollo de estándares y políticas TIC, COSO, IT-Governance, ITIL, ISO 20000, ISO 27000, ISO 38500, BS 25999, ISO 31000 análisis y gestión de riesgos tecnológicos, evaluaciones de controles, gestión de niveles de servicio, protección de datos, gestión de incidentes, planes de continuidad de negocio, gestión de proyectos, asesoría de seguridad y Planes estratégicos TIC.