



Introducción a Cobit 5

Julio R. Jolly Moore

CRMA, CFE, CRISC, CGEIT, Internal Audit Quality Assessment



Progress Through Sharing



Instituto de Auditores
Internos de Panamá

Agenda

1. ¿Qué es Cobit?
2. Estructura de Cobit 5
3. Habilitadores de Cobit 5
4. Ejemplo de evaluación de procesos de Cobit 5
5. Relación de Cobit 5 con COSO III

¿Qué es Cobit 5?



Progress Through Sharing



Instituto de Auditores
Internos de Panamá

Cobit 5



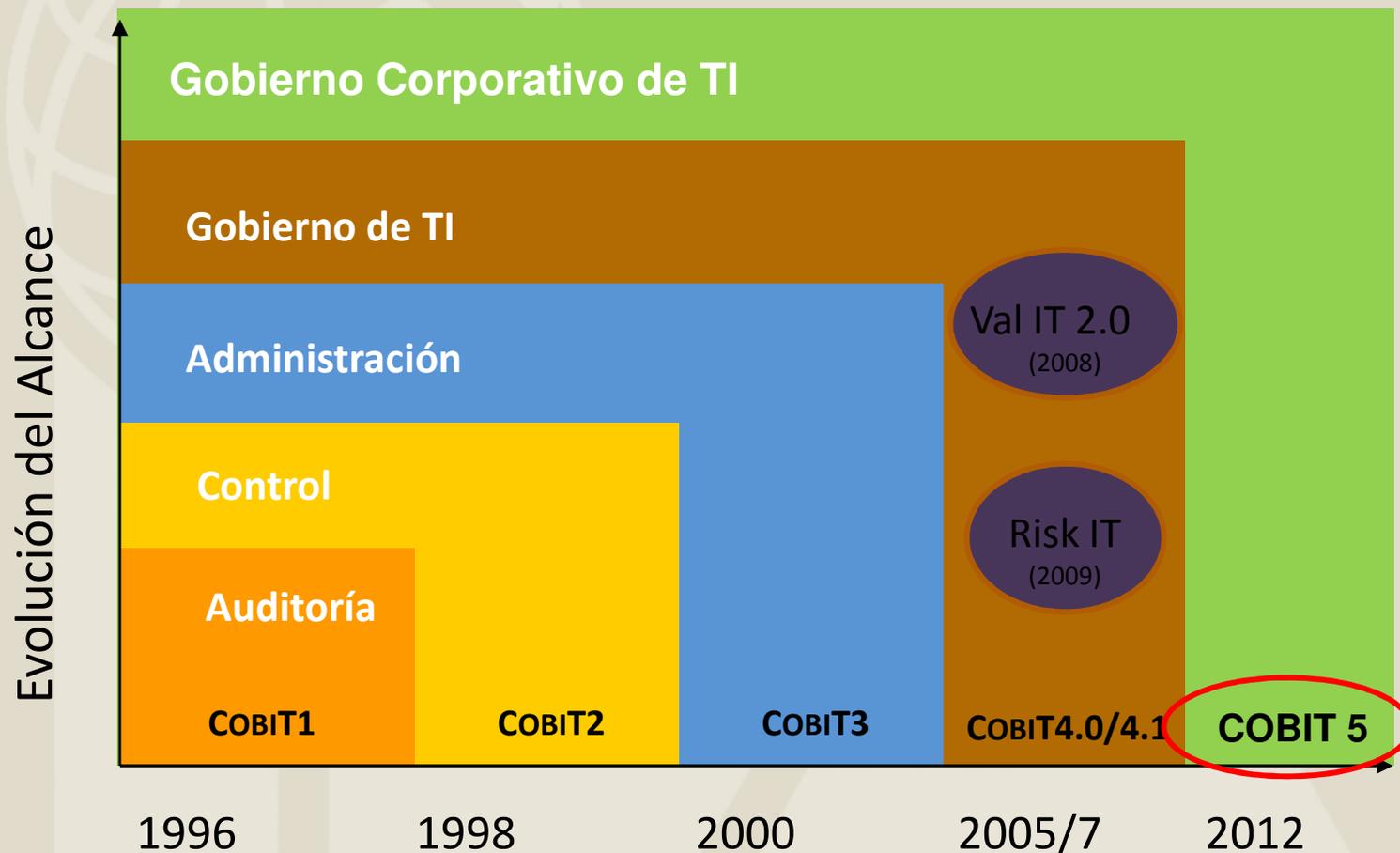
COBIT 5 une principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información así como su uso en beneficio de las partes interesadas.

Cobit 5



- Ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.
- Permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.
- Los principios y habilitadores de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

Historia de Cobit 5



Un Marco Empresarial de ISACA, en www.isaca.org/cobit

Productos de Cobit 5

COBIT 5

COBIT 5 Guías habilitadoras

COBIT 5: Procesos habilitadores

**COBIT 5:
Información habilitadora**

Otras guías habilitadoras

COBIT 5 Guías profesionales

**COBIT 5:
Implementación**

**COBIT 5:
Para seguridad de información**

**COBIT 5:
Para riesgos**

Otras guías profesionales

COBIT 5 ambiente colaborativo en línea

Cobit 5



Marco de referencia para la gestión y gobernabilidad de tecnología de información.

Para cada decisión, se debe preguntar:

- - ¿Quién recibe los beneficios?
- - ¿A quién impacta el riesgo?
- - ¿Qué recursos se necesitan?

Cobit 5



COBIT® 5 proporciona un marco global que ayuda a las empresas a alcanzar sus metas y entregar valor a través de un gobierno y una gestión eficaz de TI

- La entrega de valor requiere buen Gobierno y Gestión de la información y la tecnología relacionada
- Empresas, ejecutivos y consejos de administración deben aceptar a TI como otra parte importante del negocio
- Los requisitos externos de cumplimiento legal, regulatorio y contractual relacionadas con el uso de la información y la tecnología asociada van en aumento, amenazando el valor si no se cumplen

Principios de Cobit



Principios de Cobit 5



- **PRINCIPIO 1. Satisfacer las Necesidades de las Partes Interesadas** - Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros habilitadores para permitir la creación de valor del negocio mediante el uso de TI.

Principios de Cobit 5



- **PRINCIPIO 2: Cubrir la Empresa Extremo-a-Extremo - COBIT 5** integra el gobierno y la gestión de TI en el gobierno corporativo:
 - Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
 - Considera que los habilitadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principios de Cobit 5



- **PRINCIPIO 3: Aplicar un Marco de Referencia único integrado**—Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

Principios de Cobit 5



- **PRINCIPIO 4: Hacer Posible un Enfoque Holístico**—Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de habilitadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa.

Principios de Cobit 5

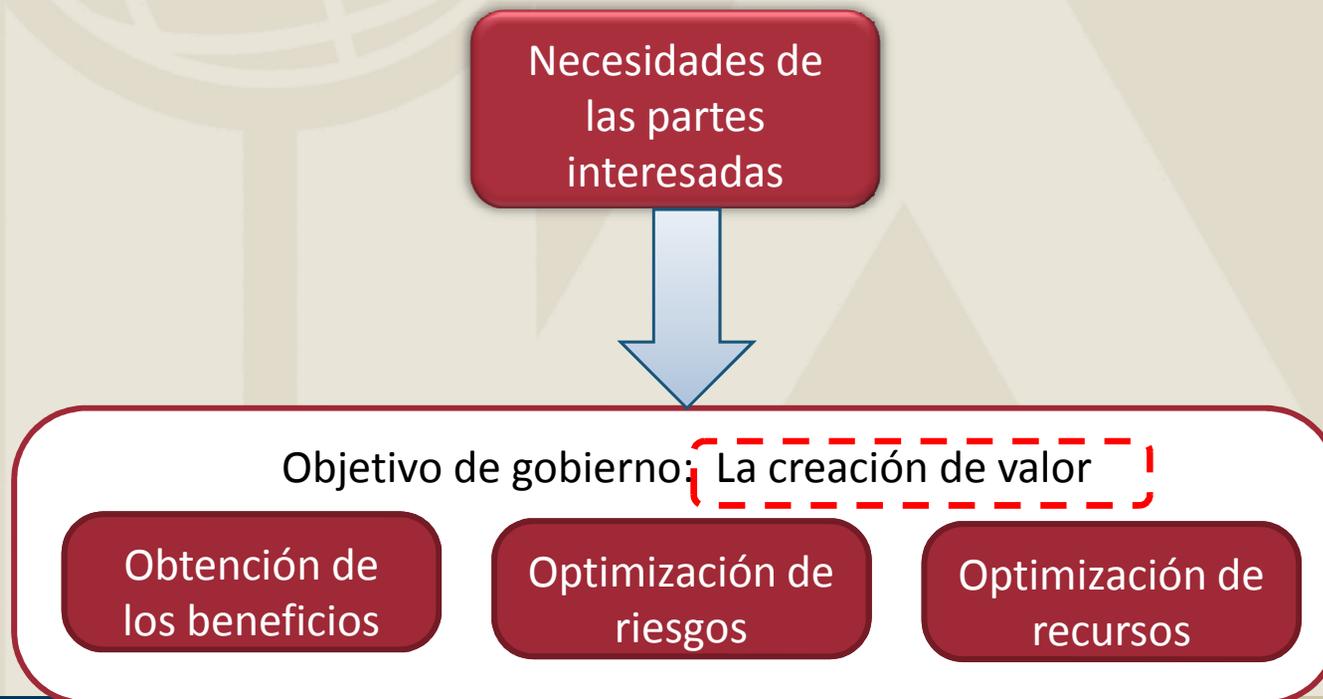


- **PRINCIPIO 5: Separar el Gobierno de la Gestión**—El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

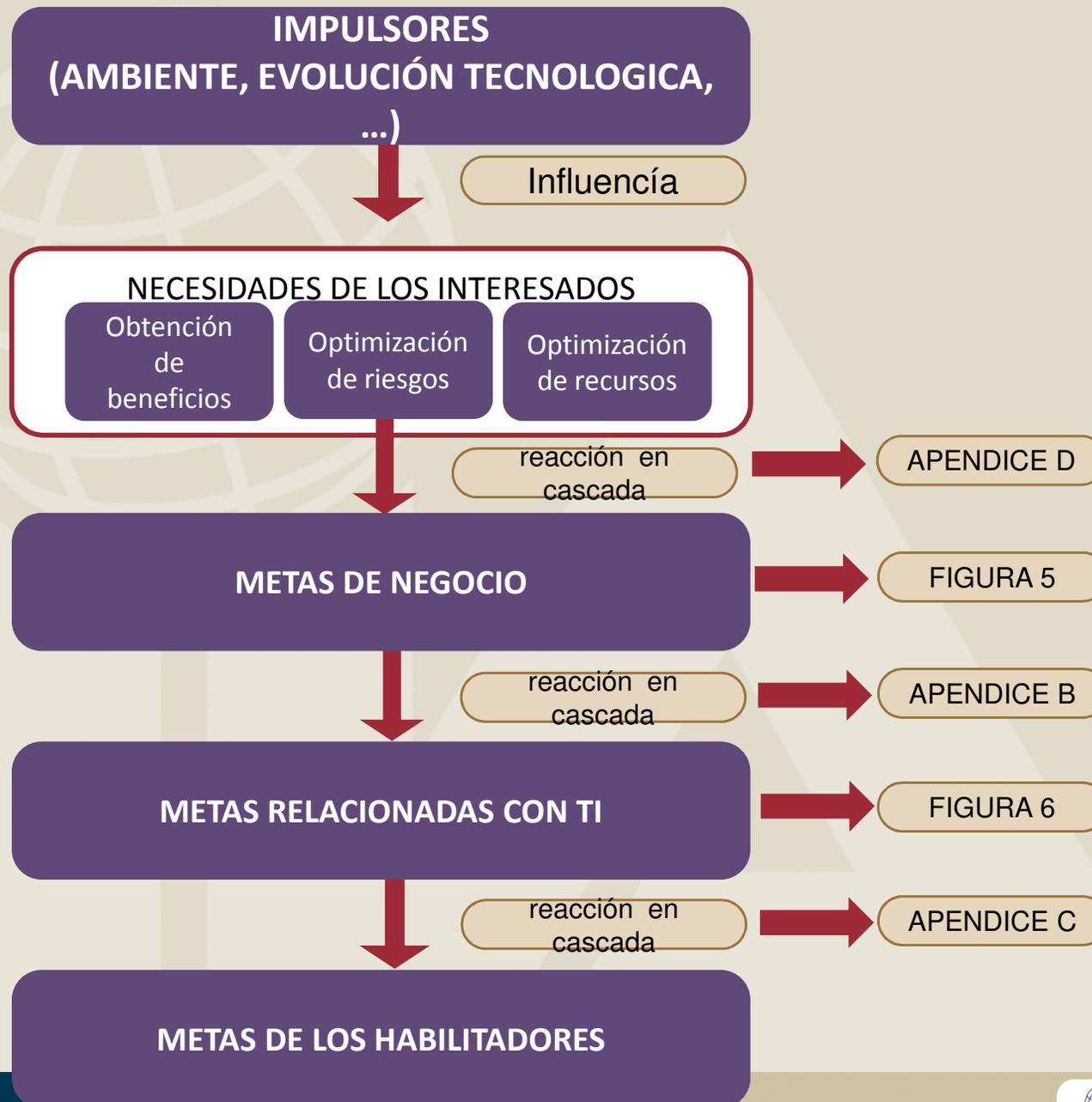
Estructura de Cobit 5

Objetivo de Cobit 5

Las empresas existen para crear valor a sus Interesados. Para cualquier empresa la creación de valor es un objetivo de Gobierno. La creación de valor significa obtener beneficios a un costo óptimo de recursos y un riesgo optimizado.



Cascada de Metas



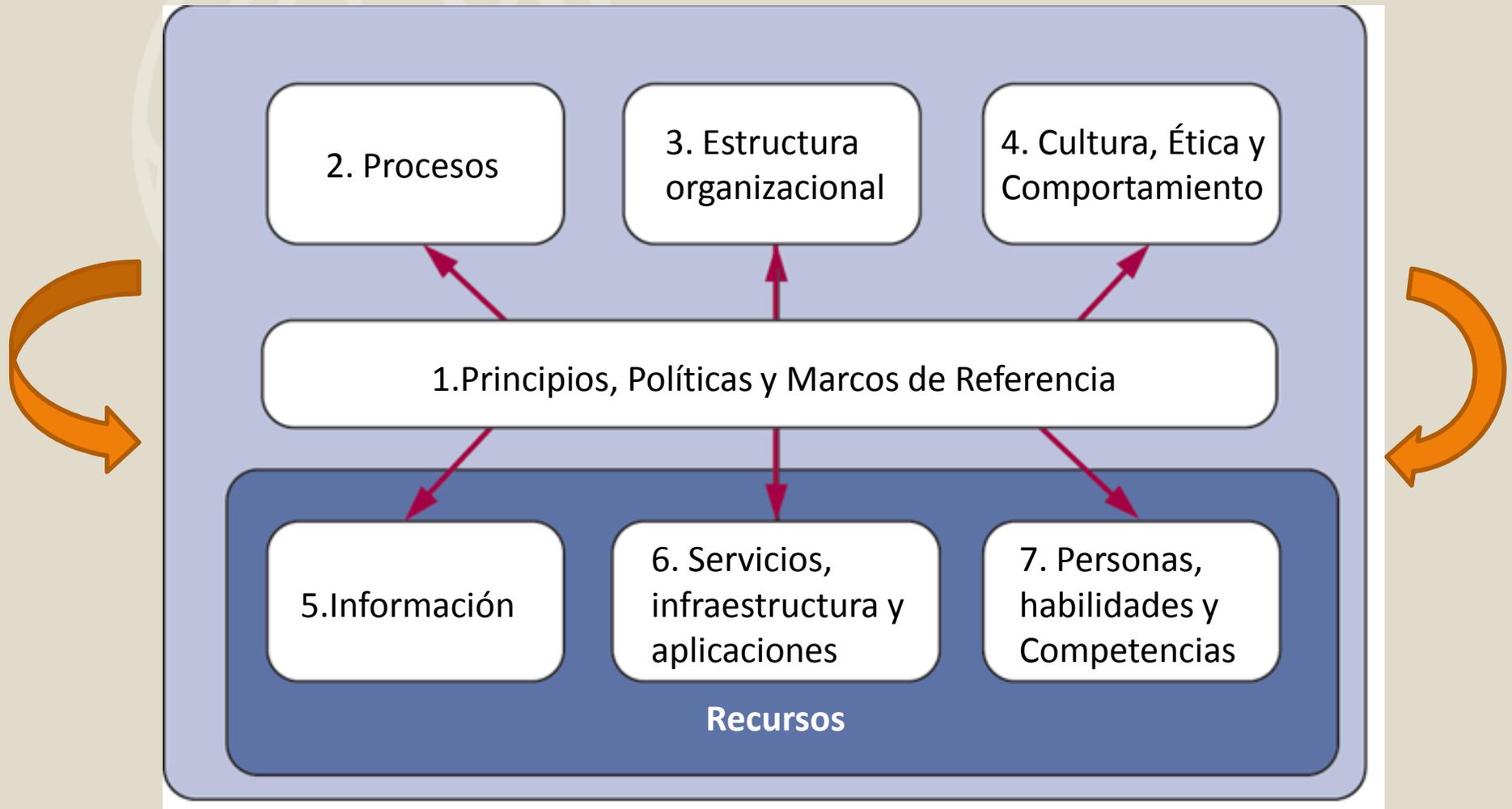
Cascada de metas

- **Impulsores:** Son aquellos elementos que pueden influenciar la dirección de una organización, como por ejemplo: requerimientos regulatorios, nuevas tecnología, nuevos mercados, etc.
- **Necesidades de los interesados:** Entendiendo que los “interesados” son todos aquellos que tienen un interés en la empresa, como por ejemplo: clientes, empleados o accionistas, sus necesidades son obtener un beneficio, optimizar riesgos, reducir costos, etc.

Cascada de metas

- **Metas de negocio:** Son los objetivos de una organización para cumplir con una estrategia de crecimiento y desarrollo.
- **Metas de TI:** Son aquellos objetivos desarrollados específicamente para apoyar y “habilitar” el cumplimiento con las metas de negocio.
- **Habilitadores:** Son aquellos elementos que van a permitir el logro del propósito de un proceso (recursos, políticas, personas, etc.) y las metas de la empresa.

Enfoque en los Habilitadores



Habilitadores de Cobit 5

- **Principios, políticas y marcos de referencia:** son el vehículo para traducir el comportamiento deseado en una guía práctica para la gestión del día a día.
- **Procesos:** describen un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir un conjunto de resultados que soporten el logro de las metas relacionadas con TI.
- **Estructuras organizativas:** son las entidades clave en una empresa para la toma de decisiones.
- **Cultura, ética y comportamiento** de los individuos y de la empresa: son muy a menudo subestimados como factor de éxito en las actividades de gobierno y de gestión.

Habilitadores de Cobit 5

- **Información**, está inmersa a través de cualquier organización e incluye toda la información producida y utilizada por la empresa. La información es requerida para mantener la organización funcionando y bien gobernada. A nivel operacional la información es frecuentemente el producto clave de la empresa en sí misma.
- **Servicios, infraestructura y aplicaciones** incluyen la infraestructura, la tecnología y las aplicaciones que proveen a la empresa la capacidad de procesamiento y los servicios.
- **Personas, habilidades y competencias** están relacionadas con las personas y son requeridas para completar con éxito todas las actividades y para tomar las decisiones correctas, además de emprender acciones correctivas.

Componentes de Cobit 5

Cobit 5 es un marco compuesto de los siguientes elementos

- **Grupos de procesos (2)**
 - **Gobierno** y **Administración**
- **Dominios (5)**
 - Evaluar, dirigir y controlar (EDM) – **Proceso de Gobierno**
 - Alinear, planificar y organizar (APO) – **Proceso de Adm.**
 - Construir, adquirir e implementar (BAI) – **Proceso de Adm.**
 - Entregar , servir y proveer soporte (DSS) – **Proceso de Adm.**
 - Evaluar y valorar (MEA) – **Proceso de Adm.**
- **Procesos (37)**

Composición de Cobit 5

PROCESOS PARA EL GOBIERNO DE TI

Evaluar, dirigir y controlar

PROCESOS PARA LA ADMINISTRACIÓN DE TI

Alinear, planificar y organizar

Evaluar y valorar

Construir, adquirir e implementar

Entregar , servir y proveer soporte

Composición de Cobit 5

PROCESOS PARA EL GOBIERNO DE TI

Evaluar, dirigir y controlar

EDM01
Establecer y
mantener el marco de
gobierno de TI

EDM02
Asegurar la entrega
de beneficios

EDM03
Asegurar la
optimización de
riesgos

EDM04
Asegurar la
optimización de
recursos

EDM05
Asegurar la
transparencia

PROCESOS PARA LA ADMINISTRACIÓN DE TI

Alinear, planificar y organizar

APO01
Gestionar el
marco de TI

APO02
Gestionar la
estrategia

APO03
Gestionar la
arquitectura
empresarial

APO04
Gestionar la
innovación

APO05
Gestionar el
portafolio

APO06
Gestionar el
presupuesto y
los costos

APO07
Gestionar los
recursos humano

APO08
Gestionar las
relaciones

APO09
Gestionar los
acuerdos del
servicio

APO10
Gestionar los
proveedores

APO11
Gestionar calidad

APO12
Gestionar el
riesgo

APO13
Gestionar la
seguridad

Construir, adquirir e implementar

BAI01
Gestionar programas
y proyectos

BAI02
Gestionar la
definición de
requisitos

BAI03
Gestionar la
identificación de
soluciones

BAI04
Gestionar la
disponibilidad y
capacidad

BAI05
Gestionar
habilitación de
cambio
organizacional

BAI06
Gestionar los
cambios

BAI07
Gestionar la
aceptación del
cambio y la
transición

BAI08
Gestionar el
conocimiento

BAI09
Gestionar los activos

BAI10
Gestionar la
configuración

Entregar, servir y proveer soporte

DSS01
Gestionar
operaciones

DSS02
Gestionar
solicitudes y
servicio de
incidentes

DSS03
Gestionar los
problemas

DSS04
Gestionar la
continuidad

DSS05
Gestionar los
servicios de
seguridad

DSS06
Gestionar los
controles de
proceso del
negocio

Evaluar y valorar

MEA01
Desempeño y
cumplimiento

MEA02
Sistema de
control interno

MEA03
Cumplimiento de
los requisitos
externos

Composición de Cobit 5

PROCESOS PARA EL GOBIERNO DE TI

EVALUAR, DIRIGIR Y CONTROLAR

EDM01
Establecer y mantener el marco de gobierno de TI

EDM02
Asegurar la entrega de beneficios

EDM03
Asegurar la optimización de riesgos

EDM04
Asegurar la optimización de recursos

EDM05
Asegurar la transparencia

PROCESOS PARA LA ADMINISTRACIÓN DE TI

Alinear, planificar y organizar

APO01
Gestionar el marco de TI

APO02
Gestionar la estrategia

APO03
Gestionar la arquitectura empresarial

APO04
Gestionar la innovación

APO05
Gestionar el portafolio

APO06
Gestionar el presupuesto y los costos

APO07
Gestionar los recursos humano

APO08
Gestionar las relaciones

APO09
Gestionar los acuerdos del servicio

APO10
Gestionar los proveedores

APO11
Gestionar calidad

APO12
Gestionar el riesgo

APO13
Gestionar la seguridad

Construir, adquirir e implementar

BAI01
Gestionar programas y proyectos

BAI02
Gestionar la definición de requisitos

BAI03
Gestionar la identificación de soluciones

BAI04
Gestionar la disponibilidad y capacidad

BAI05
Gestionar habilitación de cambio organizacional

BAI06
Gestionar los cambios

BAI07
Gestionar la aceptación del cambio y la transición

BAI08
Gestionar el conocimiento

BAI09
Gestionar los activos

BAI10
Gestionar la configuración

Entregar, servir y proveer soporte

DSS01
Gestionar operaciones

DSS02
Gestionar solicitudes y servicio de incidentes

DSS03
Gestionar los problemas

DSS04
Gestionar la continuidad

DSS05
Gestionar los servicios de seguridad

DSS06
Gestionar los controles de proceso del negocio

Evaluar y valorar

MEA01
Desempeño y cumplimiento

MEA02
Sistema de control interno

MEA03
Cumplimiento de los requisitos externos



Ejemplo de Evaluación de Capacidades

Conocer los objetivos de negocio

- Conocer y comprender los objetivos de negocios del plan estratégico de la empresa:
 - Metas de crecimiento a corto, mediano y largo plazo
 - Planes de expansión
 - Nuevos productos y/o servicios
 - Presencia en nuevos mercados

Identificación de objetivos de negocio según Cobit 5

DIMENSIÓN	OBJETIVO DE NEGOCIO (Según Cobit)		
FINANCIERA	1	Aumentar valor de las inversiones de negocios	
	2	Mantener un portafolio de productos y servicios competitivos	
	3	Administrar riesgos de negocio (salvaguardar activos)	
	4	Cumplimiento con leyes y regulaciones externas	
	5	Transparencia financiera	
	6	Crear una cultura de servicio orientada al cliente	← IDENTIFICAR EL
CLIENTE	7	Mantener la continuidad y disponibilidad del servicio	OBJETIVO DE NEGOCIO
	8	Agilizar las respuestas a los cambios del ambiente de negocio	DE COBIT QUE SE
	9	Realizar toma de decisiones estratégicas basadas en información	AJUSTE AL OBJETIVO
	10	Optimizar los costos de la entrega de servicios	ESTRATÉGICO DE LA ORGANIZACIÓN
INTERNA	11	Optimizar la funcionalidad de los procesos de negocio	
	12	Optimizar los costos de los procesos de negocio	
	13	Administrar los cambios del negocio	
	14	Crear productividad operacional y del personal	
	15	Cumplimiento con políticas internas	
APRENDIZAJE Y CRECIMIENTO	16	Contar con personal capacitado y motivado	
	17	Crear una cultura de innovación de negocios y productos	

Identificación de objetivos de tecnología

A partir de la identificación de los objetivos de negocio de la organización alineados con Cobit:

- Identificar los objetivos de tecnología de la empresa para evaluar su alineación.

Identificación de los procesos de TI que soportan el negocio

- Identificar los procesos relacionados al entorno de TI que soportan los objetivos de TI evaluados.

Mapeo de Cobit 5 de metas de tecnología con procesos de TI



Alineamiento de la estrategia de TI y el negocio

Entrega de los servicios de TI alineado con los requerimientos del negocio

Seleccionar los procesos de TI que soportan los objetivos de TI previamente identificados y que son considerados como PRIMARIOS, según Cobit

		Financial					Customer					Internal					Learning and Growth	
COBIT 5 Process		08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Evaluate, Measure and Monitor	EDM04 Ensure Resource Optimisation	S	S	S	S	S	S	S	P	S	S	P	S	S	S	S	P	S
	EDM05 Ensure Stakeholder Transparency	S	S	P	S	P	P	S	S	S	S	S	S	S	S	P	S	S
	AP001 Manage the IT Management Framework	P	P	S	S	S	S	S	S	P	S	P	S	S	S	S	P	P
Plan and Organise	AP003 Manage Enterprise Architecture	P	S	S	S	S	S	S	P	S	P	S	S	S	S	S	S	S
	AP004 Manage Innovation	S	S	S	P	S	S	P	P	S	P	S	S	S	S	S	S	P
	AP005 Manage Portfolio	P	S	S	P	S	S	S	S	S	S	S	S	P	S	S	S	S
	AP006 Manage Budget and Costs	S	S	S	P	P	S	S	S	S	S	S	S	S	S	S	S	S
	AP007 Manage Human Resources	S	S	S	S	S	S	S	S	S	P	S	P	S	S	S	P	P
	AP009 Manage Service Agreements	P	S	S	S	S	S	S	S	S	S	S	S	S	P	S	S	S
	AP010 Manage Suppliers	S	S	P	S	S	P	S	P	S	S	S	S	S	S	S	S	S
Implement and Improve	AP011 Manage Quality	S	S	S	P	S	P	S	S	S	S	P	S	S	S	S	S	S
	AP012 Manage Risk	S	P	P	S	P	S	S	S	P	S	S	S	P	S	S	S	S
	AP013 Manage Security	P	P	P	P	S	S	S	P	S	S	S	S	P	S	S	S	S
	AP014 Manage Compliance	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S



Evaluar la madurez de las actividades del proceso

AP002 Gestionar la Estrategia

Área: Gestión

Dominio: Alinear, Planificar y Organizar

Descripción del Proceso

Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.

Declaración del Propósito del Proceso

Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.

Actividades

1. Desarrollar y mantener un entendimiento de las estrategias y objetivos del negocio, así como del entorno y los retos operativos actuales.
2. Desarrollar y mantener un entendimiento del entorno externo a la empresa.
3. Identificar las partes interesadas más importantes y obtener comprensión de sus requerimientos.
4. Identificar y analizar las fuentes de los cambios en la empresa y en el entorno externo.
5. Determinar prioridades para el cambio estratégico.
6. Entender la actual arquitectura de empresa y trabajar con el proceso de arquitectura de empresa para determinar cualquier brecha potencial en la arquitectura.

Niveles de capacidad de procesos revisados

Optimizado

El proceso está siendo mejorado para cumplir con los objetivos relevantes actuales del negocio, y los proyectados

Nivel 5 Proceso optimizado

PA 5.1 Atributo de innovación de procesos
PA 5.2 Atributo de optimización de procesos

Predecible

El proceso se realiza consistentemente dentro de límites definidos

Nivel 4 Proceso predecible

PA 4.1 Atributo de medición de procesos
PA 4.2 Atributo de control de procesos

Establecido

Se utiliza un proceso definido basado en un estándar

Nivel 3 Proceso establecido

PA 3.1 Atributo de definición de procesos
PA 3.2 Atributo de despliegue de procesos

Nivel 2 Proceso gestionado

PA 2.1 Atributo de gestión del desempeño
PA 2.2 Atributo de gestión de productos de trabajo

Gestionado

El proceso se gestiona y se establecen productos de trabajo controlados que se mantienen

Nivel 1 Proceso ejecutado

PA 1.1 Atributo de desempeño de procesos

Ejecutado

El proceso se lleva a cabo y alcanza su propósito

Nivel 0 Proceso incompleto

Incompleto

El proceso no se ejecute o no logra su propósito



Progress Through Sharing

© 2012 ISACA. All Rights Reserved.





Relación de COSO con Cobit 5

Relación de COSO y Cobit

COMPONENTE DE COSO	PRINCIPIOS DE COSO	PROCESOS DE COBIT
AMBIENTE DE CONTROL	1. La organización demuestra el compromiso para con la integridad y los valores éticos.	EDM01, APO01, APO07
	2. La junta de directores demuestra independencia ante la administración y ejerce vigilancia para el desarrollo y ejecución del control interno.	EDM01 a EDM05
	3. La administración establece, con la vigilancia de la junta, las estructuras, líneas de presentación de reporte, y las autoridades y responsabilidades apropiadas en la búsqueda de los objetivos.	EDM01 APO01
	4. En alineación con los objetivos la organización demuestra el compromiso para atraer, desarrollar, y retener personas competentes.	APO01 APO07
	5. En la búsqueda de los objetivos la organización tiene personas responsables por sus responsabilidades de control interno.	TODOS

Relación de COSO y Cobit

COMPONENTE DE COSO	PRINCIPIOS DE COSO	PROCESOS DE COBIT
EVALUACIÓN DE RIESGO	6. La organización especifica los objetivos con suficiente claridad para permitir la identificación y valoración de los riesgos relacionados con los objetivos.	TODOS LOS PROCESOS
	7. La organización identifica los riesgos para el logro de sus objetivos a través de la entidad y analiza los riesgos como la base para determinar cómo deben ser administrados los riesgos.	EDM03 APO12
	8. En la valoración de los riesgos para el logro de los objetivos la organización considera el potencial por el fraude.	EDM01 APO01 APO07 MEA03
	9. La organización identifica y valora los cambios que de manera importante podrían impactar al sistema de control interno.	APO01 BAI02 BAI05 a BAI07

Relación de COSO y Cobit

COMPONENTE DE COSO	PRINCIPIOS DE COSO	PROCESOS DE COBIT
ACTIVIDADES DE CONTROL	10. La organización selecciona y desarrolla las actividades de control que contribuyan a la mitigación, a niveles aceptables, de los riesgos para el logro de los objetivos.	TODOS LOS PROCESOS
	11. La organización selecciona y desarrolla las actividades de control generales sobre la tecnología para respaldar el logro de los objetivos.	TODOS LOS PROCESOS
	12. La organización despliega las actividades de control tal y como se manifiestan en las políticas que establecen lo que se espera y en los procedimientos relevantes para llevar a cabo esas políticas.	APO01

Relación de COSO y Cobit

COMPONENTE DE COSO	PRINCIPIOS DE COSO	PROCESOS DE COBIT
INFORMACIÓN Y COMUNICACIÓN	13. La organización obtiene o genera y usa información de calidad, relevante, para respaldar el funcionamiento de los otros componentes del control interno.	TODOS LOS PROCESOS
	14. La organización comunica internamente la información, incluyendo los objetivos y responsabilidades para el control interno, necesaria para respaldar el funcionamiento de los otros componentes del control interno.	TODOS LOS PROCESOS
	15. La organización se comunica con terceros en relación con las materias que afectan el funcionamiento de los otros componentes del control interno.	EDM05

Relación de COSO y Cobit

COMPONENTE DE COSO	PRINCIPIOS DE COSO	PROCESOS DE COBIT
MONITOREO	16. La organización selecciona, desarrolla, y lleva a cabo evaluaciones continuas y/o separadas para comprobar si los componentes del control interno están presentes y están funcionando.	MEA02
	17. La organización evalúa y comunica las deficiencias del control interno, haciéndolo de una manera oportuna, a las partes responsables por realizar la acción correctiva, incluyendo la administración principal y la junta de directores, según sea apropiado.	EDM05 MEA02

CONCLUSIONES



Progress Through Sharing



Instituto de Auditores
Internos de Panamá

CONCLUSIONES

1. Cobit es un marco de referencia para la gestión del gobierno y de la administración de tecnología de información
2. Cobit 5 proporciona principios y guías del gobierno y administración para la información y la tecnología relacionada que son componentes críticos para el ambiente de control interno.
3. COSO y Cobit 5 son guías fundamentales para los auditores en su búsqueda de mantener un ambiente de control interno y administración de riesgos
4. Cobit 5 es gratis para miembros y no miembros de ISACA en: <http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>

Introducción a Cobit 5

Muchas gracias

Julio R. Jolly Moore

CRMA, CFE, CRISC, CGEIT, Internal Audit Quality Assessment

jjolly@bdo.com.pa