Mejores prácticas de Tecnología de la Información

Cerrando las brechas de COBIT 4.1 a COBIT 5

Julio del 2014

José Luis Antigua, CISA, ACDA, ACT, República Dominicana
jose.antigua@bdo.com.do
Director de Riesgo & TI en BDO Dominicana

Juan Carlos Morales, CISA, CISM, CRISC, CGEIT, Guatemala
juancarlos.moralesbathen@yahoo.com
Consultor de Gobierno de TI y Gestión de Riesgos

Antecedentes

La tecnología está en constante cambio. Los productos de hoy son de corta duración, los equipos digitales han reemplazado los análogos, los equipos móviles inteligentes son parte de la cotidianidad y las redes sociales han permitido que las naciones, empresas y clientes hoy estén a pocos “grados de separación”.

Las instituciones y comercios cada día se hacen más dependientes de estas tecnologías, pues les crean ventajas competitivas incluyendo eficiencia y eficacia de los procesos para el cumplimiento de sus objetivos. De igual manera, el uso de tecnologías trae consigo importantes retos y riesgos que, de no ser administrados de manera correcta, podrían volverse en contra de quienes las utilizan.

Antecedentes

En la República Dominicana y otros países de América Latina, las leyes, regulaciones, reglamentos, instructivos y otros mecanismos de supervisión de las actividades empresariales atienden los aspectos tecnológicos del negocio de manera limitada.

Los cambios tecnológicos experimentados en los últimos años han ido revolucionando de manera exponencial la forma de operar cualquier entidad, lo que **amerita nuevas reglas para administrar de manera integral los riesgos vinculados a la tecnología, el crecimiento sostenible y la justa competencia**.

A continuación presentamos algunas de las herramientas de supervisión en su estatus actual, la versión más actual de los marcos internacionales de referencia por excelencia para GRC (con énfasis en tecnología) y algunas pautas para su adopción.

Gobierno Corporativo (2002)

- Base principal: COSO – I

Como parte de los aspectos del Ambiente de Control, incluye:

- Reglamento para Consejo de Dirección o Administración
- Creación código de ética y conducta
- Creación comité de auditoría

Reglamento de Riesgo Operacional (2009)

- Hace referencia al uso de COSO – II (artículo 4)

- COBIT 4.1 (artículo 4)
  - Planificación y Organización
  - Adquisición e Implementación
  - Entrega y Soporte
  - Monitoreo y Evaluación

Circular 11-12 para Tercerización o Subcontratación de Servicios (aspecto TI)

- Basado en Adquisición e Implementación de CObIT 4.1

- Incluye
  - Aspectos del proceso de Adquisición e Implementación (AI 2)
  - Materialidad, responsabilidades, confidencialidad, continuidad, acceso a la información y monitoreo
  - Contratos

Ley 53-07 Crímenes y Delitos de Alta Tecnología

- Conceptos no actualizados
- No se consideran tecnologías actuales, por ejemplo, hosting (nube) y principalmente BYOD
- Concepto poco integral de seguridad
- Considera confidencialidad, integridad y disponibilidad

Ley 65-00 Derecho de Autor

- Incluye explícitamente aspectos de software en sus artículos 73 al 75.

- Alcance limitado respecto a los elementos que permitan su aplicación y debido control considerando el entorno empresarial y posibilidades de licenciamiento actuales (incluyendo SaaS)

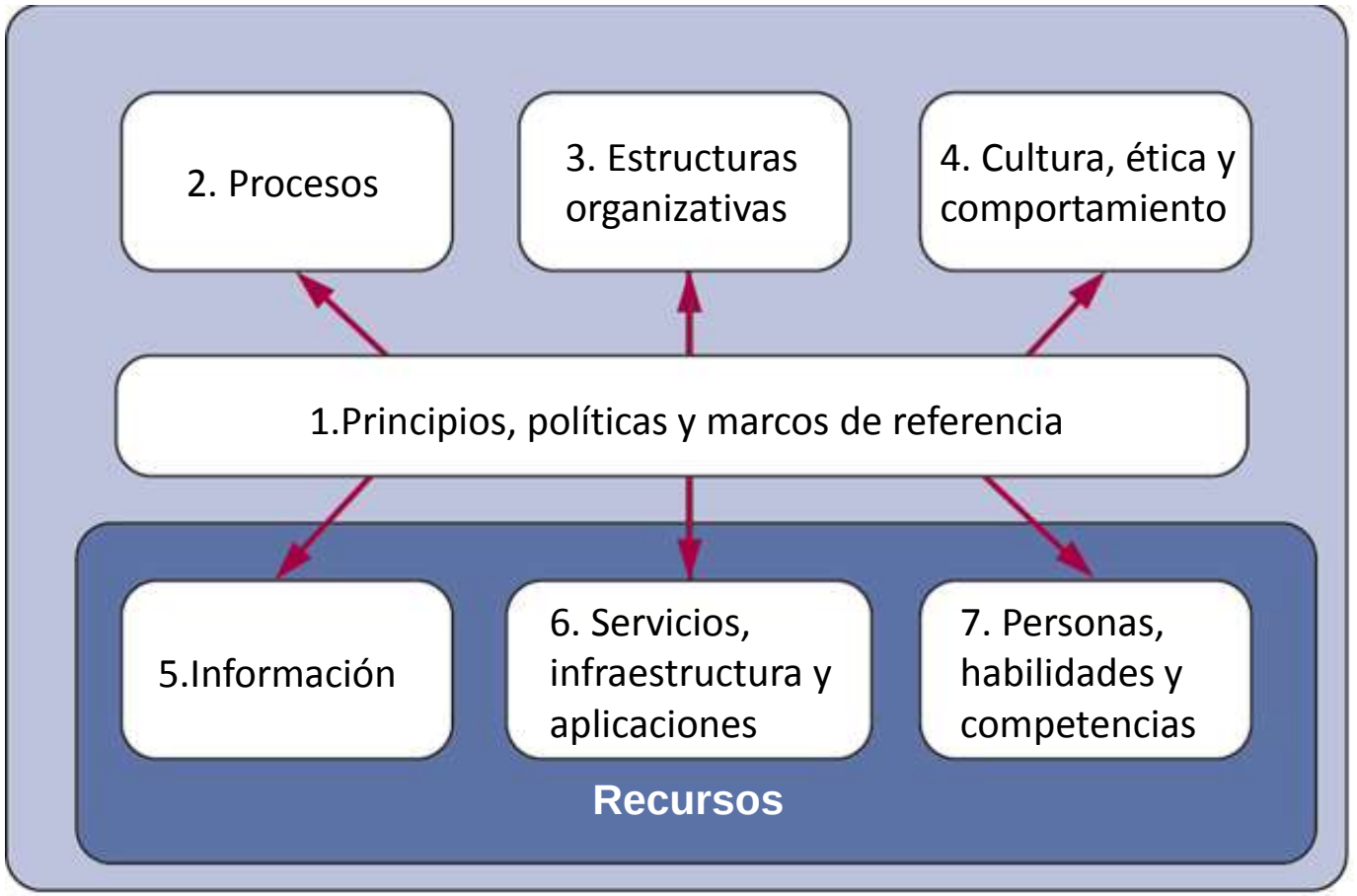
- A pesar de la actualización del 2006, el enfoque es poco integral

Estructura de COBIT 5

- COBIT 5 se basa en:
  - 5 principios y
  - 7 catalizadores

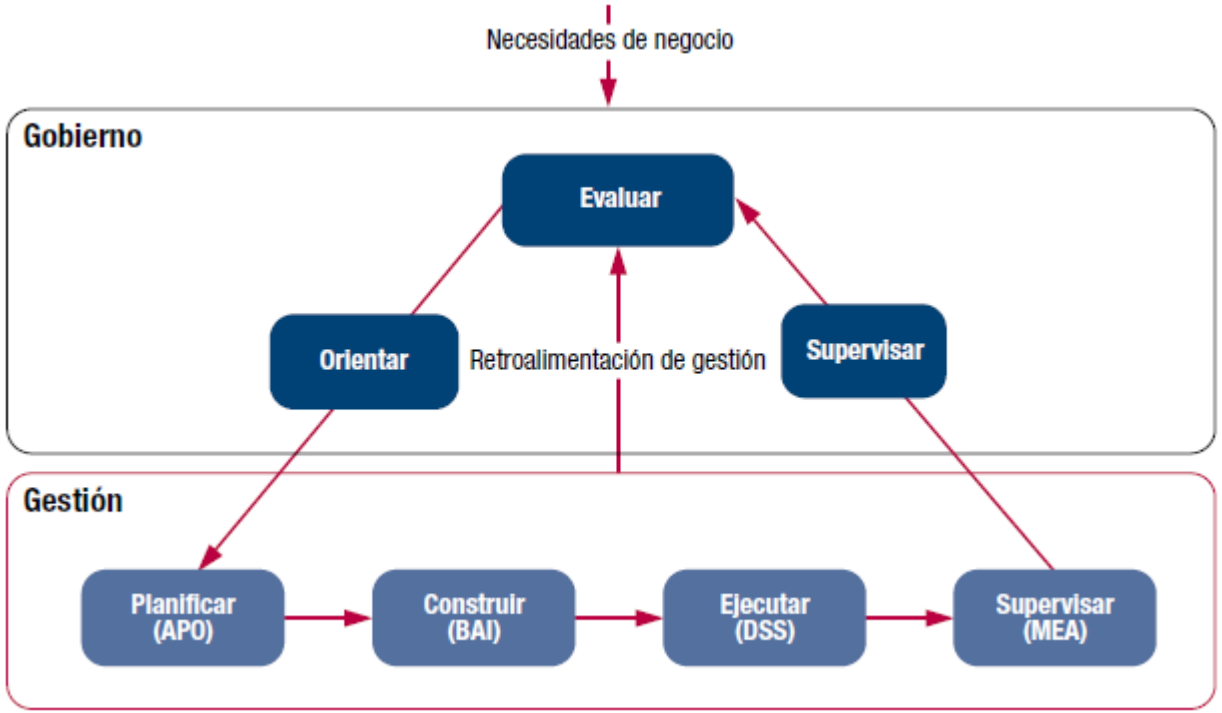
Principios de COBIT 5

Principio 4: Hacer posible un enfoque holístico



Principio 5: Separar el gobierno de la gestión

Áreas clave de gobierno y gestión



Áreas de cambio

- Nuevos principios GEIT
- Mayor atención a los catalizadores
- Nuevo modelo de procesos de referencia
- Separación de los procesos de gobierno de los de gestión
- Prácticas y actividades
- Metas revisadas y métricas ampliadas
- Entradas y salidas a nivel de prácticas de gestión y de gobierno
- Matriz RACI ampliada y a nivel de prácticas
- Nuevo modelo de capacidad de procesos

¿En qué consiste migrar a COBIT 5?

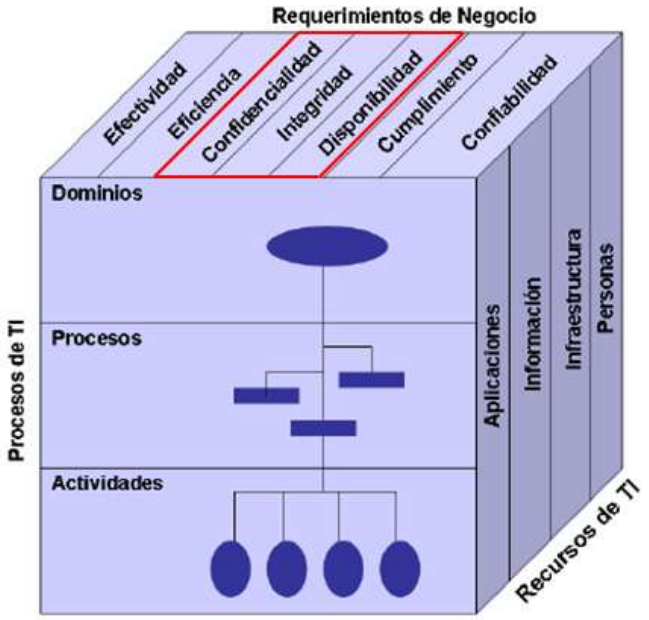
- Migrar de COBIT 4.1 a COBIT 5 no es lo mismo que hacer una migración de software o de hardware.

¿En qué consiste migrar a COBIT 5?

- Depende de lo que se entienda por haber “implementado" COBIT 4.1.
- Si eso significa que algunos controles están en su lugar, entonces migrar a COBIT 5 es un gran cambio de enfoque.

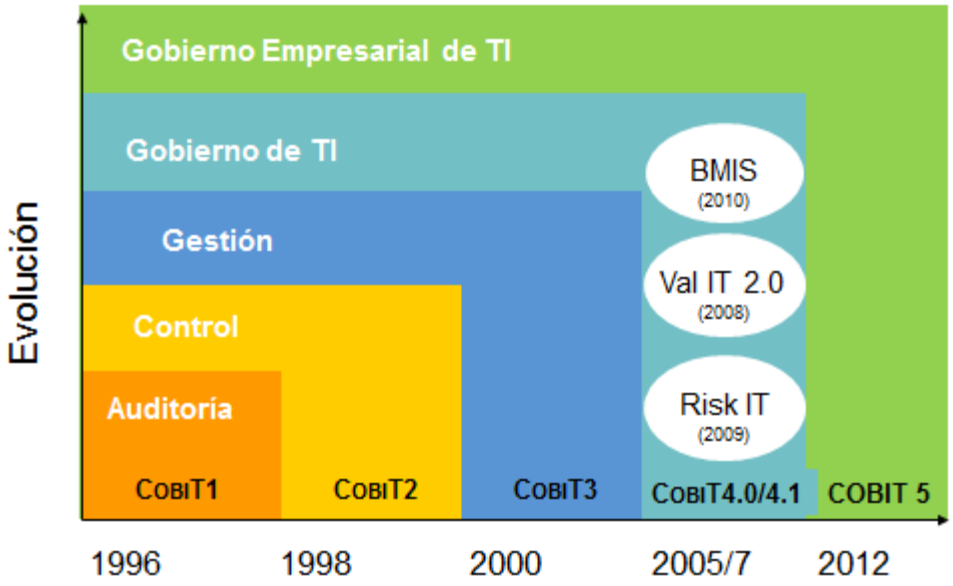
Adoptar y adaptar COBIT 4.1

- Una correcta adopción de COBIT 4.1 podría comprender un modelo de procesos integrados para la gestión de TI, con un marco de gobierno para asegurar el uso adecuado de TI y la entrega de valor.



¿En qué consiste migrar a COBIT 5?

- Para las organizaciones que han “implementado” COBIT 4.1, la migración al nuevo marco es un proceso natural de progresión en el que la organización va a ampliar su cobertura del gobierno de TI a una iniciativa de gobierno empresarial de TI.



¿En qué consiste migrar a COBIT 5?

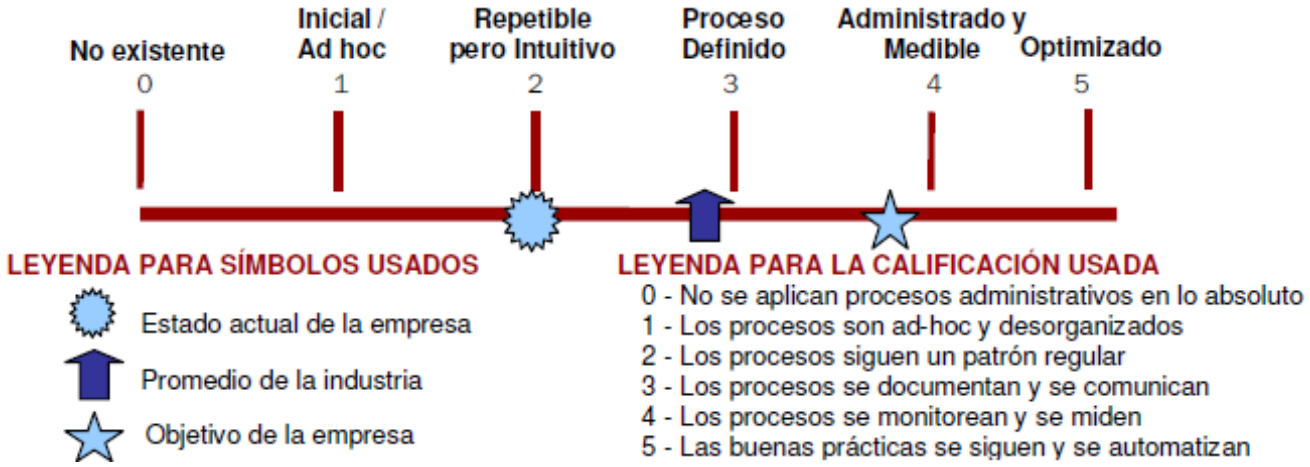
- Podríamos decir que la migración es más bien una transición hacia una nueva manera de trabajar para satisfacer las necesidades de todas las partes interesadas utilizando el modelo de cascada

¿Migrar o no migrar?

- Si la organización se encuentra todavía inmersa en la implementación de procesos utilizando COBIT 4.1 como marco de referencia, se recomienda continuar y finalizar antes de considerar una migración al nuevo marco, COBIT 5.

¿Migrar o no migrar?

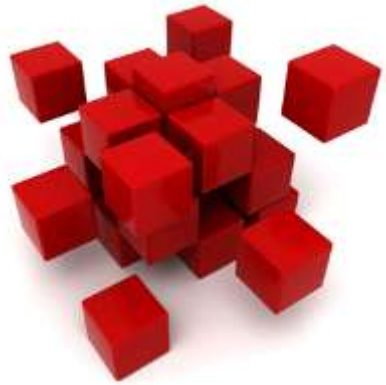
- Si la organización ha puesto en práctica los controles recomendados por COBIT 4.1 y ha llegado a lo que cree es un razonable grado de madurez, es el momento de considerar la migración a COBIT 5.



¿Cuándo migrar a COBIT 5?

La siguiente es una lista de factores que nos llevan a pensar que es hora de migrar a COBIT 5:

- Repetidas fallas en los procesos críticos de TI que afectan a la empresa.
- Riesgos relacionados con TI que pueden impactar fuertemente a la organización.
- Controles orientados a TI que no cubren aspectos críticos de la empresa.



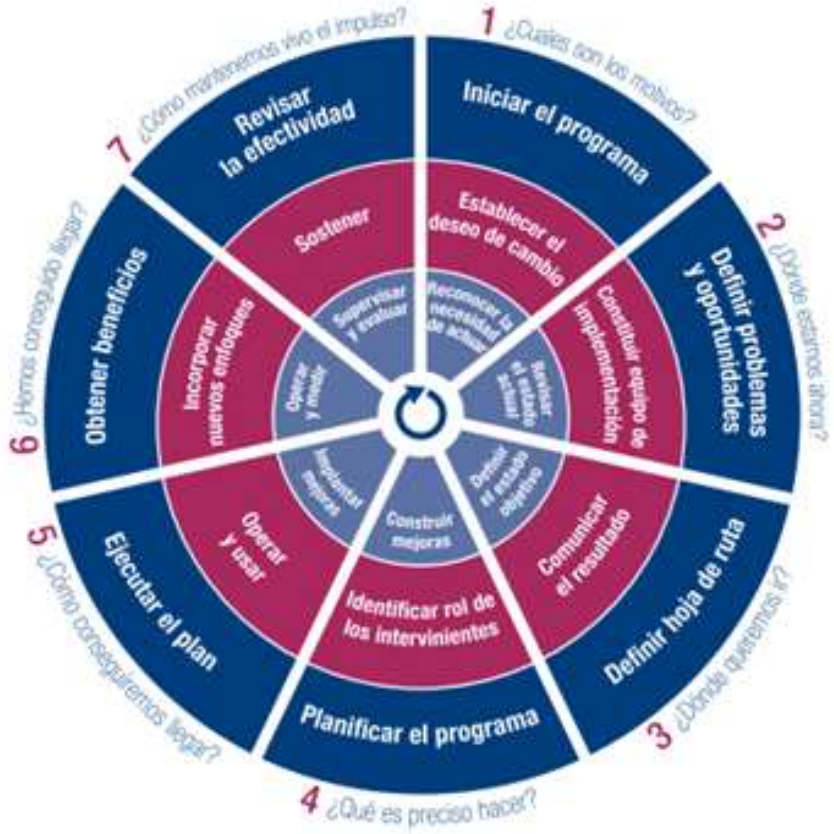
¿Cómo iniciar la Migración?

Antes de iniciar una migración al nuevo marco, se recomienda:

- Definir con claridad los objetivos de la migración
- Identificar los beneficios de negocio que la organización logrará mediante la adopción del nuevo marco.

¿Cómo iniciar la Migración?

- La clave para el éxito de la migración es que se debe comenzar abordando los puntos de dolor claves dentro de la organización.



¿Qué pasos se deben dar en la Migración?

Una vez identificados los puntos de dolor, se pueden llevar a cabo los siguientes pasos:

- Iniciar una evaluación para determinar el estado y la madurez de los procesos que se están ejecutando actualmente, si los hubiere.
- Elaborar una estrategia de migración mediante la identificación de los procesos y los habilitadores necesarios de COBIT 5 a ser implementados.
- Identificar los departamentos y servicios que se verán afectados por esta migración.

¿Qué pasos se deben dar en la Migración?

- Asegurarse de que se crea un plan de gestión de proyectos con las líneas de tiempo y se asigna un presupuesto para este esfuerzo.
- Ejecutar la actividad de la migración a través del proceso de gestión del cambio.
- Abordar las consecuencias del cambio organizacional que será creado por la migración y tener un plan de transición para hacer el roll-out de la migración.
- Comunicar el impacto positivo que se logrará con la migración para obtener el buy-in de la alta dirección.

¿Qué pasos se deben dar en la Migración?

- Se recomienda realizar ganancias rápidas y dar prioridad a las mejoras más beneficiosas que son más fáciles de implementar para motivar al equipo de migración y a la organización a continuar con el proyecto.

Conclusión General

A la luz del marco COBIT y la realidad de TI actual, se propone la adopción de un marco integral de gobierno y gestión de TI como punto de partida para:

- Administrar las TIC en la organización
- Determinar requerimientos mínimos del sistema de administración de seguridad
- Desarrollar estrategias de supervisión interna (cumplimiento, seguridad, auditoría interna)
- Desarrollar estrategias de supervisión externa (auditoría externa, leyes y regulaciones)
- Administrar riesgos de TI por factores internos y externos

Fuentes consultadas

- Alliance, B. S. (2014, June 1). *2013 Global Survey.* Retrieved June 30, 2014, from The Business Software Alliance: www.bsa.org
- Curtis. (2012). Risk Assesment in Practice. Carolina del Norte: COSO
- ISACA. (2012). *COBIT5 Framework.* Illinois: ISACA.
- ISACA. (2012). *COBIT5 Implementation.* Illinois: ISACA.
- ISACA. (2012). *COBIT5 and Infosec.* Illinois: ISACA.
- *ISACA. 2012. Manual de preparación CISA 2013. Illinois: ISACA*
- Leyes y Reglamentos de la República Dominicana: Ley Monetaria y Financiera183-02, Ley sobre derecho de audotr 65-00, Ley sobre crímenes y delitos de alta tecnología 53-07, Reglamento Riesgo Operacional (2009) y circulares relacionadas.
- Verizon. (2014). *Data Breach Investigations Report.* Verizon.