



Nivel de capacidad en las empresas de acuerdo con COBIT

Capacity level in companies according to COBIT

Christian René Castillo Carvajal¹, Harold Andrés Castillo², Oscar Alfonso Fernández³

Para citar este artículo: Castillo, C., Castillo, H., y Fernández, O. (2019). Nivel de capacidad en las empresas de acuerdo con COBIT. *TIA*, 7(1), pp. 16-21.

Resumen

Este artículo está diseñado para medir el nivel de capacidad en las empresas de acuerdo con el marco de trabajo de COBIT 5. En este sentido, se realizan una serie de pasos para llegar a conocer el estado en que se encuentra la empresa. En primer lugar, se empieza con la revisión de los objetivos a nivel de tecnología que se encuentren alineados con los de la empresa. En segundo lugar, el nivel de capacidad será medido de acuerdo con los controles que la empresa ha determinado para mitigar los riesgos que se presentan. Finalmente, la empresa conocerá el nivel de capacidad con la que se cuenta por cada uno de sus procesos, y se podrá saber que se debe realizar para mejorar.

Palabras clave: COBIT 5, framework, gobierno de TI, nivel de capacidad, procesos.

Abstract

This article is designed to measure the level of capacity in companies in accordance with the COBIT 5 framework. In this sense, a series of steps are taken to get to know the state of the company. First, it begins with the revision of the objectives at the technology level that are aligned with those of the company. Second, the level of capacity will be measured according to the controls that the company has determined to mitigate the risks that arise. Finally, the company will know the level of capacity available for each of its processes, and it will be possible to know what must be done to improve.

Keywords: COBIT 5, capacity level, enterprise IT, framework, process.

ARTÍCULO DE REFLEXIÓN

Fecha de recepción:
11-04-2018

Fecha de aceptación:
13-11-2019

ISSN: 2344-8288

Vol. 7 No. 1

Enero - Junio 2019

Bogotá-Colombia

¹ Ingeniero de Sistemas, Universidad Distrital Francisco José de Caldas, Colombia. Correo electrónico: chrcastillo@gmail.com

² Ingeniero de Sistemas, Universidad Distrital Francisco José de Caldas, Colombia. Correo electrónico: andre9_90@hotmail.com

³ Ingeniero de Sistemas, Universidad Distrital Francisco José de Caldas, Colombia. Correo electrónico: ocaferos@gmail.com

INTRODUCCIÓN

Actualmente la tecnología es un apoyo para las organizaciones en cuanto que es un activo valioso para el desarrollo de los procesos internos y de la información que esta genera y almacena. Por lo tanto, esta tecnología con el pasar del tiempo va evolucionando y con ella los procesos van cambiando y actualizando, para esto COBIT da un panorama de soporte y aplicación de procesos de manera más eficaz.

Muchas de las empresas que existen en Colombia desean aplicar marcos de trabajo o frameworks a sus empresas por varias razones ya que permite determinar en qué estado se encuentra la empresa actualmente, saber que se debe realizar para mejorar en el día a día los procesos internos de acuerdo con el framework, reconocer los beneficios en la tecnología de la información para impulsar el valor de sus interesados, etc.

¿QUÉ ES COBIT?

Es un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las Tecnologías de la Información (TI) corporativas. Dicho de una manera sencilla, COBIT ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

OBJETIVOS EN LA EMPRESA

Como primer paso para conocer el nivel de capacidad en la empresa es necesario que los objetivos que fueron definidos en la Planeación Estratégica de Tecnología de la Información (PETI) se encuentren alineados de acuerdo con los objetivos establecidos en la empresa y de acuerdo con el modelo de negocio que este se adapta.

RIESGOS DE LA EMPRESA

Los riesgos son las probabilidades de que las amenazas exploten los puntos débiles generando pérdidas o daños en los activos que impactan los objetivos de la organización. Estos representan para la empresa pérdidas sustanciales de reputación y marca empresarial, y creciente competencia por lo que se perderían clientes y a su vez dinero.

La ecuación de riesgo para cualquier empresa se expresa de la siguiente forma:

$$\text{RIESGO} = \text{ACTIVO} + \text{VULNERABILIDAD} + \text{AMENAZA} + \text{POSIBILIDAD} + \text{IMPACTO}.$$

Es por esto que la empresa debe determinar qué riesgos son los que se encuentran presentes y qué afecta directamente al incumplimiento de los objetivos de TI para generar los controles que mitiguen el impacto o la posibilidad con que se presentan.

CONTROLES DE LA EMPRESA

Los controles son disposiciones establecidas por la organización para mitigar la probabilidad de existencia de riesgos que afectan los activos de información. Estos pueden ser tipo administrativo, técnico o físico dependiendo de la protección que se realizará contra la amenaza.

- Control administrativo: si se desea que los usuarios de una aplicación X tengan una complejidad en la contraseña se debe generar una política de contraseñas.
- Control técnico: si se desea que la empresa este blindada contra páginas web que puedan afectar a los activos por virus o similares se genera bloqueos a nivel de firewall.
- Control físico: si la empresa no desea restringir el acceso a ciertas áreas de la empresa se deben implementar controles biométricos.

Estos controles tienen una forma de ejecución ya sea manual, automático, semiautomático o manual por su naturaleza, y un tipo de control de tipo preventivo, correctivo, detectivo, disuasivo, de monitoreo, etc., por lo tanto, es indispensable que la empresa, que es la que conoce el negocio, realice un análisis sobre qué realizar para mitigar el riesgo, lo cual es posible mediante COBIT 5 ya que se podrá establecer el nivel de capacidad con el que cuenta la empresa.

NIVEL DE CAPACIDAD DE COBIT

COBIT define en su versión quinta (5) seis niveles de capacidad que son alcanzados independientemente de cada proceso enmarcado en la empresa. Estos son listados a continuación:

- 0 proceso incompleto: El proceso no está implementado o no alcanza su propósito. A este nivel hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- 1 proceso ejecutado (un atributo): El proceso implementado alcanza su propósito.
- 2 proceso gestionado (dos atributos): El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- 3 proceso establecido (dos atributos): El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- 4 proceso predecible (dos atributos): El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- 5 proceso optimizado (dos atributos): El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

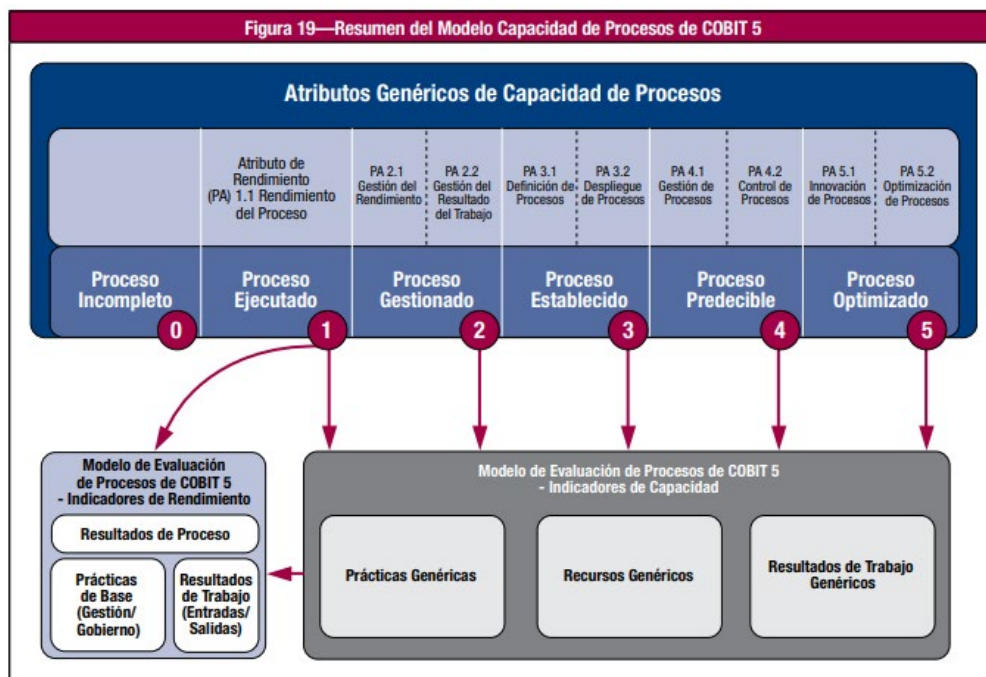


Figura 1. Capacidad de Procesos COBIT 5.

Fuente: [1].

Estos procesos en su calificación son con enfoque de la norma ISO/IEC 15504 en donde se afirma que un nivel solo puede alcanzar el siguiente nivel si cumple totalmente el nivel inferior, ejemplo:

“Un nivel 3 de capacidad de proceso (establecido) requiere que los atributos de definición y despliegue del proceso se hayan alcanzado ampliamente, sobre la consecución completa de los atributos del nivel 2 de capacidad de procesos (proceso gestionado)” COBIT 5.

Esto quiere decir que si el proceso gestionado no se encuentra planificado, supervisado y ajustado de tal manera que brinde resultados con base en una correcta ejecución del proceso no se podría encontrar en un nivel establecido porque este define la existencia de un documento formal de la correcta implementación para la obtención de resultados.

Esto es verificado en la aplicación de cada uno de los procesos internos de la organización para dar un claro status o evaluación en general de la organización específica por áreas de los procesos internos que realiza la empresa. De acuerdo con la evaluación específica se dan enfoques o recomendaciones en la mejora y/o corrección de procesos en ejecución para conseguir el objetivo establecido por la Gestión de Tecnología (GT) dentro de la empresa.

Estas recomendaciones están alineadas en los procesos de COBIT 5 donde si son requeridos en el gobierno participa el EDM (Evaluar, Orientar y Supervisar) y si son enfocados en la gestión realizada en los procesos internos de la organización participa los APO (Alinear, Planificar y Organizar), el BAI (Construir, Adquirir e Implementar), el DSS (Entregar, Dar Servicio y Soporte) y el MEA (Supervisar, Evaluar y Valorar).

Los beneficios que proporciona COBIT 5 con su modelo de capacidad son los siguientes:

- Enfoque mejorado en los procesos en ejecución para confirmar que se está realmente

consiguiendo su objetivo y que está entregando los resultados esperados.

- Confiabilidad y repetitividad mejorada de las actividades y valoraciones de la evaluación de la capacidad de los procesos reduciendo discusiones y falta de acuerdo entre las partes interesadas sobre los resultados de la evaluación.
- Incremento de la utilidad de los resultados de la evaluación de la capacidad de los procesos ya que el nuevo modelo establece una base para que se lleven a cabo evaluaciones más formales y rigurosas, tanto para propósitos internos como externos.
- Cumplimiento con un estándar de evaluación de procesos generalmente aceptado y de esta forma con un fuerte soporte al enfoque de evaluación de procesos por el mercado.

En la Figura 2, se muestra la categoría de habilidades que pueden tener el campo de acción los procesos de COBIT 5.

EVALUACIONES DE CAPACIDAD

Estas evaluaciones pueden ser utilizadas por varios factores y con diferentes grados de rigor. Uno de estos es el interno, que es con el fin de comparar las distintas áreas de la empresa o para la mejora de los mismos procesos para beneficio propio de la empresa. Otro factor es el externo que son enfocados en las evaluaciones formales, informes y certificaciones.

MODELO DE REFERENCIA DE PROCESOS DE COBIT 5

Para finalizar se expone el modelo de referencia de procesos de COBIT 5, en la Figura 3, en donde se encuentran los 37 procesos de COBIT 5 en la aplicación de gobierno y gestión de TI, comúnmente llamados *procesos catalizadores*.

Figura 39—Categorías de Habilidades de COBIT 5	
Dominio de Procesos	Ejemplos de Categorías de Habilidades
Evaluar, Orientar y Supervisar (EDM)	<ul style="list-style-type: none"> • Gobierno de TI Empresarial
Alinear, Planificar y Organizar (APO)	<ul style="list-style-type: none"> • Formulación de políticas de TI • Estrategia TI • Arquitectura de la empresa • Innovación • Gestión Financiera • Gestión de la Cartera
Construir, Adquirir e Implementar (BAI)	<ul style="list-style-type: none"> • Análisis de Negocios • Gestión de Proyectos • Evaluación de Usabilidad • Definición de requisitos y gestión • Programación • Ergonomía de Sistemas • Retirada del servicio de software • Gestión de la Capacidad
Entregar, dar Servicio y Soporte (DSS)	<ul style="list-style-type: none"> • Gestión de la disponibilidad • Gestión de los Problemas • Servicio de recepción y gestión de incidentes • Administración de la seguridad • Operaciones TI • Administración de base de datos
Supervisar, Evaluar y Valorar (MEA)	<ul style="list-style-type: none"> • Revisión de cumplimiento • Supervisión del rendimiento • Auditoría de Controles

Figura 2. Categorías de habilidades de COBIT 5.

Fuente: [1].

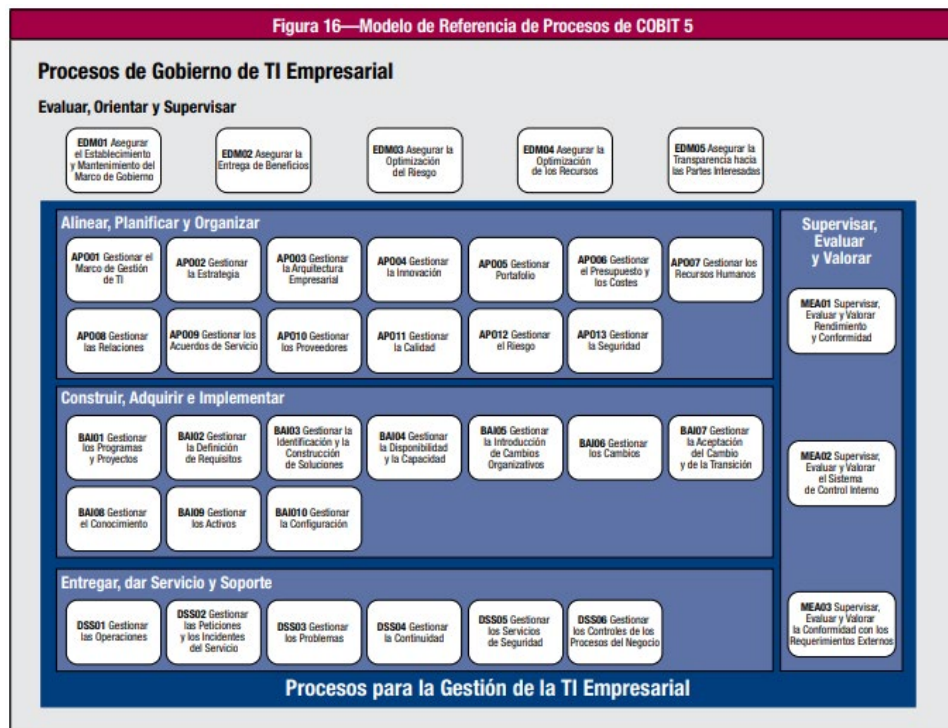


Figura 3. Modelo de Referencia de Procesos de COBIT 5.

Fuente: [1]

CONCLUSIONES

- El nivel de capacidad que ofrece este marco de trabajo (COBIT 5) va enmarcado en un proyecto con inicio y fin, el cual se establece para medir el nivel en el que se encuentra la organización de acuerdo con los controles que ya se han definido para mitigar los riesgos.
- De la revisión del nivel de capacidad en una empresa se pueden establecer recomendaciones para mejorar o generar controles suplementarios para el cumplimiento del proceso en el que está alineado.
- COBIT al ser un marco de trabajo brinda un panorama de la gestión de TI empresarial, por lo que cada empresa de acuerdo con su modelo de negocio puede que no aplique a uno o varios procesos que COBIT dispone.

RECOMENDACIONES

Como trabajo complementario a este se puede pensar en las evaluaciones que se realizan con respecto a este marco de trabajo pensando en las certificaciones externas para las empresas que desean obtenerlo.

AGRADECIMIENTOS

A Victor Vasquez y Dora Arismendi gerentes de KPMG con experiencia de más de 10 años auditando tecnología en Colombia por la estructura de este artículo y para la presentación de este a la materia de Gestión y Modelado de la Información de la especialización de Proyectos Informáticos de la Universidad Distrital.

REFERENCIAS

- [1] ISACA, *Un marco de negocio para el gobierno y la gestión de las TI de la empresa. COBIT 5*. Rolling Meadows, Illinois: ISACA, 2012.
- [2] A. Almanza, *La aplicación de Cobit en las organizaciones ¿vale la pena el esfuerzo?*, 2012. [En línea]. Disponible en: <http://repository.unimilitar.edu.co/bitstream/10654/6537/2/AlmanzaGomezAlvarovan2012.pdf>
- [3] C. Francavilla, *Como aporta COBIT 5 y gobernanza de TI a la gobernanza empresarial*, 2014. [En línea]. Disponible en: <https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014-CO-BIT%20y%20Gobernanza%20de%20TI.pdf>
- [4] M. de la Torre, L. Giraldo, C. Villalta, *Diagnóstico para la implantación de COBIT en una empresa de Producción. Área Piloto: Departamento de Sistemas*, 2012. [En línea]. Disponible en: <https://dspace.ups.edu.ec/bitstream/123456789/2695/13/UPS-GT000307.pdf>
- [5] Universidad EAFIT, *COBIT: Modelo para auditoría y control de sistemas de información*, 2007. [En línea]. Disponible en: <http://www.eafit.edu.co/es-cuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf>
- [6] R. Quintero, *TI y la entrega de valor en la empresa*, 2013. [En línea]. Disponible en: <https://www.auditool.org/blog/auditoria-de-ti/603-ti-y-la-entrega-de-valor-en-la-empres>