FUNDAMENTOS PARA OBJETIVOS DE CONTROL

EN LAS TIC

ISBN: 978-9942-28-558-4
Título: Fundamentos para Objetivos de Control en las TIC
Autor: Quintanilla Romero, Marco Antonio
Autor: Crespo Alban, Guido Gonzalo
Editorial: MQR®

Materia: Educación. investigación. temas relacionados con la tecnología
Publicado: 2017-04-07
NºEdición: 2
Idioma: Español

www.uceinvestigar.com

FUNDAMENTOS PARA OBJETIVOS DE CONTROL EN LAS TIC

ÍNDICE

1. INTRODUCCIÓN

1.1. Antecedentes

Las empresas poseen un capital activo muy valioso: información y tecnología. Cada vez en mayor medida, el éxito de una empresa depende de la comprensión de ambos componentes. Las buenas prácticas concentradas en el marco de referencia COBIT, permiten que los negocios se alineen con la tecnología de la información para así alcanzar los mejores resultados.

La información y la tecnología que la soporta representan los activos más valiosos de muchas empresas, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados. Estas empresas también entienden y administran los riesgos asociados, es decir, el aumento en los requerimientos regulatorios, así como también una gran dependencia de muchos de los procesos de negocio en TI. Pero todos estos elementos son clave para el gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

De esta forma COBIT es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio.

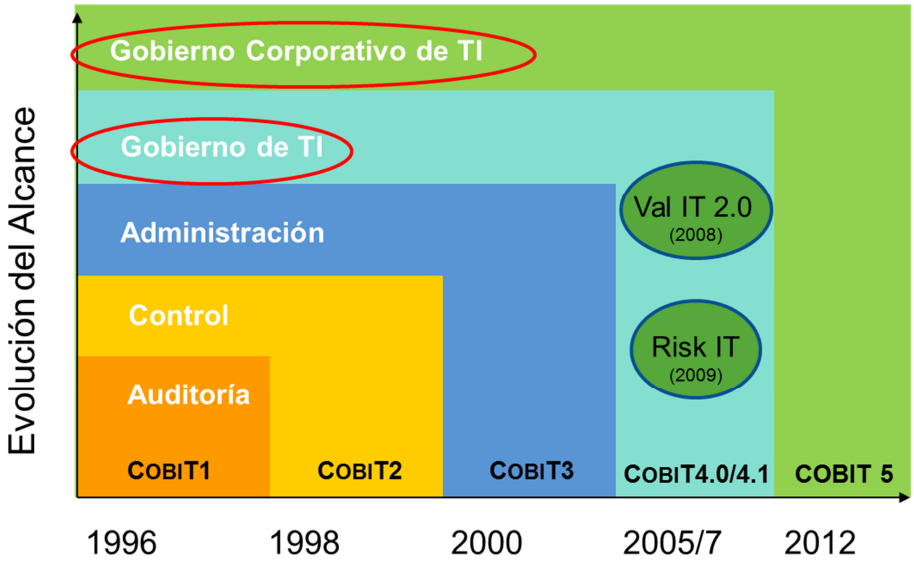
COBIT permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización.

COBIT enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio.

Adicionalmente COBIT busca brindar mejoras a diferentes niveles:

- Compendio de mejores prácticas aceptadas internacionalmente.
- Orientado al gerenciamiento de las tecnologías.
- Complementado con herramientas y capacitación.
- Respaldado por una comunidad de expertos.
- En evolución permanente de acuerdo al sistema empresarial.
- Mantenido por una organización sin fines de lucro, con reconocimiento internacional (ISACA).
- Mapeado con otros estándares.
- Orientado a Procesos, sobre la base de Dominios de Responsabilidad.

Finalmente se presenta la evolución que ha tenido COBIT en sus diferentes versiones y publicaciones que se han emitido, lo cual se menciona a continuación:



Como se puede observar en la gráfica detallada anteriormente, el marco de referencia COBIT ha evolucionado de manera importante, es decir de ser una herramienta de auditoría (COBIT 1) a convertirse en un marco de gobierno de tecnología de la información (COBIT 5).

1.2. Resumen Ejecutivo

Administración de la Información:

COBIT 5 de ISACA es el único marco de negocios para la administración y la gestión de la información y la tecnología en la empresa. Ofrece principios, prácticas, herramientas analíticas y modelos aceptados mundialmente diseñados para ayudar a los líderes de negocios y de TI a maximizar la confianza y el valor de la información y de los activos de tecnología de su empresa.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

Está diseñada para los gerentes de seguridad de la información, los gerentes de seguridad corporativa, los usuarios finales, los proveedores de servicios, los administradores de TI y los auditores de TI para alinear principios de ciber seguridad con una estrategia general para el gobierno, la gestión del riesgo y el cumplimiento, así como ocho principios para transformar la seguridad.

Áreas de Enfoque del Gobierno de TI

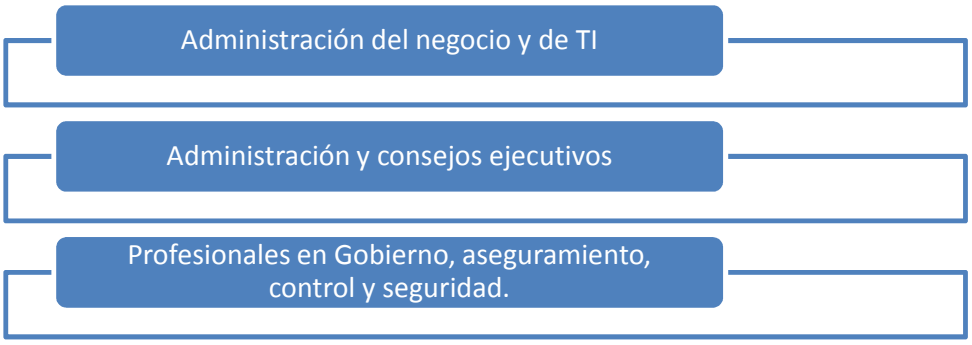
Las áreas de enfoque del gobierno de TI, COSO, recursos TI de COBIT y criterios de información COBIT), ofrecen un puente entre lo que los gerentes operativos deben realizar y lo que los ejecutivos desean gobernar.

El Gobierno asegura que los objetivos de la empresa se logren mediante la evaluación de las necesidades de las partes interesadas, las condiciones y opciones, estableciendo la dirección a través de la priorización y decisión, y monitoreando el del ejercicio de gobierno y la gestión eficaz en la práctica requiere el uso adecuado de todos los facilitadores.

El proceso COBIT como modelo de referencia nos permite enfocar fácilmente sobre las actividades empresariales relevantes.

El modelo de referencia COBIT 5 subdivide proceso de las prácticas relacionadas con la TI y las actividades de la empresa en dos grandes áreas: la gobernanza y la gestión con la administración dividida en dominios de los procesos

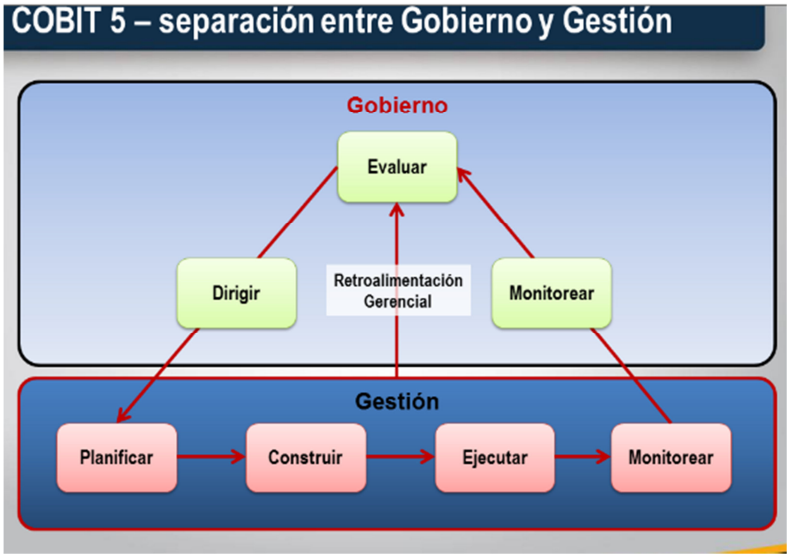
Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a lo siguiente:



- Se proyecta como una guía específica para los profesionales de la Seguridad de la Información y otros interesados
- Se construye sobre el marco del COBIT 5, un enfoque robusto para el gobierno y la gestión de la seguridad de la información, sobre la base de los procesos de negocios de la organización
- Presentará una visión extendida del COBIT 5 , que explica cada uno de sus componentes desde la perspectiva de la seguridad
- Creará valor para todos los interesados a través de explicaciones, actividades, procesos y recomendaciones
- Propondrá una visión del gobierno y la gestión de la seguridad de la información mediante una guía detallada para establecerla, implementarla y mantenerla, como parte de las políticas, procesos y estructuras de la organización

El gobierno asegura que los objetivos empresariales se logran evaluando las necesidades de los accionistas, las condiciones y opciones; establecer la dirección a través de la priorización y la toma de decisiones; y monitorear el desempeño, el cumplimiento y el progreso versus la dirección y objetivos acordados.

Por su parte la gestión se ocupa de planificar, construir, ejecutar y monitorear las actividades alineadas con la dirección establecida por el organismo de gobierno para el logro de los objetivos empresariales.



Si bien estos estándares y modelos enfatizan el control del negocio y la seguridad y servicio de TI, COBIT es el único que se ocupa de los controles específicos de TI desde la perspectiva del

negocio. De hecho, COBIT 5 se basa en ISO/IEC 15504 e ITIL. No se pretende que COBIT reemplace estos modelos de control, sino lo que se destacan son los elementos de gobierno y gestión y las prácticas necesarias para crear valor para la compañía.

La cultura empresarial es de vital importancia. Una cultura proactiva será más receptiva que una que no lo es. Sin embargo, hay que considerar el énfasis que COBIT hace en la creación de valor para el accionista por estar guiado por los objetivos del negocio, la alineación con estándares internacionales reconocidos y su simplicidad. Las áreas de gobierno y gestión emanan de tan sólo 5 principios y 7 habilitadores.

Marco de Negocio para el Gobierno y la Gestion de las TI de la empresa

La publicación COBIT 5 contiene el marco COBIT 5 para el gobierno y la gestión de las TI de la empresa. La publicación es parte de la familia de productos de COBIT 5:

El marco COBIT 5 se construye sobre cinco principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI de la empresa.

2. PRINCIPIOS DE COBIT 5

2.1. Principio 1 – Satisfacer las Necesidades de las Partes Interesadas

Las compañías 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.

Los indicadores clave de metas y de proceso permiten traducir las necesidades de los interesados, internos y externos utilizando la estrategia empresarial "cascada de metas", que comienza con las

metas de la empresa, continúa con las metas relacionadas de TI, que se convierte en "habilitadores", y finalmente se alcanzan al desarrollar las actividades de las metas.

Cascada de Metas de COBIT 5

Las metas en cascada de COBIT 5 traducen las necesidades de las Partes Interesadas en metas específicas, accionables y personalizadas dentro del contexto de la Organización, de las metas relacionadas con la TI y de las metas habilitadoras. Las necesidades de las partes interesadas están influenciadas por los cambios de estrategia, un negocio y entorno regulatorio cambiantes y las nuevas tecnologías.

Permite definir las prioridades para implementar, mejorar y asegurar el gobierno corporativo de la TI, en base de los objetivos (estratégicos) de la Organización y los riesgos relacionados.
Definen los objetivos y las metas tangibles y relevantes, en diferentes niveles de responsabilidad.

Filtran la base de conocimiento de COBIT 5, en base de las metas corporativas para extraer una orientación relevante para la inclusión en los proyectos específicos de implementación, mejora o aseguramiento.

Identifican y comunican qué importancia tienen los habilitadores (algunas veces muy operacionales) para lograr las metas corporativas.

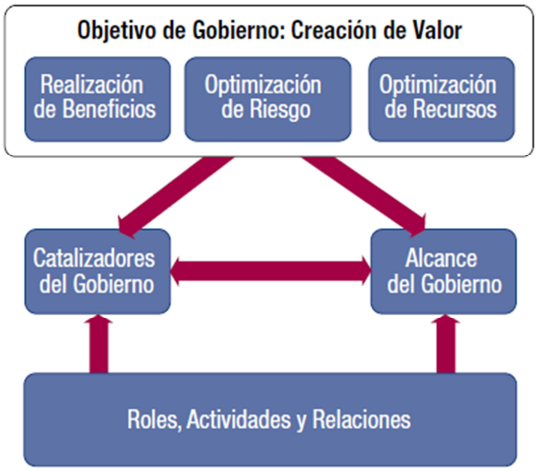
El logro de metas empresariales requiere un número de resultados relacionados con las TI que están representados por las metas relacionadas con las TI.

2.2. Principio 2 – Cubrir la Empresa de Extremo a Extremo

COBIT 5 integra el gobierno y la administración de la tecnología de la información relacionadas desde una perspectiva integral a nivel de toda la Organización. Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas, contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

Proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI basada en varios catalizadores.

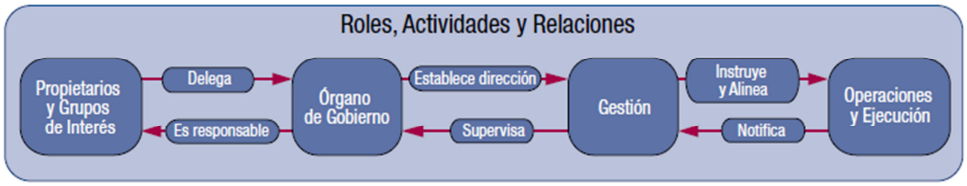
Los catalizadores permite a cada grupo de interés definir requisitos exhaustivos y completos para la información y el ciclo de vida de procesamiento de la información, conectando de este modo el negocio y su necesidad de una información adecuada y la función TI, y soportando el negocio y el enfoque de contexto.



Catalizadores de Gobierno.- Son los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que o hacia los que las acciones son dirigidas y los objetivos pueden ser alcanzados.

Alcance de Gobierno.- El alcance de COBIT 5 es la empresa. El gobierno puede ser aplicado a toda la empresa, a una entidad, a un activo tangible o intangible, etc.

Roles, Actividades y Relaciones.- Un último elemento son los roles, actividades y relaciones de gobierno. Definen quién está involucrado en el gobierno, como se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno.

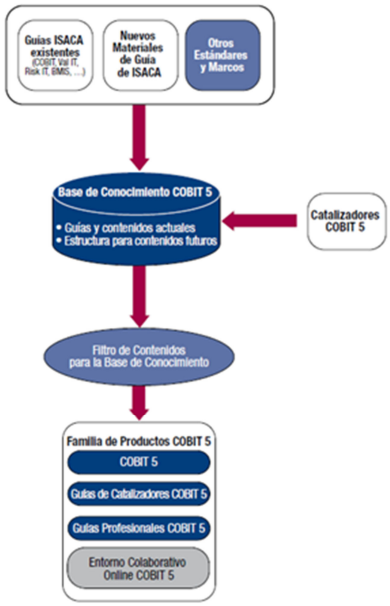


2.3. Principio 3 – Aplicar un Marco de Referencia Único Integrado

COBIT 5 está alineado con los últimos marcos y normas relevantes usadas por las organizaciones:

- Corporativo: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000.
- Relacionado con TI: ISO/IEC 38500, ITIL, la serie ISO/IEC 27000, TOGAF, PMBOK/PRINCE2, CMMI

Se está desarrollando el modelo de capacidad de los procesos para facilitar al usuario de COBIT el mapeo de las prácticas y actividades contra los marcos y normas de terceros.



2.4. Principio 4 – Hacer Posible un Enfoque Holístico

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI, impulsados por las metas en cascada, es

decir las metas de alto nivel relacionadas con la TI definen qué deberían lograr los diferentes habilitadores.

Los habilitadores están descritos por el marco de COBIT 5 **en siete categorías**.

- **Principios, políticas y marcos de referencia:** son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.

- **Procesos:** describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

- **Estructuras organizativas**: son las entidades de toma de decisiones clave en una organización.

- **Cultura, ética y comportamiento**: son a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.

- **Información:** impregna toda la organización e incluye toda la producida y utilizada por la empresa, esta es necesaria para mantener la organización funcionando, a nivel operativo, la información es el producto clave de la empresa.

- **Servicios, infraestructuras y aplicaciones**: incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

- **Personas, habilidades y competencias**: están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la toma de decisiones y de acciones correctivas.

Dimensiones de los Catalizadores de COBIT 5

Todos los catalizadores tienen un conjunto de dimensiones comunes que permite a una entidad manejar sus complejas interacciones y facilita resultados exitosos

Las cuatro dimensiones comunes de los catalizadores son:

1. Grupos de interés
2. Metas
3. Ciclo de vida
4. Buenas prácticas

Posteriormente en la sección 3 se realizará una explicación detallada de los habilitadores y catalizadores respectivamente.

2.5. Principio 5 – Separar el Gobierno de la Gestión

El marco de COBIT 5 realiza una clara distinción entre gobierno y gestión; estos dos métodos abarcan diferentes tipos de actividades y necesidades de acuerdo a los requerimientos de la organización, las mismas que tiene diferentes estructuras de acuerdo a los niveles organizacionales y que serán utilizadas para diversos propósitos.

La posición de COBIT 5 sobre esta fundamental distinción entre gobierno y gestión es:

1. **Gobierno.-** El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo de administración bajo la dirección de su presidente.

Es necesario identificar los tipos de gobiernos que existen:

- Gobierno Corporativo
- Gobierno de Proyectos
- Gobierno de Tecnologías de Información
- Gobierno Ambiental
- Gobierno Económico y Financiero

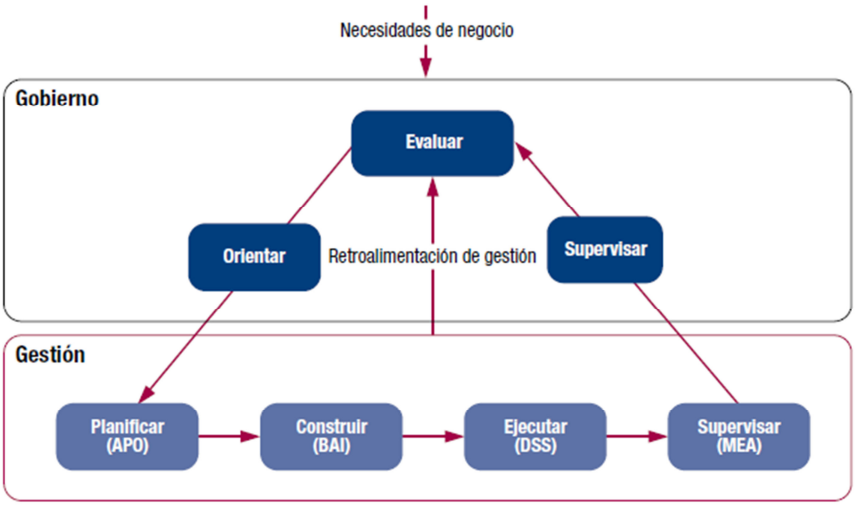
Cada uno de estos tipos de organización enlistados tiene una o más fuentes de orientación, cada uno con los objetivos similares pero con frecuencia varían los términos, las técnicas y metodologías para su realización y aplicación.

Estos enfoques se basan normalmente en facilitadores de diversos tipos por ejemplo: los principios, las políticas, los modelos arcos, estructuras organizacionales.

Ejemplo de un Modelo de Gobierno

2. **Gestión.-** La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales, la descripción de este proceso es continuamente identificar, evaluar y reducir los riesgos relacionados con TI dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa CEO.

El objetivo de este proceso es integrar la gestión de riesgos empresariales relacionados con TI con el ERM en general y equilibrar los costos y beneficios de la gestión de riesgos de la empresa.



Dado el papel de gobierno evaluar, orientar y vigilar – se requiere un conjunto de interacciones entre gobierno y gestión para obtener un sistema de gobierno eficiente y eficaz.

Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. COBIT 5 proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. Es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas es uno de los pasos más importantes y críticos hacia el buen gobierno.

Interacciones entre Gobierno y Gestión

De acuerdo a los mencionado por (ISACA, 2012),"Partiendo de las definiciones entre gobierno y gestión, está claro que comprenden diferentes tipos de actividades, con diferentes responsabilidades; sin embargo, dado el papel de gobierno – evaluar, orientar y vigilar – se requiere un conjunto de interacciones entre gobierno y gestión para obtener un sistema de gobierno eficiente y eficaz." Estas interacciones, empleando una estructura de catalizadores, se muestran a alto nivel en la figura 14

Figura 14—Interacciones Gobierno y Gestión en COBIT 5	
Catalizador	**Interacción Gobierno-Gestión**
Procesos	En el ilustrativo modelo de procesos de COBIT 5 (COBIT 5: Procesos Catalizadores), se distingue entre los procesos de gobierno y de gestión, incluyendo conjuntos específicos de prácticas y actividades para cada uno. El modelo de procesos también incluye una matriz RACI que describe las responsabilidades de las diferentes estructuras organizativas y roles en la empresa.
Información	El modelo de procesos describe las entradas y salidas de los distintos procesos basados en prácticas a otros procesos, incluyendo la información intercambiada entre los procesos de gobierno y gestión. La información empleada en evaluar, orientar y supervisar la TI empresarial es intercambiada entre gobierno y gestión tal y como se describe en las entradas y salidas del modelo de procesos.
Estructuras organizativas	En cada empresa, se definen varias estructuras organizativas; en función de su composición y ámbito de decisiones, las estructuras pueden ubicarse en el área de gobierno o en el de gestión. Dado que el gobierno trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno - por ejemplo, decidir sobre la cartera de inversiones y establecer el umbral de riesgo - y las decisiones y operaciones que las implementan.
Principios, políticas y marcos	Los principios, políticas y marcos son los vehículos mediante los cuales las decisiones de gobierno son sancionadas en la empresa, y por esa razón son una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones).
Cultura, ética y comportamientos	El comportamiento también es un catalizador clave del buen gobierno y la gestión empresarial. Se establece al más alto nivel (liderando mediante el ejemplo) y es, por tanto, una interacción importante entre el gobierno y la gestión.
Personas, habilidades y competencias	Las actividades de gobierno y de gestión requieren conjuntos de habilidades distintas, pero una habilidad esencial para miembros tanto del órgano de gobierno como de gestión es entender tanto las propias actividades como cuáles son sus diferencias.
Servicios, infraestructura y aplicaciones	Se requieren servicios, soportados por las aplicaciones e infraestructura, para proporcionar la información adecuada al órgano de gobierno y soportar las actividades de gobierno a la hora de evaluar, establecer la orientación y supervisar.

Modelo de Referencia de Procesos de COBIT 5

COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas en las áreas Clave de Gobierno y Gestión de COBIT 5. Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Empresas más pequeñas pueden tener pocos procesos; empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas. COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular. La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI, es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El proceso administrativo

Según el autor (Henry, 1879) “Un proceso es el conjunto de pasos o etapas para llevar a cabo una actividad, y en el proceso administrativo se distinguen fases o etapas sucesivas a través de las

cuáles se efectúa la administración, mismas que se interrelacionan y forman un proceso integral. Tales etapas son: planificación, organización, dirección y control”

Cada dominio contiene un número de procesos. A pesar de que, según hemos descrito antes, la mayoría de los procesos requieren de actividades de “planificación”, “implementación”, “ejecución” y “supervisión”, bien en el propio proceso, o bien en la cuestión específica a resolver (como por ejemplo: calidad, seguridad), están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial. El modelo de referencia de procesos de COBIT 5 es el sucesor del modelo de procesos de COBIT 4.1 e integra también los modelos de procesos de Risk IT y Val IT. La figura 16 muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5. Los detalles de todos los procesos, de acuerdo con el modelo de proceso anteriormente descrito, están recogidos en la guía COBIT 5: Procesos Catalizadores.

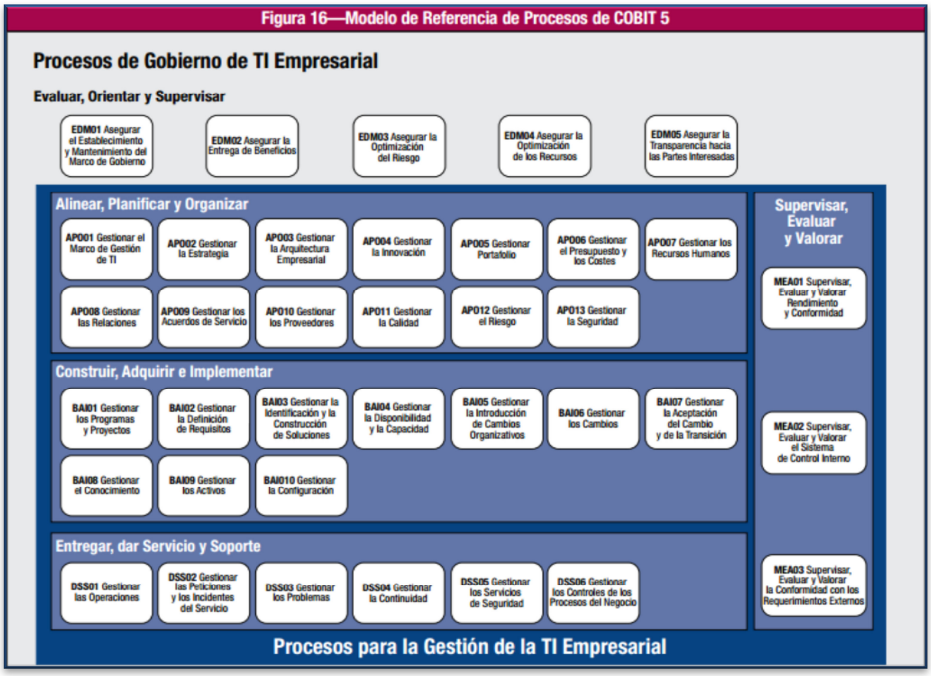
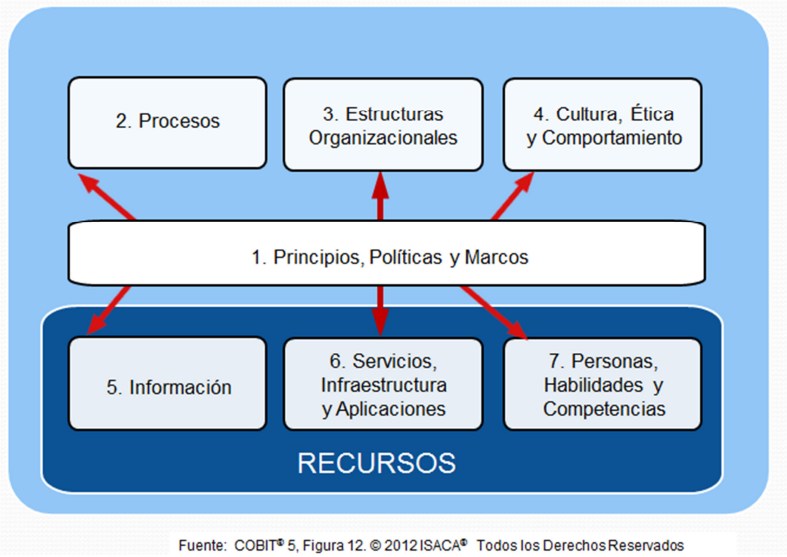


Figura 16—Modelo de Referencia de Procesos de COBIT 5

3. HABILITADORES DE COBIT 5



Fuente: COBIT® 5, Figura 12. © 2012 ISACA® Todos los Derechos Reservados

COBIT 5 une los cinco 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.

3.1. Habilitador 1 – Principios, Políticas y Marcos

Los principios y las políticas se refieren a los mecanismos de comunicación disponibles para trasmitir la dirección e instrucciones de los cuerpos de gobierno y de dirección. En la siguiente figura se muestran las particularidades del catalizador principios, políticas y marco de referencia comparadas con una descripción genérica de un catalizador.

El modelo de principios, políticas y marcos de trabajo muestra:

- **Partes Interesadas**: En los principios y políticas, las partes interesadas pueden ser internas o externas a la empresa.

Éstas incluyen el Consejo y el comité ejecutivo de dirección, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores del servicio, clientes y agencias reguladoras. Sus intereses están divididos: Algunas partes interesadas definen y establecen las políticas mientras que las otras tienen que alinearse y cumplir con ellas.

- **Metas y métricas**: Los principios, políticas y marcos de referencia son los instrumentos para comunicar las reglas, en apoyo a las metas de gobierno y los valores de la empresa, conforme los define el Consejo y el comité ejecutivo de dirección.

Los principios han de ser:

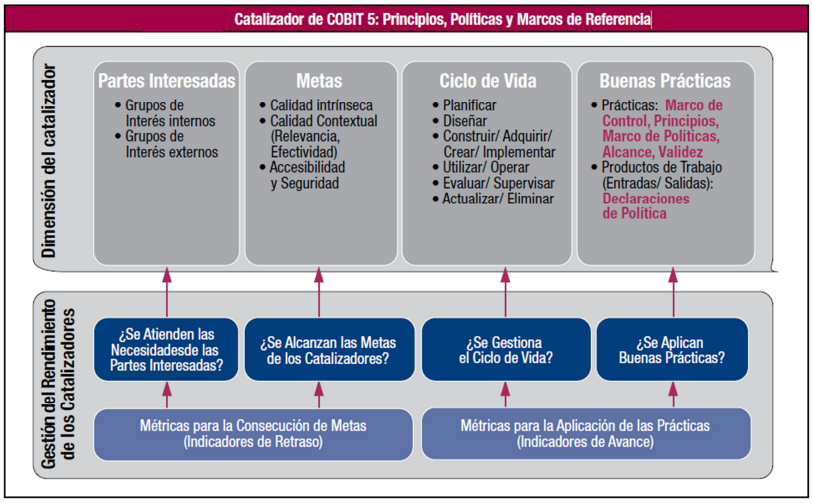
- Limitados en número
- Redactados en un lenguaje sencillo, expresando de la forma más clara posible, los valores fundamentales de la empresa.

Las políticas proporcionan una directriz más detallada respecto a cómo llevar a la práctica los principios y su influencia respecto a cómo la toma de decisiones se alinea con dichos principios.

Unas buenas políticas son:

- Efectivas – Logran el propósito establecido.
- Eficientes – Garantizan que los principios se implementan de la forma más eficiente posible.
- No intrusivas – Parecen lógicas para quiénes han de cumplir con ellas, es decir, no generan resistencia innecesaria.

Acceso a las políticas – ¿existen mecanismos que proporcionen un acceso fácil a las políticas a todas las partes interesadas? En otras palabras, ¿las partes interesadas saben dónde encontrar las políticas?



Los marcos de gestión y gobierno deberían proporcionar a la dirección una estructura, directrices, herramientas, etc. Que permitan la adecuada gestión y gobierno TI de la empresa. Los marcos de trabajo deberían ser:

- Exhaustivos, cubriendo todas las áreas necesarias.
- Abiertos y flexibles, permitiendo su adaptación a la situación específica de la empresa.
- Actualizados, es decir, reflejando la dirección y objetivos de gobierno actuales de la empresa.
- Disponibles y accesibles a todas las partes interesadas.
- **Ciclo de vida:** Las políticas tienen un ciclo de vida que ha de apoyar la consecución de las metas definidas. Los marcos de referencias son clave porque proporcionan la estructura para definir una directriz coherente. Por ejemplo, un marco de referencias para políticas proporciona la estructura con la que se pueden crear y mantener un conjunto coherente de éstas y proporciona también el ámbito en el que movernos y navegar dentro de y entre ellas.

En función del entorno exterior en el que opere la empresa, pueden existir requerimientos normativos de diferentes niveles que requieran fuertes controles internos y, como consecuencia, un marco fuerte de políticas. Se debe prestar especial atención, en lo que respecta a marcos de trabajo y políticas, a la actualización de dichas políticas – cuando éstas se revisan y actualizan, ¿existen mecanismos sólidos que garanticen que las personas están al corriente de las novedades, que las nuevas versiones se ponen fácilmente a disposición (ver punto anterior) y que la información obsoleta se archiva o elimina?

- **Buenas prácticas:**

Las buenas prácticas requieren que las políticas formen parte del marco de gobierno y de gestión general, proporcionando una estructura (jerárquica) a la que deberían ceñirse todas las políticas y actuando de enlace con los principios subyacentes.

Como parte del marco de políticas, se han de describir los siguientes elementos:

- El alcance y la validez
- Las consecuencias por no cumplir con la política
- El significado de la gestión de las excepciones
- La forma con la que se ha de comprobar y medir el cumplimiento con la política

Está generalmente reconocido que los marcos de gestión y gobierno pueden proporcionar una directriz valiosa respecto a las afirmaciones que se vayan a incluir en las políticas.

Las políticas deberían estar alineadas con el umbral de riesgo de la empresa. Las políticas son un componente clave de los sistemas de control interno en la empresa, cuyo propósito es gestionar y contener el riesgo. Como parte de las actividades de gobierno sobre los riesgos, se define la tolerancia de la empresa a los mismos, debiendo ésta quedar reflejada en las políticas. Una empresa adversa al riesgo tendrá políticas más restrictivas que una empresa más agresiva.

Las políticas necesitan ser revalidadas y/o actualizadas a intervalos regulares.

- **Relaciones con otros catalizadores**—Las relaciones con otros catalizadores incluyen:

Los principios, políticas y marcos de referencia deberían reflejar la cultura y valores éticos de la empresa y éstos deberían fomentar el comportamiento deseado; por lo tanto, hay una relación fuerte con el catalizador cultura, ética y comportamiento.

La práctica de los procesos y las actividades son el vehículo más importante para la ejecución de las políticas.

Las estructuras organizativas pueden definir e implementar políticas en su ámbito de control; sus actividades también están definidas por políticas.

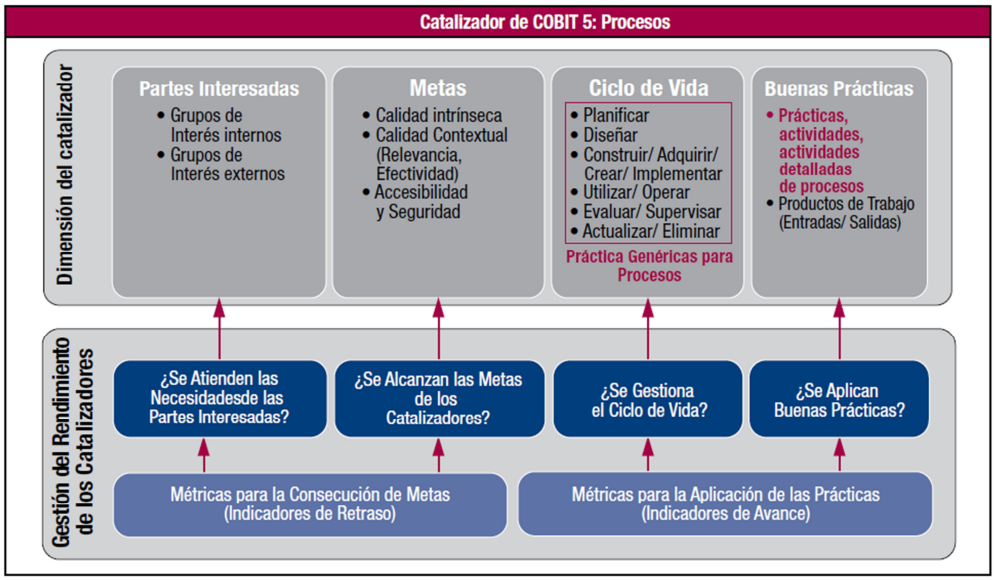
Las políticas también son información, por lo tanto todas las buenas prácticas que aplican a la información aplican también a las políticas.

MEDIOS SOCIALES
Una empresa está considerando la manera de afrontar el rápido crecimiento del uso de los medios sociales de comunicación y la presión de sus empleados para disponer de pleno acceso. Hasta ahora, la organización ha sido conservadora o restrictiva en la dotación de accesos a este tipo de servicios, principalmente por razones de seguridad. Hay presión desde diferentes frentes para adoptar otra posición respecto a los medios sociales. Los empleados reclaman niveles de acceso similares a los domésticos, y la organización también desea utilizar y explotar los beneficios de los medios sociales para fines relacionados con el marketing y comunicación pública. Se adopta la decisión de definir una política de uso de los medios de sociales en sistemas y redes de la empresa, incluyéndose los ordenadores portátiles que ésta proporciona a sus empleados. La nueva política se ajusta al marco de políticas existentes bajo la categoría de "políticas de uso aceptado", la cuál es más relajada que las políticas precedentes. En consecuencia, se desarrolla la comunicación para explicar las razones de la nueva política. Al mismo tiempo, también hay impacto en otros catalizadores: • Los empleados necesitan aprender cómo tratar con el nuevo medio para evitar situaciones embarazosas para la empresa. Necesitan aprender comportamientos adecuados en línea con la nueva dirección que está tomando su empresa y desarrollar así las habilidades adecuadas. • Se necesitan efectuar cambios en varios procesos relacionados con la seguridad. Se abre el acceso a un nuevo medio, de manera que se necesitan cambiar configuraciones y parámetros de seguridad y, posiblemente, se necesiten definir determinadas medidas compensatorias.

Nota: COBIT 5 es un ejemplo de marco de trabajo según se describe en este catalizador.

3.2. Habilitador 2 – Procesos

En la siguiente figura se muestran las particularidades del catalizador procesos comparadas con la descripción genérica de los catalizadores.



Un proceso se define como 'una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de un número dado de fuentes (incluyéndose otros procesos), manipulando las entradas y produciendo salidas (p. ej., productos, servicios).'

El modelo de los procesos muestra:

- **Partes interesadas**: Los procesos tienen partes interesadas internas y externas, cada una con sus propios roles; las partes interesadas y sus niveles de responsabilidad están documentadas en las matrices RACI. Entre las partes interesadas externas se incluyen a los clientes, socios comerciales, accionistas y reguladores. Entre las internas se incluyen el Consejo, la dirección, empleados y voluntarios.

- **Metas**: Las metas de los procesos se definen como 'declaraciones que describen el resultado deseado de un proceso. Un resultado puede ser un dispositivo, un cambio significativo en el estado de otros procesos o una mejora significativa en las capacidades de otros procesos'. Forman parte de la cascada de metas, es decir, las metas de los procesos apoyan a las metas relacionadas con las TI los cuáles, a su vez, apoyan a las metas empresariales.

Las metas de los procesos se pueden categorizar como:

- **Metas intrínsecas**— ¿El proceso dispone de calidad intrínseca? ¿Es preciso y está alineado con las buenas prácticas? ¿Cumple con las reglas externas e internas?
- **Metas contextuales**— ¿El proceso se particulariza y se adapta a la situación específica de la empresa? ¿Es relevante, comprensible y fácil de aplicar?
- **Seguridad y Acceso**—El proceso se mantiene confidencial y, cuando se requiere, está a disposición de quién tiene la necesidad.

En cada uno de los niveles de la cascada de metas, y por lo tanto también para los procesos, se definen métricas que miden el grado de consecución de los mismos. Las métricas se pueden definir como 'una entidad cuantificable que permite medir la consecución de las metas de un proceso. Las métricas deberían ser – específicas, medibles, practicables (permitan tomar decisiones), relevantes y oportunas– (SMART)'.

Para gestionar un catalizador de forma efectiva y eficiente, se necesitan definir métricas que midan el grado en el que se logran los resultados esperados. Adicionalmente, un segundo aspecto en la gestión del rendimiento del catalizador nos proporciona el grado en el que se aplican las buenas prácticas. También se pueden definir métricas asociadas que ayuden a gestionar el catalizador.

- **Ciclo de vida**: Cada proceso tiene un ciclo de vida. Éste se define, crea, opera, supervisa y se adapta/actualiza o retira.

Las prácticas generales sobre procesos, como las que se definen en el modelo de evaluación de procesos de COBIT basadas en ISO/IEC 15504, pueden ayudar en la definición, ejecución, supervisión y optimización de los procesos.

- **Buenas prácticas**: *COBIT 5: Procesos Catalizadores* contiene un modelo de referencia para los procesos, en el que se describen buenas prácticas internas sobre procesos en niveles de detalle crecientes: prácticas, actividades y actividades detalladas:14

Prácticas:

Para cada proceso de COBIT 5, las prácticas de gobierno/gestión proporcionan un conjunto completo de los requerimientos de alto nivel para una gestión y un gobierno práctico y efectivo, de la TI de la empresa. Y son:

- Declaraciones sobre acciones que proporcionan beneficios, optimizan el nivel de riesgo y el uso de los recursos
- Alineadas con los estándares y buenas prácticas más relevantes y comúnmente aceptadas
- Genéricas y, por tanto, necesitan adaptarse a cada empresa.
- En los procesos se contemplan los roles de las figuras de TI y de negocio (de principio a fin).

El cuerpo de gestión y gobierno de la empresa necesita tomar decisiones relativas a las prácticas de gobierno y gestión:

- Seleccionando aquéllas que sean aplicables y, de entre éstas, decidiendo cuáles se implementarán
- Añadiendo y/o adaptando prácticas, cuando sea necesario
- Definiendo y añadiendo prácticas no relacionadas con las TI, para la integración en los procesos de negocio
- Eligiendo cómo implementarlas (frecuencia, ámbito, automatización, etc.)
- Aceptando el riesgo por no implementar aquéllas que podrían ser aplicables

Actividades:

En COBIT 5, las acciones principales para operar los procesos se definen como las 'directrices para lograr las prácticas de gestión que permitan un gobierno y una gestión satisfactorios de las TI de una empresa'. Las actividades de COBIT 5 proporcionan el cómo, el porqué y el qué implementar en cada una de las prácticas de gestión y gobierno para mejorar el rendimiento y/o identificar una solución TI y el riesgo en la prestación de los servicios.

Este material es de uso por parte de:

- Equipo de dirección, proveedores de servicio, usuarios finales y profesionales de las TI que necesiten planificar, construir, ejecutar o supervisar las TI de una empresa.
- Profesionales de aseguramiento que deban dar su opinión respecto a las implementaciones existentes, a las propuestas, o respecto a mejoras necesarias.

Actividades detalladas:

Las actividades podrían no tener un nivel de detalle suficiente para su implementación.

Podrían necesitarse directrices adicionales para ser:

- Obtenidas de los estándares y buenas prácticas más relevantes tales como ITIL, la serie ISO/IEC 27000 y PRINCE2
- Desarrolladas como actividades más detalladas o específicas como desarrollos adicionales en la familia de productos COBIT 5

Entradas y salidas:

Las entradas y salidas de COBIT 5 son los productos de trabajo/elementos del proceso, considerados necesarios para sostener la operación del mismo. Permiten adoptar decisiones clave, proporcionan registros y evidencias de auditoría sobre las actividades de dichos procesos y permiten la investigación en caso de incidente. Las entradas y salidas se definen en el nivel clave de la práctica del gobierno/gestión, podrían incluir determinados productos de trabajo usados únicamente dentro del proceso y suelen ser entradas esenciales para otros procesos.

"Pueden existir buenas prácticas externas de cualquier otro tipo o nivel de detalle, la mayoría de ellas harán referencia a otros estándares y marcos de referencia. Los usuarios pueden consultar en todo momento las mencionadas buenas prácticas externas, sabiendo que COBIT 5 se alinea, cuando sea relevante, con dichos estándares en cuyo caso estará disponible la información de dichas referencias" (ISACA, 2012).

Gestión del Rendimiento de los Catalizadores.

Las empresas esperan resultados positivos de la aplicación y uso de los catalizadores. En la gestión del rendimiento de los catalizadores, tienen que formularse las siguientes preguntas y ser respondidas regularmente – basándose en métricas:

- ¿Se atienden las necesidades de las partes interesadas?
- ¿Se alcanzan las metas del catalizador?
- ¿Se gestiona el ciclo de vida del catalizador?
- ¿Se aplican buenas prácticas?

En el caso de un catalizador de proceso, las dos primeras preguntas tienen que ver con el resultado actual del catalizador, y a las métricas utilizadas para medir en qué medida se alcanzan las metas se les pueden denominar 'indicadores de retraso'.

En COBIT 5: *Procesos Catalizadores* se define una relación de métricas para cada meta del proceso.

Las dos últimas tratan del funcionamiento actual del catalizador en sí mismo, y las métricas relacionadas se pueden denominar 'indicadores de avance'.

Nivel de capacidad del proceso:

COBIT 5 incluye un esquema de evaluación de las capacidades de los procesos basado en ISO/IEC 15504. Esto se trata en el capítulo 8 de COBIT 5 y hay directrices adicionales disponibles en publicaciones separadas del COBIT 5 de ISACA. En resumen, el nivel de capacidad del proceso mide el cumplimiento de metas y la aplicación de buenas prácticas.

Relaciones con otros catalizadores:

Los enlaces entre los procesos y las demás categorías de catalizadores existen a través de las siguientes relaciones:

- Los procesos necesitan información (como un tipo de entrada) y pueden producir información (como producto de trabajo).
- Los procesos necesitan estructuras organizativas y roles para operar, tal y como se muestra en las matrices RACI, p. ej., comité de dirección TI, comité de riesgos de la empresa, el Consejo, auditoría, Director de Informática/Sistemas (CIO), Director General Ejecutivo (CEO).
- Los procesos proporcionan, y también requieren, capacidades de servicio (infraestructuras, aplicaciones, etc.).
- Los procesos pueden, y deberán, depender de otros procesos.
- Los procesos proporcionan, o necesitan, políticas y procedimientos para asegurar una implementación y ejecución consistentes.
- Aspectos culturales y relativos al comportamiento determinan lo bien que se ejecutan los procesos. *Ejemplo de un Catalizador Proceso en la Práctica.*

El ejemplo siguiente ilustra un catalizador proceso, sus interconexiones y dimensiones.

Modelo de Referencia de Procesos de COBIT 5

Procesos de Gestión y Gobierno

Uno de los principios directrices en COBIT 5 es la distinción que se realiza entre la gestión y el gobierno. En línea con este principio, se espera que la empresa implemente una serie de procesos de gobierno y otros de gestión para proporcionar un gobierno y una gestión integral de las TI empresariales.

Teniendo en cuenta los procesos para el gobierno y la gestión, en el contexto empresarial, la diferencia entre los dos tipos de procesos reside en los objetivos de los mismos:

- **Procesos de Gobierno**

Los procesos de gobierno se ocupan de los objetivos de gobierno de las partes interesadas, proporcionan valor, optimizar riesgos y recursos – e incluyen prácticas y actividades enfocadas a evaluar opciones estratégicas, proporcionando dirección a la TI y supervisando sus resultados (Evaluación, Dirección y Supervisión (EDM) – en línea con los conceptos del estándar ISO/IEC 38500).

- **Procesos de Gestión**

Alineado con la definición de gestión, las prácticas y actividades de los procesos de gestión abarcan las áreas de responsabilidad de Planificación, Construcción, Ejecución y Supervisión (PBRM) de las TI de la empresa, debiendo dar cobertura, de principio a fin, a toda ella.

INTERCONEXIONES DEL CATALIZADOR PROCESO

Una organización tiene asignados 'gestores de procesos' a procesos de TI. Estos gestores se encargan de definir y operar, de manera efectiva y eficiente, los procesos TI en un contexto de buen gobierno y buena gestión de la TI en la empresa.

Inicialmente, los gestores de procesos se focalizarán en el catalizador proceso, considerando las dimensiones del mismo:

- **Partes interesadas:** Las partes interesadas de los procesos incluyen a todos sus actores, es decir, todos los participantes que son responsables de hacer o de que se haga, consultados o informados (RACI) por o durante, las actividades del proceso. A este respecto, se puede utilizar la matriz RACI tal y como se describe en *COBIT 5: Procesos Catalizadores*
- **Metas:** Para cada proceso, se necesitan definir unas metas y métricas asociadas, que sean adecuadas. Por ejemplo, en el proceso *AP008 Gestionar las Relaciones (en COBIT 5: Procesos Catalizadores)* uno puede encontrar un conjunto de metas y métricas, como las siguientes:
  - **Meta:** Las estrategias de negocio, los planes y requerimientos se comprenden y están documentados y aprobados.
    - **Métrica:** Porcentaje de programas alineados con las prioridades y requerimientos de negocio de la empresa.
  - **Meta:** Existencia de buenas relaciones entre la empresa y los departamentos de TI.
    - **Métrica:** Resultados de las encuestas de satisfacción de usuarios y personal de TI.
- **Ciclo de vida:** Cada proceso tiene un ciclo de vida, es decir, se ha de crear, ejecutar, supervisar y adaptar cuando sea necesario. En último término, los procesos dejan de existir. En este caso, los gestores de los procesos necesitarían primero definir y diseñar los procesos. Para diseñar los procesos pueden utilizar los diferentes elementos de *COBIT 5: Procesos Catalizadores*, p. ej., para definir responsabilidades y desglosar el proceso en prácticas y actividades y para definir sus productos de trabajo (entradas y salidas). En un paso posterior, el proceso necesitará hacerse más robusto y eficiente, a este propósito, los gestores de los procesos pueden utilizar el nivel de capacidad de los procesos. Se pueden utilizar atributos de capacidad de los procesos del Modelo de Capacidades de los Procesos de COBIT 5 inspirado en la norma ISO/IEC 15504, de manera que:
  - El nivel 2 de capacidad de un proceso requiere la consecución de dos atributos: La Gestión del Rendimiento y la Gestión de los Productos de Trabajo. El primer atributo requiere de varias actividades relativas a la fase de planificación:
    - Los objetivos de rendimiento del proceso están definidos.
    - El rendimiento del proceso está planificado.
    - Las responsabilidades para la ejecución del proceso están definidas.
    - Los recursos están definidos.
    - Etc.

    El mismo nivel de capacidad prescribe varias actividades para la fase de 'supervisión' del ciclo de vida del proceso:
    - El rendimiento del proceso es supervisado.
    - El rendimiento del proceso se ajusta a lo planificado.
    - Etc.
  - La misma aproximación se puede utilizar para obtener directrices en las distintas fases del ciclo de vida, desde los distintos atributos de rendimiento de las capacidades hasta niveles crecientes de capacidad de los procesos.
- **Buenas Prácticas:** Tal y como se indica en el punto anterior, COBIT 5 en *COBIT 5: Procesos Catalizadores*, se describen con gran detalle buenas prácticas para los procesos. Allí se puede encontrar inspiración y ejemplos de procesos, cubriéndose un amplio espectro de actividades para al buen gobierno y buena gestión de la TI de la empresa.

Además de las directrices del catalizador de tipo proceso, los gestores del proceso pueden decidir referirse a otro tipo de catalizadores tales como:

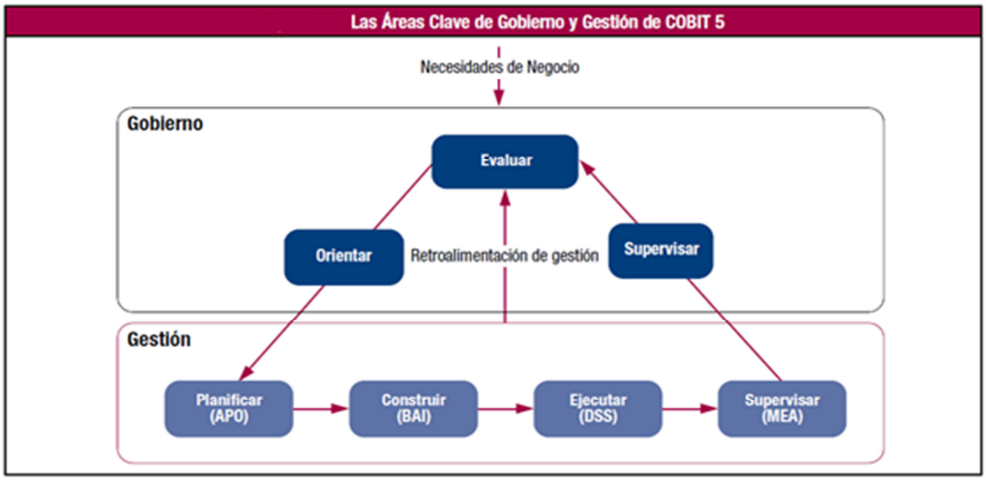
- Las matrices RACI que describen roles y responsabilidades. Otros catalizadores permiten examinar a fondo esta dimensión de manera que:
  - En los catalizadores de habilidades y competencias, se pueden definir las metas requeridas para cada rol (p. ej., niveles de habilidades técnicas y de comportamiento) y sus métricas asociadas.
  - Las matrices RACI también contienen varias estructuras organizativas. Éstas se pueden desarrollar más en el catalizador de estructuras organizativas, donde se puede proporcionar una descripción más detallada de la estructura, se pueden definir los resultados esperados y las métricas asociadas (p. ej., las decisiones), y se pueden definir buenas prácticas (p. ej., ámbito de control, principios operativos de la estructura y niveles de autoridad).
- Los principios y las políticas formalizarán los procesos y prescribirán el por qué de su existencia, sobre quiénes aplican y cómo se utilizará el proceso. Esta es el área de foco del catalizador de principios y políticas.

Aunque los resultados de los dos tipos de procesos son diferentes y están dirigidos a audiencias diferentes, internamente, desde el propio contexto del proceso, todos ellos requieren una 'planificación', 'construcción e implementación', 'ejecución' y 'supervisión' de las actividades del mismo.

Modelo de Referencia de Procesos de COBIT 5

COBIT 5 no es prescriptivo, aunque a lo largo de esta obra queda patente que incita a las empresas a implementar procesos de gobierno y de gestión de manera que las áreas más importantes queden cubiertas, tal y como se muestra en la siguiente figura.

Teóricamente una empresa puede organizar sus procesos como mejor considere que éstos se adaptan, siempre que se cubran los objetivos básicos relativos a su gobierno y gestión. Las empresas pequeñas podrían tener un número menor de procesos, mientras que las empresas más grandes y complejas podrían tener bastantes procesos, todos ellos para cubrir los mismos objetivos.



A pesar de lo indicado anteriormente, COBIT 5 incluye un modelo de referencia de procesos en el que se definen y describen, con detalle, una relación de procesos de gestión y gobierno.

Proporciona un modelo de referencia de procesos que representan todos los procesos que normalmente se pueden encontrar en la empresa relacionados con actividades de TI, ofreciendo un modelo de referencia comprensible a los directores de negocio y de operaciones de TI. El modelo de procesos propuesto es un modelo completo de referencia, aunque no el único posible. Cada empresa debe definir su propio conjunto de procesos, considerando su situación específica.

La incorporación de un modelo de referencia y un lenguaje común para todas las partes involucradas en actividades de TI en la empresa, es uno de los pasos más críticos e importantes hacia el buen gobierno. Proporciona un marco de trabajo para la medida y supervisión del rendimiento de las TI, estableciendo una comunicación con los proveedores de servicio e integrándose con las buenas prácticas de gestión.

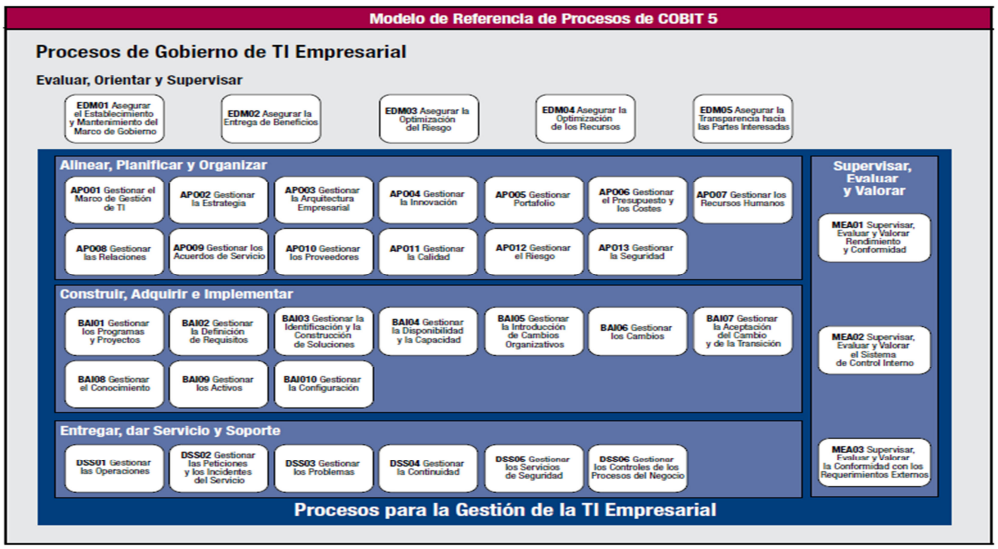
El modelo de referencia de COBIT 5 divide a los procesos de gobierno y gestión de una empresa de TI en dos áreas principales de actividad – gobierno y gestión – divididas en dominios de procesos:

- **Gobierno**—Este dominio contiene cinco procesos de gobierno; en cada uno de ellos se definen prácticas de Evaluación, Dirección y Supervisión (EDM).
- **Gestión**—Estos cuatro dominios están alineados con las áreas de responsabilidad de Planificación, Construcción, Ejecución y Supervisión (PBRM) (evolución de los dominios de COBIT 4.1), proporcionando cobertura, de principio a fin, a toda la TI. Cada dominio contiene una relación de procesos, al igual que en COBIT 4.1 y versiones anteriores.

Aunque, tal y como se ha descrito previamente, la mayoría de los procesos requieren actividades de 'planificación', 'implementación', 'ejecución' y 'supervisión' dentro del proceso o dentro del asunto particular que se esté tratando (p. ej., calidad, seguridad), se disponen en dominios alineados con lo que, generalmente, representan las áreas de actividad más relevantes relativas a TI a nivel empresarial.

En COBIT 5, los procesos también contemplan el alcance completo de las actividades de negocio y de TI relativas al gobierno y gestión de la TI de la empresa, de manera que el modelo de procesos sea realmente extensible a toda ella.

El modelo de referencia de COBIT 5 es el sucesor del de COBIT 4.1, integrando también los modelos de proceso de Risk TI y Val TI. La siguiente figura se muestra el conjunto completo de los 37 procesos de gestión y gobierno de COBIT 5. Los detalles de todos los procesos, de acuerdo al modelo de referencia descrito anteriormente, están incluidos en *COBIT 5: Procesos Catalizadores.*



3.3. Habilitador 3 – Estructuras Organizacionales

Las especificaciones para el catalizador de estructuras organizativas comparadas con la descripción de un catalizador genérico se muestran en la figura siguiente.

El modelo de estructuras organizativas muestra:

- **Partes Interesadas**:

Las partes interesadas en las estructuras organizativas pueden ser internas y externas a la empresa e incluyen a: los miembros individuales de la estructura, otras estructuras, entidades organizativas, clientes, proveedores y reguladores. Sus roles varían e incluyen la toma de decisiones, influenciar y asesorar. Las participaciones de cada una de las partes interesadas también varían, es decir, ¿qué interés tienen en las decisiones tomadas por la estructura?

- **Metas**

Las metas para el catalizador de las estructuras organizativas, deberían incluir en sí mismo un mandato adecuado, principios operativos bien definidos y la aplicación de otras buenas prácticas. El resultado del catalizador de las estructuras organizativas debería incluir varias buenas actividades y decisiones.

- **Ciclo de vida**

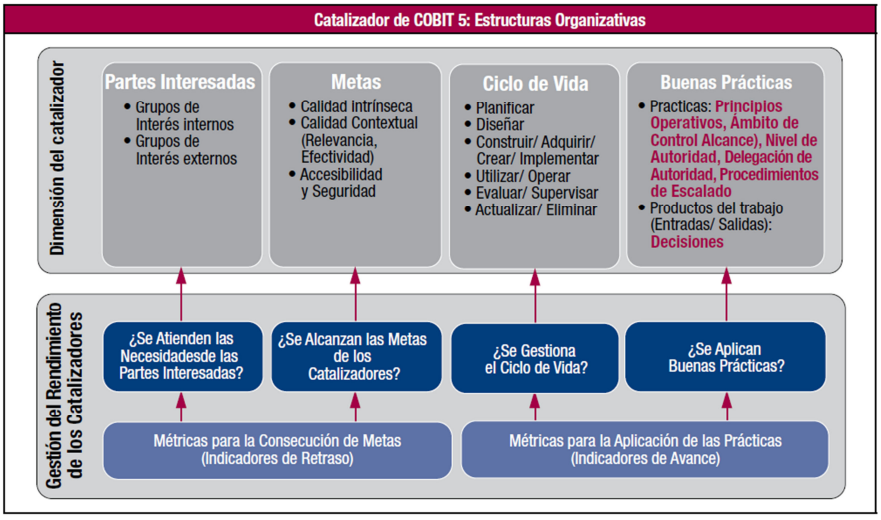
Una estructura organizativa tiene un ciclo de vida. Es creada, existe y es ajustada y, finalmente, puede ser disuelta. Durante su creación, se debe definir un mandato –una razón y un propósito para su existencia.

- **Buenas prácticas**

Se pueden distinguir varias buenas prácticas para las estructuras organizativas como:

  - Principios operativos — Las modalidades prácticas respecto a cómo la estructura operará, como frecuencia de reuniones, documentación y reglas de mantenimiento.
  - Composición — Las estructuras tienen miembros, los cuales son partes interesadas internas o externas.

- Ámbito de control — Los límites de los derechos de decisión de la estructura organizativa.
- Niveles de autorización/derechos de decisión — Las decisiones que la estructura está autorizada a tomar.
- Delegación de autoridad — La estructura puede delegar (un subconjunto de) sus derechos de decisión a otras estructuras dependientes que le reportan.
- Procedimiento de escalado — La ruta de escalado para una estructura organizativa describe las acciones requeridas en caso de problemas en la toma de decisiones.



Relaciones con otros catalizadores—Los vínculos con otros catalizadores incluyen:

- Las matrices RACI vinculan actividades de procesos con estructuras organizaciones y/o roles individuales en la empresa. Estas tablas describen el nivel de involucramiento de cada rol para cada práctica del proceso: (R) Responsable de hacer, (A) Responsable de que se haga, (C) Consultado e (I) Informado.
- La cultura, la ética y el comportamiento determinan la eficiencia y efectividad de las estructuras organizativas y de sus decisiones.
- La composición de las estructuras organizativas deberían tener en cuenta y requerir el conjunto apropiado de competencias de sus miembros.
- El mandato y los principios operativos de las estructuras organizativas son guiados por el marco de políticas implementado.
- Entradas y salidas – Una estructura requiere entradas (normalmente información) antes de que pueda tomar decisiones informadas y, asimismo, produce salidas, p. ej.: decisiones, otra información o solicitudes de entradas adicionales.

Estructuras Organizativas Ilustrativas en COBIT 5

Como se ha mencionado en la discusión del modelo de procesos de COBIT 5, se ha creado y descrito un modelo referencial de procesos ilustrativo de COBIT 5 en *COBIT 5: Procesos Catalizadores*. El modelo incluye matrices RACI, las cuales usan varios roles y estructuras. La figura que sigue describe estos roles y estructuras predefinidos.

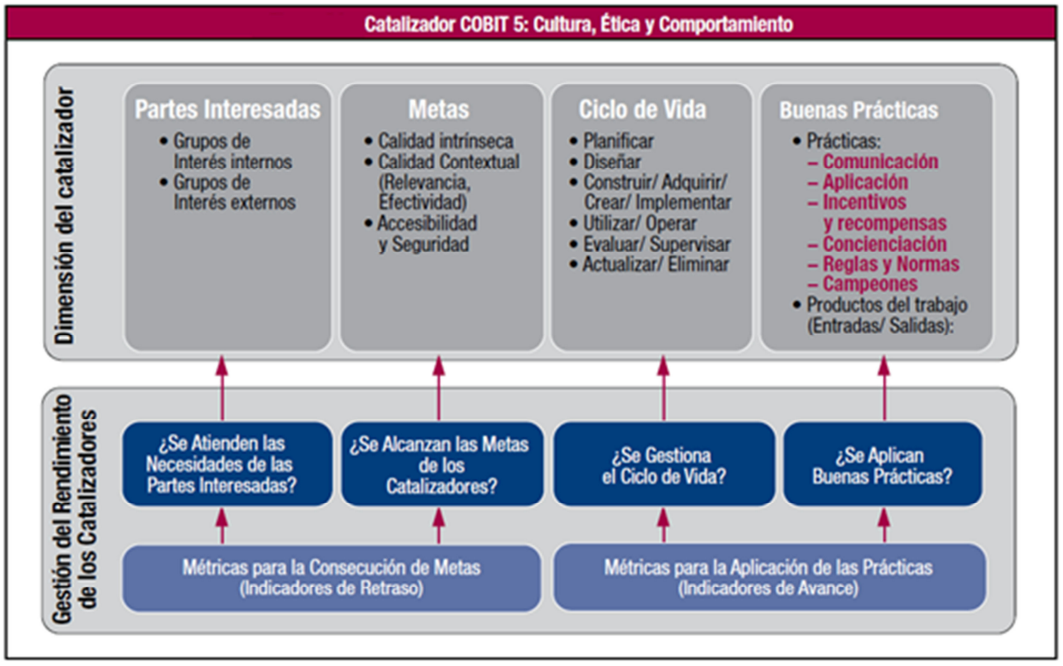
Notas:

- No se tienen que corresponder necesariamente con las funciones actuales que las empresas tienen implementadas, pero sin embargo proporcionan valor en el sentido de que el propósito de la estructura o de los roles son iguales para la mayoría de las empresas.
- El propósito de esta tabla no es prescribir un organigrama organizativo universal para cada empresa. Más bien, debería ser considerado como algo ilustrativo.

Roles y Estructuras Organizativas de COBIT 5	
Rol/Estructura	**Definición/Descripción**
Consejo de Administración	El grupo de los ejecutivos de mayor cargo y/o directores no ejecutivos de la empresa que son responsables del gobierno de la empresa, teniendo el control total de sus recursos
Director General Ejecutivo (CEO)	El ejecutivo de más alto rango a cargo de la gerencia total de la empresa
Director General Financiero (CFO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión financiera, incluyendo el riesgo financiero y cuentas confiables y precisas
Director General Operativo (COO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la operación de la empresa
Director General de Riesgos (CRO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión de riesgos en toda la empresa. Se puede establecer un directivo de riesgos de TI para supervisar los riesgos relacionados con TI
Director de Informática/Sistemas (CIO)	El ejecutivo de mayor cargo responsable de alinear TI con las estrategias del negocio y que también es responsable de que se planifique, se consigan los recursos necesarios y se gestione la entrega de servicios y soluciones de TI para soportar los objetivos de la empresa
Director de Seguridad de la Información (CISO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la seguridad de la información de la empresa, en todas sus formas
Ejecutivo de Negocio	Un individuo de la gerencia responsable de la operación de una unidad de negocio específica o de una subsidiaria
Propietario del Proceso de Negocio	Un individuo responsable del rendimiento de un proceso en la realización de sus objetivos, realizando mejoras y aprobando cambios al proceso
Comité de Estrategia de TI	Un grupo de ejecutivos de alto cargo designado por el Consejo para asegurar que el Consejo está involucrado y se mantiene informado de las cuestiones y decisiones más relevantes de TI. El comité es responsable de que se haga la gestión de la cartera de inversiones facilitadas por TI, los servicios de TI y los activos de TI, asegurando que el valor es entregado y el riesgo gestionado. El comité es normalmente presidido por un miembro del Consejo y no por el CIO
Comité de Supervisión (Proyectos y Programas)	Un grupo de partes interesadas y expertos quienes son responsables de la dirección de programas y proyectos, incluyendo la gerencia y la supervisión de planes, asignación de recursos, entrega de beneficios y valor y la gestión de los riesgos de programas y proyectos
Consejo de Arquitectura	Un grupo de partes interesadas y expertos quienes son responsables de la dirección de las cuestiones y decisiones relacionadas con la arquitectura de empresa y de establecer las políticas y los estándares para dicha arquitectura
Comité de Riesgo Empresarial	El grupo de ejecutivos de la empresa quienes son responsables del consenso y la colaboración requerida a nivel empresa para soportar las actividades y decisiones de la gestión de riesgo empresarial (ERM). Se puede establecer un consejo de riesgos de TI para considerar los riesgos de TI con mayor detalle y asesorar al comité de riesgos de la empresa
Jefe de Recursos Humanos	El ejecutivo de mayor cargo responsable de todos los aspectos de planificación y políticas relacionadas con todos los recursos humanos de la empresa
Cumplimiento	La función en la empresa responsable de dirigir el cumplimiento legal, regulatorio y contractual
Auditoría	La función en la empresa responsable de proveer auditorías internas
Jefe de Arquitectura	Un miembro de la gerencia responsable del proceso de arquitectura de la empresa
Jefe de Desarrollo	Un miembro de la gerencia responsable del proceso de desarrollo de soluciones relacionadas con TI
Jefe de Operaciones de TI	Un miembro de la gerencia responsable de los entornos y la infraestructura para las operaciones de TI
Jefe de Administración de TI	Un miembro de la gerencia responsable de los registros relacionados con TI y responsable de soportar las cuestiones administrativas de TI.
Oficina de Gestión de Programas y Proyectos (PMO)	La función responsable de apoyar a los gerentes de programas y proyectos, recopilando, evaluando y notificando información sobre la conducción de sus programas y proyectos que los constituyen
Oficina de Gestión de Valor (VMO)	La función que actúa como secretaría para la gestión de las inversiones y portafolios de servicios, incluyendo la evaluación y asesoramiento sobre oportunidades de inversión y casos de negocio, recomendando métodos y controles de gobierno/gestión del valor y reportando el progreso de creación y sustento del valor generado a partir de las inversiones y servicios
Gerente de Servicios	Un individuo que gestiona el desarrollo, implementación, evaluación y gestión continua de nuevos y existentes productos y servicios para un cliente (usuario) específico o grupo de clientes (usuarios)
Gerente de Seguridad de la Información	Un individuo que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de la empresa
Gerente de Continuidad d el Negocio	Un individuo que gestiona, diseña, supervisa y/o evalúa las capacidades de la continuidad de negocio de la empresa, para garantizar que las funciones críticas de la empresa continúan operando ante eventos disruptivos.
Oficial de Privacidad	Un individuo que es responsable de la supervisión de los riesgos e impactos para el negocio de las leyes de privacidad y de la dirección y coordinación de la implementación de políticas y actividades que garanticen que se alcanzan las directivas de privacidad. También es denominado Director de Protección de Datos.

3.4. Habilitador 4 – Cultura, Ética y Comportamiento

Cultura, ética y comportamiento se refiere al conjunto de conductas individuales y colectivas dentro de una empresa. Las especificaciones para el catalizador de cultura, ética y comportamiento, comparadas con la descripción del catalizador genérico se muestran en la siguiente figura.



El modelo de cultura, ética y comportamiento muestra:

- **Partes interesadas**—Las partes interesadas en cultura, ética y comportamiento pueden ser internas y externas respecto a la empresa. Las partes interesadas internas incluyen a la empresa entera, mientras que las partes interesadas externas incluyen a reguladores, p. ej. auditores externos o entidades de supervisión. Las participaciones son de dos tipos: algunas partes interesadas, p. ej. representantes legales, gerentes de riesgos, gerentes de recursos humanos, consejos de salarios y directivos, tratan con la definición, implementación y refuerzo de comportamientos deseados, y otros tienen que alinearse con las reglas y normas definidas.

- **Metas**—Las metas para el catalizador de cultura, ética y comportamiento, se relacionan con:

  - Ética organizativa, determinada por los valores por los cuales la empresa quiere subsistir.
  - Éticas individuales, determinada por los valores personales de cada individuo dentro de la empresa y dependiendo de un importante grado de factores externos tales como religión, origen étnico, antecedentes socioeconómicos, geografía y experiencias personales
  - Comportamientos individuales, que determinan colectivamente la cultura de una empresa. Muchos factores, tales como los externos mencionados anteriormente,

pero también las relaciones interpersonales dentro de la empresa, objetivos personales y ambiciones, rigen los comportamientos. Algunos comportamientos que pueden ser relevantes en este contexto incluyen:

- Comportamiento hacia la toma de riesgos – ¿Cuánto riesgo siente la empresa que puede absorber y cuánto riesgo está dispuesta a aceptar?
- Comportamiento hacia el cumplimiento de políticas - ¿Hasta qué punto la gente acepta y/o cumple con las políticas?
- Comportamiento hacia los resultados negativos - ¿Cómo trata la empresa con los resultados negativos, es decir, eventos de pérdida u oportunidades perdidas? ¿Aprende de ellos e intenta corregir o serán asignadas culpas sin el tratamiento de la causa raíz?

- **Ciclo de vida**—Una cultura organizativa, una postura ética y los comportamientos individuales, etc., todos tienen sus ciclos de vida. Comenzando desde una cultura existente, una empresa puede identificar cambios necesarios y trabajar orientada hacia su implementación. Se pueden utilizar para ello varias herramientas –descritas en las buenas prácticas.

- **Buenas prácticas**—Las buenas prácticas para crear, fomentar y mantener los comportamientos deseados a lo largo de toda empresa incluyen:

  - Comunicación a lo largo de toda la empresa de los comportamientos deseados y los valores corporativos subyacentes.
  - Concienciación de los comportamientos deseados, fortalecidos por la conducta ejemplar ejercitada por los gerentes de mayor cargo y otros líderes.
  - Incentivos para fomentar y elementos disuasivos para hacer cumplir los comportamientos deseados. Existe un vínculo claro entre el comportamiento individual y el esquema de recompensas de recursos humanos que la empresa haya implementado.
  - Reglas y normas, las cuales proveen mayor guía sobre el comportamiento organizativo deseado. Esto se vincula en forma muy clara con los principios y políticas que la empresa haya implementado.

- **Relaciones con otros catalizadores**—Los vínculos con otros catalizadores incluyen:

  - Los procesos pueden ser diseñados de manera perfecta, pero si las partes interesadas de un proceso no desean ejecutar las actividades del proceso como se

pretende – es decir, si su comportamiento es de no cumplimiento— no se alcanzarán los resultados de desempeño del proceso.

- Igualmente, las estructuras organizativas pueden ser diseñadas y construidas de acuerdo con los manuales, pero si sus decisiones no son implementadas —por razones de diferentes agendas personales, falta de incentivos, etc. dichas estructuras no resultarán en un gobierno y gestión decentes para la TI de la empresa.
- Los principios y las políticas son mecanismos de comunicación muy importantes de los valores corporativos y el comportamiento deseado.

MEJORA DE LA CALIDAD

Una empresa se enfrenta de forma repetida a serios problemas de calidad con las nuevas aplicaciones. A pesar del hecho de que está implementada una metodología de proyectos de desarrollo de software, demasiado a menudo los errores de software causan problemas operativos en el día a día del negocio.

Una investigación muestra que la dirección y los miembros del equipo de desarrollo son evaluados y recompensados basándose en la entrega de sus proyectos en plazo y dentro del presupuesto. No se les mide por criterios de calidad o criterios de beneficios para el negocio. En consecuencia, se focalizan diligentemente en los tiempos de entrega y en la reducción de costes durante el desarrollo, p. ej. en tiempos de pruebas. La investigación también muestra que es virtualmente inexistente el cumplimiento con la metodología establecida y los procedimientos, porque esto llevaría tiempo adicional del presupuesto de desarrollo (a favor de la calidad). Además, la estructura de la organización es tal que la participación oficial de desarrollo finalizar cuando el desarrollo se ha entregado al equipo de operaciones. A partir de entonces, la participación de desarrollo es sólo indirecta, a través de la gestión de incidencias establecida y los procesos de administración de problemas.

La lección aprendida es que deben utilizarse mejores incentivos para la solución de la gestión de equipos de desarrollo para fomentar el trabajo de calidad.

RIESGOS RELACIONADOS CON TI

Algunos síntomas de una cultura inadecuada o problemática con respecto a los riesgos relacionados con TI, incluyen:

- Falta de alineamiento estratégico entre el umbral real de riesgo y su traducción en políticas. Los valores reales de la gestión hacia el riesgo pueden ser razonablemente agresivos y de toma de riesgos, mientras que las políticas que se crean reflejan una actitud mucho más conservadora. De ahí, existe una falta de correspondencia entre valores y los medios para realizar los valores, llevando inevitablemente a conflictos. Los conflictos pueden surgir, por ejemplo, entre los incentivos establecidos para la gestión y la aplicación de políticas no alineadas.
- La existencia de una "cultura de la culpa". Este tipo de cultura debería ser evitada por todos los medios; es el inhibidor más efectivo de una comunicación relevante y eficiente. En una cultura de la culpa, las unidades de negocio tienden a apuntar con el dedo a TI cuando los proyectos no son entregados en fecha o no alcanzan las expectativas. Haciendo esto, ellos fracasan en darse cuenta como la involucración de las unidades de negocio afecta el éxito del proyecto. En casos extremos, las unidades de negocio pueden asignar culpas por no alcanzarse unas expectativas que dicha unidad nunca comunicó claramente. El "juego de la culpa" sólo perjudica la comunicación efectiva entre todas las unidades, generando retrasos adicionales. El liderazgo ejecutivo debe identificar y rápidamente controlar una cultura de la culpa si la colaboración ha de ser fomentada en toda la empresa.

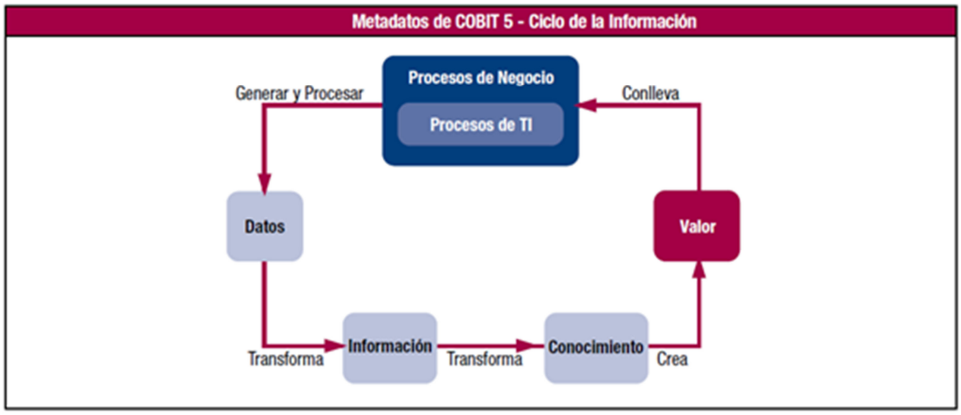
3.5. Habilitador 5 – Información

El catalizador información considera toda la información relevante para la empresa, no sólo la información automatizada.

La información puede ser estructurada o desestructurada, formalizada o informal.

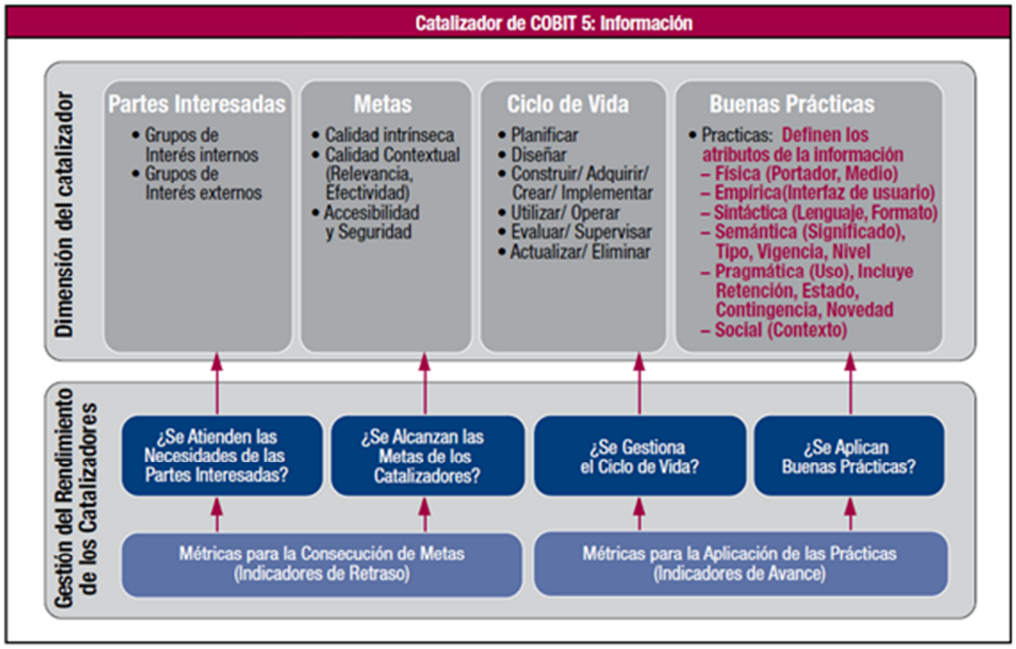
La información puede ser considerada como una etapa dentro del "ciclo de la información" de una empresa. Dentro del ciclo de la información (figura a continuación), los procesos de negocio generan y procesan datos, transformándolos en información y conocimiento, y en última instancia generando valor para la empresa. El alcance del catalizador información se refiere principalmente a

la fase de “información” dentro del ciclo de la información, pero también se cubren los aspectos de datos y conocimientos en COBIT 5.



Catalizador Información de COBIT 5

Las especificaciones para el catalizador información, comparadas con la descripción del catalizador genérico, se muestran en la figura a continuación.



El modelo de la información (Information Model, IM) muestra:

- **Partes interesadas**—Pueden ser internas o externas a la empresa. El modelo genérico también sugiere que, más allá de identificar a las partes interesadas, sus intereses deben ser identificados, p. ej. por qué se preocupan o están interesados en la información.

Con respecto a qué partes interesadas en la información existen, los roles que tratan con ella se pueden agrupar en diferentes categorías, que van desde propuestas detalladas –sugiriendo roles específicos sobre datos o información como arquitecto, propietario, apoderado, administrador, proveedor, beneficiario, modelador, director de calidad, director de seguridad– hasta propuestas más generales –por ejemplo, distinguiendo entre productores de información, custodios de información y consumidores de información:

- Productor de información, responsable de la creación de la información.
- Custodio de información, responsable de almacenar y mantener la información.
- Consumidor de información, responsable de utilizar la información.

Esas categorías se refieren a actividades específicas en relación al recurso de información. Las actividades dependen de la fase del ciclo de vida de la información; por lo tanto, para encontrar una categoría de roles que tenga un apropiado nivel de granularidad para el modelo de la información (IM), se puede usar la dimensión del ciclo de vida del modelo de la información (IM). Esto significa que los roles de las partes interesadas en la información pueden ser definidos en términos de las fases del ciclo de vida de la información, p. ej., planificadores de la información, adquirentes de la información, usuarios de la información. A la vez, esto significa que la dimensión de partes interesadas de la información no es una dimensión independiente; diferentes fases del ciclo de vida tienen diferentes partes interesadas.

Mientras que los roles relevantes dependen de la fase del ciclo de vida de la información, los intereses se pueden relacionar con las metas de la información.

- **Metas**—Las metas para la información están divididas en tres sub-dimensiones de calidad:
- **Calidad intrínseca**—El grado en que los valores de los datos están en conformidad con los valores reales o verdaderos.

Esto incluye:

- Precisión: El grado en que la información es correcta y confiable
- Objetividad: El grado en que la información es objetiva, sin prejuicios e imparcial
- Credibilidad: El grado en que la información es considerada como verdadera y creíble
- Reputación: El grado en que la información está altamente considerada en términos de su origen o contenido

- **Calidad contextual y de representatividad**

El grado en que la información es aplicable a la tarea del usuario de la información y es presentada en una manera clara e inteligible, reconociendo que la calidad de la información depende del contexto de su uso. Esto incluye:

  - Relevancia: El grado en que la información es aplicable y útil para la tarea a realizar
  - Completitud: El grado en que la información no tiene carencias y es de la suficiente profundidad y amplitud para la tarea a realizar
  - Vigencia: El grado en que la información está lo suficientemente actualizada para la tarea a realizar
  - La cantidad apropiada de información: El grado en que el volumen de información es adecuado para la tarea a realizar
  - Representación concisa: El grado en que la información se representa de forma compacta
  - Representación consistente: El grado en que la información se presenta en el mismo formato
  - Interpretabilidad: El grado en que la información está expresada en los idiomas, símbolos y unidades apropiados, con definiciones claras
  - Comprensibilidad: El grado en que la información sea fácil de comprender
  - Facilidad de manipulación: El grado en que la información es fácil de manipular y de aplicar a diferentes tareas

- **Accesibilidad y seguridad:** El grado en que la información está disponible o que puede obtenerse. Esto incluye:

  - Disponibilidad/ oportunidad: El grado en que la información está disponible cuando se requiera, o que es rápida y fácilmente recuperable
  - Acceso restringido: El grado en que el acceso a la información se restringe adecuadamente a las partes autorizadas

- **Ciclo de vida**: Se tiene que considerar el ciclo de vida de la información completo y se pueden requerir diferentes acercamientos para la información en diferentes fases del ciclo de vida. El catalizador información de COBIT 5 distingue las siguientes fases:

- **Planificar**— La fase en la cual se prepara la creación y uso del recurso información. Las actividades en esta fase pueden referirse a la identificación de objetivos, la

planificación de la arquitectura de la información y el desarrollo de estándares y definiciones, p. ej., definiciones de datos, procedimientos de recolección de datos.

- **Diseñar**
- **Construir/adquirir**—La fase en la cual se adquiere el recurso información. Las actividades en esta fase pueden referirse a la creación de registros de datos, la compra de datos y la carga de archivos externos.
- **Usar/operar**, que incluye:
- Almacenar: La fase en la cual la información es retenida electrónicamente o en una copia impresa (o inclusive sólo en la memoria humana). Las actividades en esta fase pueden referirse al almacenamiento de información en formato electrónico (p. ej., archivos electrónicos, bases de datos, almacenes de datos) o en copias impresas (p.ej., documentos en papel).
- Compartir: La fase en la cual la información se pone a disposición para su uso a través de un método de distribución. Las actividades en esta fase pueden referirse a los procesos involucrados en trasladar la información a los lugares donde debe ser accedida y utilizada, p.ej., distribución de documentos por correo electrónico. Para la información retenida electrónicamente, esta fase del ciclo de vida puede solaparse en gran medida con la fase de almacenar, p.ej., compartir información a través de accesos a bases de datos, servidores de archivos/documentos.
- Usar: La fase en la cual la información es utilizada para conseguir las metas. Las actividades en esta fase pueden referirse a todos los tipos de uso de la información (p.ej., toma de decisión por la gerencia, ejecución de procesos automatizados), y puede también incluir actividades como recuperación de la información y conversión de información de una forma a otra.
- De acuerdo con la perspectiva de "Llevar el Gobierno Adelante" (Taking Governance Forward), la información es un catalizador para el gobierno de la empresa, por lo que el uso de la información tal como se define en el Modelo de la Información (IM) puede ser considerado como los propósitos para los cuales las partes interesadas en el gobierno de la empresa necesitan información cuando asumen sus roles, cumplen sus actividades e interactúan unos con otros.
- Las interacciones entre las partes interesadas requieren los flujos de información cuyos propósitos se indican en el esquema: la responsabilidad de que se haga, la delegación, la supervisión, el establecimiento de dirección, la alineación, ejecución y control.

- Supervisar: La fase en la cual se asegura que el recurso de información continúa funcionando correctamente, es decir, para ser valioso. Las actividades en esta fase

pueden referirse a mantener la información actualizada, así como otros tipos actividades de gestión de la información, por ejemplo, la mejora, la limpieza, la fusión, la eliminación de datos duplicados de la información en los almacenes de datos.

- Desechar: La fase en la cual se deshecha el recurso de información cuando ya no es de uso. Las actividades en esta fase pueden referirse al archivo o destrucción de la información.

- **Mejores prácticas**: El concepto de información es entendido de forma diferente en distintas disciplinas tales como economía, teoría de la comunicación, ciencias de la información, gestión del conocimiento y sistemas de información; por lo tanto, no hay una definición universalmente consensuada considerando lo qué es la información. La naturaleza de la información puede, sin embargo, ser clarificada a través de la definición y descripción de sus propiedades.

El siguiente esquema se propone para estructurar las diferentes propiedades de la información: este consiste en seis niveles o capas para definir y describir las propiedades de la información. Estos seis niveles presentan un continuo de atributos, que van desde el mundo físico de la información, donde los atributos están relacionados con las tecnologías de información y los medios para la captura de información, almacenamiento, procesamiento, distribución y presentación, hasta el mundo social del uso de la información, la comprensión y la acción.

Podemos usar las siguientes descripciones para las capas y atributos de la información:

- **Capa del mundo físico**—El mundo en el que tienen lugar todos los fenómenos que pueden ser observados empíricamente.
  - Transporte/soportes de información — El atributo que identifica el soporte físico de la información, p.ej., papel, señales eléctricas, ondas sonoras.
- **Capa empírica**—La observación empírica de los signos que se utilizan para codificar la información y su distinción de los demás y del ruido de fondo.
  - Canales de acceso a la información — El atributo que identifica el canal de acceso a la información, p.ej., las interfaces de usuario.
- **Capa sintáctica**—Reglas y principios para la construcción de frases en lenguaje natural o artificial. La sintaxis se refiere a la forma de información.
  - Código/ idioma — El atributo que identifica el idioma/formato de representación utilizado para codificar la información y las reglas para combinar los símbolos del lenguaje para formar las estructuras sintácticas.

- **Capa semántica**—Las reglas y principios para construir el significado de las estructuras sintácticas. La semántica se refiere al significado de la información.
  - Tipo de información — El atributo que identifica el tipo de información, p.ej., información financiera versus no financiera, información de origen interno versus externo, valores pronosticados/previstos versus observados, planificados versus valores realizados.
  - Vigencia de la Información — El atributo que identifica el horizonte temporal contemplado por la información, p.ej., la información sobre el pasado, el presente o el futuro.
  - Nivel de información — El atributo que identifica el grado de detalle de la información, p.ej., las ventas por año, trimestre, mes.
- **Capa pragmática**—Las reglas y estructuras para la construcción de grandes estructuras del lenguaje que cumplan con propósitos específicos en la comunicación humana. La capa pragmática se refiere a la utilización de la información.
  - Periodo de retención — El atributo que identifica cuánto tiempo la información puede ser retenida antes de que sea destruida.
  - Estado de la información — El atributo que identifica si la información es operativa o histórica.
  - Novedad
  - El atributo que identifica si se trata de información que crea nuevo conocimiento o confirma el conocimiento existente, p.ej., información frente a confirmación.
  - Contingencia
  - El atributo que identifica la información que es requerida como precedente de esta información (para que sea considerada como información).
- **Capa del mundo social**—El mundo que se construye socialmente mediante el uso de estructuras de la lengua en el nivel pragmático de la semiótica, p.ej., contratos, leyes, cultura.
  - Contexto — El atributo que identifica el contexto en el que la información tiene sentido, se utiliza, tiene un valor, etc., p.ej., el contexto cultural, el dominio del contexto del asunto.

Otras consideraciones acerca de la información: Las inversiones en información y tecnologías relacionadas se basan en los casos de negocio, que incluyen análisis coste-beneficio. El coste y beneficio no se refiere sólo a factores tangibles y medibles, sino que también tiene en cuenta factores intangibles tales como la ventaja competitiva, la satisfacción del cliente y la incertidumbre de la tecnología. Sólo cuando se aplica o se utiliza el recurso de la información es cuando una empresa genera beneficios de la misma, por lo que el valor de la información está determinado

únicamente a través de su uso (internamente o mediante su venta), ya que la información no tiene valor intrínseco. Es sólo cuando se pone la información en acción cuando se puede generar ese valor.

IM es un modelo nuevo y es muy rico en términos de diferentes componentes. Este modelo se desarrollará en el futuro en una publicación aparte. Para hacerlo más tangible para el usuario de COBIT 5, y para hacer su relevancia más clara en el contexto general del marco de COBIT 5, se proporcionan los ejemplos 13, 14 y 15 de posible utilización de IM.

MODELO DE INFORMACIÓN UTILIZADO PARA LAS ESPECIFICACIONES DE LA INFORMACIÓN

Cuando se desarrolla una nueva aplicación, IM se puede utilizar para ayudar con las especificaciones de la aplicación y la información o modelos de datos asociados.

Los atributos de información de IM se pueden utilizar para definir las especificaciones de la aplicación y los procesos de negocio que va a utilizar la información.

Por ejemplo, el diseño y las especificaciones del nuevo sistema necesitan especificar:
- **Capa física**—¿Dónde se almacenará la información?
- **Capa empírica**—¿Cómo se puede acceder a la información?
- **Capa sintáctica**—¿Cómo se estructurará y codificará la información?
- **Capa semántica**—¿Qué tipo de información es? ¿Cuál es el nivel de información?
- **Capa pragmática**—¿Cuáles son los requisitos de retención? ¿Qué otra información es necesaria para que esta información sea útil y utilizable?

En cuanto a la dimensión de los interesados combinado con el ciclo de vida de la información, se puede definir quién tendrá qué tipo de acceso a los datos durante qué fase del ciclo de vida de la información.

Cuando se pruebe la aplicación, los probadores pueden mirar los criterios de información de calidad para desarrollar un amplio conjunto de casos de prueba.

MODELO DE INFORMACIÓN PARA DETERMINAR LA PROTECCIÓN NECESARIA

Los grupos de seguridad dentro de la empresa se pueden beneficiar de la dimensión de los atributos de IM, cuando se les encarga la protección de la información, siendo necesario establecer:
- **Capa física**—¿Cómo y dónde se almacena físicamente la información?
- **Capa empírica**—¿Cuáles son los canales de acceso a la información?
- **Capa sintáctica**—¿Cuáles son los requisitos de retención? ¿La información es histórica u operacional?

El uso de estos atributos permitirá al usuario determinar el nivel de protección y los mecanismos de protección necesarios.

En cuanto a otra dimensión IM, los profesionales de la seguridad también pueden considerar las etapas del ciclo de vida de la información, ya que la información tiene que ser protegida durante todas las fases del ciclo de vida. De hecho, la seguridad comienza en la fase de planificación de la información e implica diferentes mecanismos de protección para el almacenamiento, el intercambio y la eliminación de información. IM asegura que la información esté protegida durante todo el ciclo de vida de la información.

Habilitador 6 – Servicios, Infraestructura y Aplicaciones

Las capacidades de servicio se refieren a recursos tales como las aplicaciones y las infraestructuras que están movilizadas en la prestación de servicios relacionados con TI.

Los detalles para el catalizador de las capacidades de servicio en comparación con la descripción genérica de catalizador se muestran en la figura a continuación.

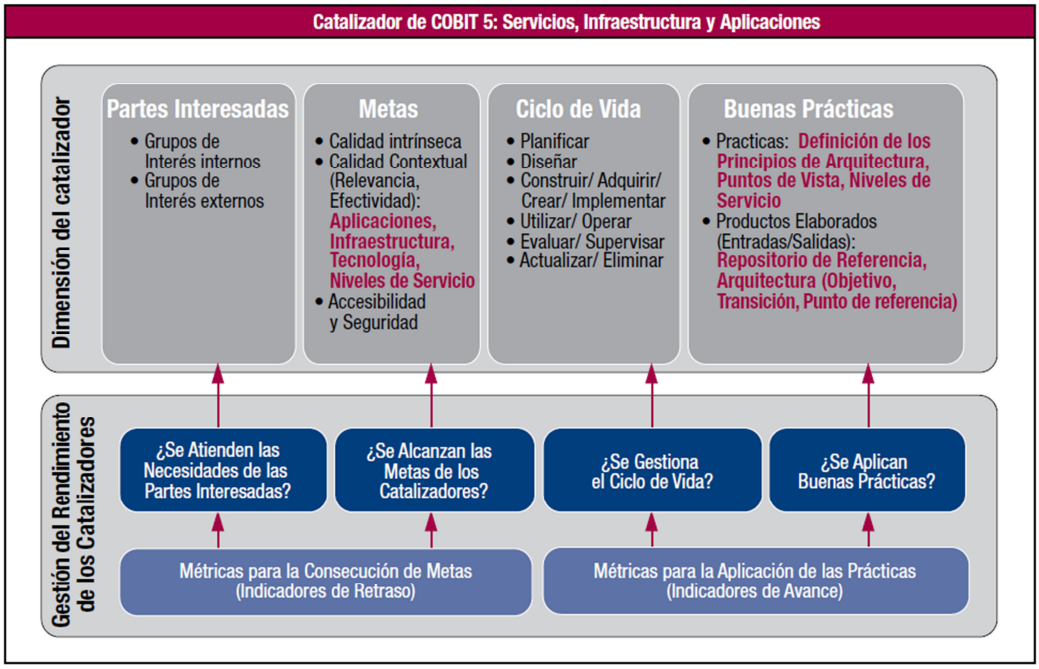
El modelo de servicios, la infraestructura y aplicaciones muestra:

- **Partes interesadas**—Las partes interesadas de las capacidades de servicio (el concepto combinado de servicios, infraestructura y aplicaciones) pueden ser internas y externas. Los servicios pueden ser entregados por las partes internas o externas — departamentos

de TI internos, gerentes de operaciones, proveedores de outsourcing. Los usuarios de los servicios también pueden ser internos — los usuarios del negocio — y externos a la empresa — socios empresariales, clientes, proveedores. Las participaciones de cada una de las partes interesadas deben ser identificadas y, o bien estarán centradas en la entrega adecuada de servicios o en la recepción de los servicios solicitados a los proveedores.

- **Metas**—Las metas de la capacidad de nivel de servicio se expresan en términos de servicio — aplicaciones, infraestructura, tecnología — y de niveles de servicio, teniendo en cuenta que los servicios y niveles de servicio son más económicos para la empresa. Una vez más, las metas se refieren a los servicios y la forma en que se proporcionan, así como sus resultados, es decir, la contribución a los procesos de negocio apoyado con éxito.

- **Ciclo de vida**—Las capacidades de servicios tienen un ciclo de vida. Las capacidades de servicio en el futuro o en proyecto se describen normalmente mediante una arquitectura objetivo. Dicha arquitectura cubre los bloques constituyentes, tales como futuras aplicaciones y el modelo de infraestructura objetivo y también describe los vínculos y las relaciones entre estos bloques de construcción.



Las capacidades de servicio actuales que se utilizan u operan para entregar servicios de TI actuales se describen en una arquitectura de base. Dependiendo del marco de tiempo de la arquitectura

objetivo, se puede definir también una arquitectura de transición, que muestre la empresa en estados incrementales entre el objetivo y la arquitectura de referencia.

- **Buenas prácticas**—Las buenas prácticas de las capacidades de servicio incluyen:

– Definición de los principios de arquitectura - Los principios de arquitectura son directrices generales que rigen la implementación y utilización de los recursos relacionados con las TI dentro de la empresa. Ejemplos de principios de arquitectura posibles:

- **Reutilización**—Los componentes comunes de la arquitectura deberían ser utilizados en el diseño e implementación de soluciones como parte de las arquitecturas objetivo o de transición.

- **Comprar frente a construir**—Las soluciones deberían ser adquiridas a menos que exista una razón para aprobar su desarrollo interno.

- **Simplicidad**—La arquitectura de la empresa debería ser diseñada y mantenida para ser tan simple como sea posible sin dejar de cumplir con los requisitos de la empresa.

- **Agilidad**—La arquitectura de la empresa debería incorporar agilidad para satisfacer las cambiantes necesidades de negocio de una manera eficaz y eficiente.

- **Apertura**—La arquitectura de la empresa debería aprovechar los estándares abiertos de la industria.

– La definición empresarial de los puntos de vista de la arquitectura más adecuados para satisfacer las necesidades de los diferentes interesados.

Esta definición comprende los modelos, catálogos y matrices utilizados para describir la arquitectura base, objetivo o de transición; por ejemplo, una arquitectura de aplicación se podría describir a través de un diagrama de interfaz de la aplicación, que muestra las aplicaciones en uso (o previstas) y las interfaces entre ellas.

– Disponer de un repositorio de arquitectura, que se puede utilizar para almacenar diferentes tipos de productos arquitectónicos, incluyendo los principios de la arquitectura

y estándares, modelos de arquitectura de referencia y otras prestaciones de arquitectura y que define los bloques que componen los servicios tales como:

- Las aplicaciones que proporcionan la funcionalidad empresarial
- La infraestructura tecnológica, incluyendo el hardware, el software del sistema y la infraestructura de redes
- La infraestructura física

– Los niveles de servicio que deben ser definidos y alcanzados por los proveedores de servicio

Existen buenas prácticas externas para los marcos de arquitectura y capacidades de servicio. Dichas buenas prácticas son guías, plantillas o normas que pueden ser utilizados para acelerar la elaboración de los entregables de la arquitectura.

Algunos ejemplos:

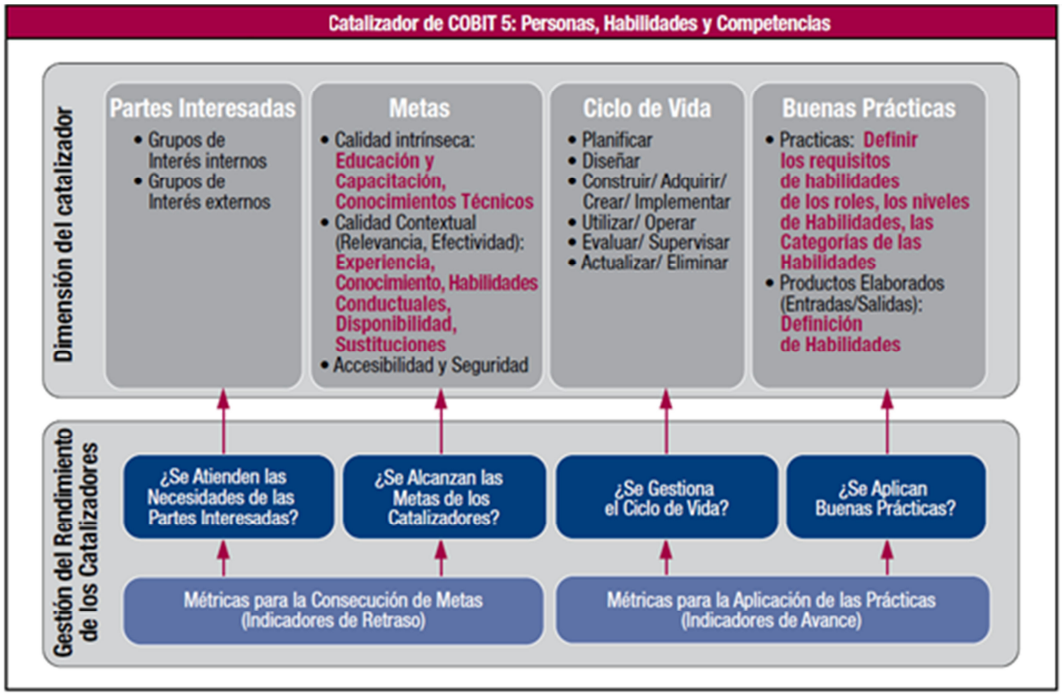
– TOGAF16 proporciona un Modelo de Referencia Técnica y un Modelo de Referencia de Infraestructura de Información Integrada.
– ITIL proporciona una guía completa sobre cómo diseñar y operar los servicios.

- **Relaciones con otros catalizadores**—Los vínculos con otros catalizadores incluyen:

– La información es una de las capacidades de servicio y las capacidades de servicio se apalancan a través de procesos para la entrega de servicios internos y externos.
– Los aspectos culturales y de comportamiento también son relevantes cuando se tiene que construir una cultura orientada al servicio.
– Dentro de COBIT 5, las entradas y salidas de las prácticas y las actividades de gestión podrían incluir las capacidades de servicio, las cuales son requeridas como entradas o entregadas como salidas.

Habilitador 7 – Personas, Habilidades y Competencias

Los detalles específicos del catalizador personas, habilidades y competencias en comparación con la descripción genérica de catalizador se muestran en la figura a continuación.



El modelo de personas, habilidades y competencias muestra:

- **Partes Interesadas**: Las capacidades y competencias de las partes interesadas son internas y externas a la empresa.

Diferentes interesados asumen diferentes roles— directivos empresariales, gerentes de proyecto, socios, competidores, formadores, reclutadores, desarrolladores, técnicos especialistas en IT, etc. —y cada papel requiere un conjunto de habilidades diferentes.

- **Metas:** Las metas de habilidades y competencias se relacionan con los niveles de educación y capacitación, habilidades técnicas, niveles de experiencia, conocimientos y habilidades de comportamiento necesarios para proporcionar y llevar a cabo con éxito las actividades del proceso, las funciones de organización, etc. Las metas de las personas incluyen los niveles adecuados de disponibilidad de personal y la tasa del volumen de negocios.

- **Ciclo de vida:**

  - Las habilidades y competencias tienen un ciclo de vida. Una empresa tiene que saber cuál es su base de conocimientos actual y planificar lo que tiene que ser. Esto se ve influido por (entre otras cuestiones) la estrategia y metas de la empresa. Las habilidades

necesitan ser desarrolladas (por ejemplo, a través de la formación) o adquiridas (por ejemplo, a través de la contratación) y desplegadas en los diversos roles dentro de la estructura organizativa. Posiblemente tengan que ser eliminadas habilidades, por ejemplo, si una actividad es automatizada o subcontratada.

- Periódicamente, por ejemplo anualmente, la empresa necesita evaluar las competencias básicas para entender la evolución que se ha producido, y que se utilizará en el proceso de planificación para el próximo período.
- Esta evaluación también puede contribuir a la recompensa y el proceso de reconocimiento para los recursos humanos.

- **Buenas prácticas:**

- Las buenas prácticas de habilidades y competencias incluyen la definición de la necesidad de requisitos de formación objetivos para cada papel desempeñado por las distintas partes interesadas. Esto se puede describir mediante diversos niveles de habilidad en las diferentes categorías de habilidades. Para cada nivel de habilidad apropiado en cada categoría profesional, debería estar disponible una definición de las cualificaciones. Las categorías de habilidades se corresponden con las actividades relacionadas con las TI realizadas, por ejemplo, la gestión de la información, el análisis de negocios.

- Otra buena práctica:

- Hay fuentes externas de buenas prácticas, tales como el Marco de Competencias para la Era de la Información (SFIA-Skills Framework for the Information Age, que establece las definiciones generales de habilidad.
- En la figura a continuación se muestran ejemplos de categorías de habilidades potenciales, mapeadas con los dominios de proceso de COBIT 5.

Categorías de Habilidades de COBIT 5	
Dominio de Procesos	**Ejemplos de Categorías de Habilidades**
Evaluar, Orientar y Supervisar (EDM)	• Gobierno de TI Empresarial
Alinear, Planificar y Organizar (APO)	• Formulación de políticas de TI • Estrategia TI • Arquitectura de la empresa • Innovación • Gestión Financiera • Gestión de la Cartera
Construir, Adquirir e Implementar (BAI)	• 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)	• 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)	• Revisión de cumplimiento • Supervisión del rendimiento • Auditoría de Controles

- **Relaciones con otros catalizadores**—Los vínculos con otros catalizadores incluyen:

  - Habilidades y competencias necesarias para realizar las actividades del proceso y tomar decisiones en las estructuras organizativas. Por el contrario, algunos procesos tienen como objetivo apoyar el ciclo de vida de las habilidades y competencias.
  - También hay un enlace a la cultura, la ética y la conducta a través de las habilidades de comportamiento, que impulsan el comportamiento individual y están influidas por la ética individual y la ética de la organización.
  - La definición de capacidades también es información, para la cual deben ser consideradas las mejores prácticas del catalizador de información.

4. IMPLEMENTACIÓN DE COBIT 5

Según lo mencionado en el documento de (ISACA, 2012) se "ha desarrollado el marco de COBIT 5 para ayudar a las compañías a implementar unos habilitadores de gobierno sanos. De hecho, la implementación de un buen Gobierno Corporativo de la Tecnología de la Información, es casi imposible sin la activación de un marco efectivo de gobierno. También están disponibles las mejores prácticas y los estándares que soportan al COBIT 5."

Los marcos, mejores prácticas y normas son útiles solamente si son adoptados y adaptados de manera efectiva. Hay que superar muchos retos y resolver varios asuntos para poder implementar GEIT de manera exitosa.

4.1. Beneficios de implementar COBIT

Las características de los beneficios son:

- Proveer un marco único reconocido a nivel mundial de las "mejores prácticas" de control y seguridad de TI
- Consolidar y armonizar estándares originados en diferentes países desarrollados.
- Concientizar a la comunidad sobre importancia del control y la auditoría de TI.
- Enlaza los objetivos y estrategias de los negocios con la estructura de control de la TI, como factor crítico de éxito
- Aplica a todo tipo de organizaciones independiente de sus plataformas de TI
- Ratifica la importancia de la información, como uno de los recursos más valiosos de toda organización exitosa.

4.2. Pasos para implementar COBIT

Comenzar en la estructura con los objetivos del negocio
Seleccionar los objetivos de control, los procesos y objetivos de control de TI apropiados para la empresa.

Operar desde el plan de negocios.

Evaluar con las guías de Auditoría los procedimientos y resultados.

Evaluar con las Guías de Administración el estado de la organización, identificar las actividades críticas conducentes al éxito y medir el desempeño para alcanzar los objetivos de la empresa.

4.3. Evaluación con las guías de Auditoría las Prácticas actuales

- Aceptar los principios del Modelo Cobit y definir que la organización lo adoptará e implementará
- Como se ha decidido adoptarlo, se tiene que familiarizar con él y ajustar los procesos a sus requerimientos
- Capacitarse y capacitar a todos los funcionarios que tendrán relación, se parte de la estrategia empresarial.
- Realizar la Evaluación de riesgos y a elaborar el Plan de Evaluación

4.4. Guía de implementación COBIT 5

La Guía de Implementación COBIT 5 cubre los siguientes asuntos:

- Posicionamiento del Gobierno Corporativo de la Tecnología de la Información (GEIT) en la organización
- Adopción de los primeros pasos para mejorar GEIT
- Factores de éxito y retos para la implementación
- Habilitación del cambio de comportamiento y organizacional relacionado con el GEIT
- Implementación de una mejora continua que incluye la habilitación del cambio y la gestión del programa
- Uso de COBIT 5 y sus componentes.
- Incremento de la creación de valor a través un gobierno y gestión efectiva de la información y de los activos tecnológicos. La función de TI se vuelve más enfocada al negocio
- Incremento de la satisfacción del usuario con el compromiso de TI y sus servicios prestados – TI es visto como facilitador clave.
- Incremento del nivel de cumplimiento con las leyes regulaciones y políticas relevantes
- Las personas que participan son más proactivas en la creación de valor a partir de la gestión de TI.

4.5. Facilitar el cambio

Una implementación con éxito depende de implementar el cambio apropiado (los catalizadores apropiados de gobierno o gestión) del modo adecuado. En muchas empresas, hay un importante foco en el primer aspecto – gobierno o gestión de TI esenciales – pero no el suficiente énfasis en

gestionar los aspectos humanos, culturales y de comportamiento del cambio y motivar a los interesados en involucrarse con el mismo.

No debería darse por hecho que las diferentes partes interesadas implicadas en, o impactadas por, un nuevo o actualizado catalizador aceptarán o adoptarán rápidamente el cambio. La posibilidad de desconocer y/o la resistencia al cambio necesitan ser resueltas mediante un enfoque estructurado y proactivo. Además, deberíamos conseguir la óptima concienciación en la implementación del programa mediante un plan de comunicación que defina lo que será comunicado, de qué manera y por quién, a lo largo de las distintas fases del programa.

La mejora sostenible se puede conseguir bien mediante la adquisición del compromiso de las partes implicadas (invirtiendo en ganar corazones y mentes y en comunicar y responder a los trabajadores) o, cuando sea necesario, mediante la exigencia del cumplimiento (invirtiendo en procesos para administrar, supervisar e imponer). En otras palabras, deben superarse las barreras humanas, el comportamiento y la cultura de modo que haya un interés común en adoptar apropiadamente el cambio, infundiendo el deseo de adoptarlo y asegurando la capacidad de adopción.

4.6. Un enfoque de ciclo de vida

La implementación del ciclo de vida proporciona a las empresas una manera de usar COBIT para solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones. Los tres componentes interrelacionados del ciclo de vida son:

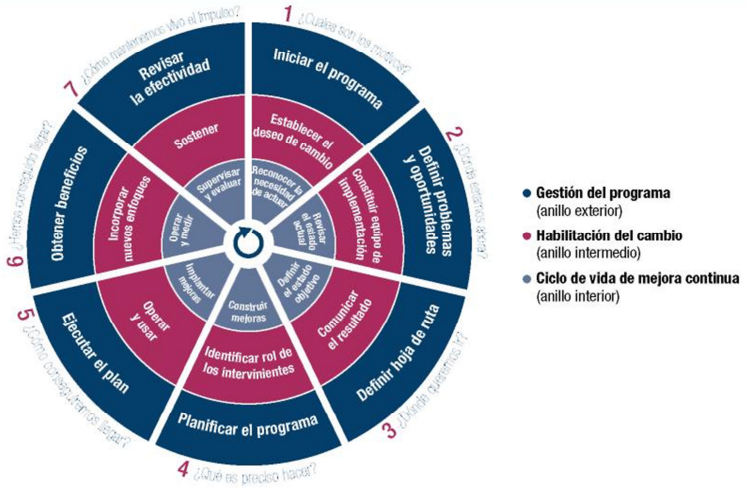
Ciclo de vida de Mejora continua – Este no es un proyecto único.

Habilitación del cambio – Abordar los aspectos culturales y de comportamiento.

Gestión del programa-

Como se ha comentado anteriormente, se debe crear un entorno apropiado para asegurar el éxito de la implementación o de la iniciativa de mejora. El ciclo de vida y sus siete fases se ilustran en la siguiente imagen:

Figura 17—Las Siete Fases de la Implementación del Ciclo de Vida



La fase 1 comienza con el reconocimiento y aceptación de la necesidad de una iniciativa de implementación o mejora. Identifica los puntos débiles actuales y desencadena y crea el ánimo de cambio a un nivel de dirección ejecutiva.

La fase 2 se concentra en definir el alcance de la iniciativa de implementación o mejora empleando el mapeo de COBIT de metas empresariales con metas de TI a los procesos de TI asociados, y considerando cómo los escenarios de riesgos podrían destacar los procesos clave en los que focalizarse. Los diagnósticos de alto nivel también pueden ser útiles para delimitar y entender áreas de alta prioridad en las que hacer foco. Se lleva a cabo una evaluación del estado actual y se identifican los problemas y deficiencias mediante la ejecución de un proceso de revisión de capacidad. Se deberían estructurar iniciativas de gran escala como múltiples iteraciones del ciclo de vida - para cada iniciativa de implementación que exceda de seis meses, existe un riesgo de perder el impulso, el foco y la involucración de las partes interesadas.

Durante la **fase 3**, se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos (quick wins) y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

La fase 4 planifica soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados. Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

Las soluciones propuestas son implementadas en prácticas día a día **en la fase 5**. Se pueden definir las mediciones y establecer la supervisión empleando las metas y métricas de COBIT para asegurar que se consigue y mantiene la alineación con el negocio y que el rendimiento puede ser medido. El éxito requiere el compromiso y la decidida apuesta de la alta dirección así como la propiedad por las partes afectadas a nivel TI y de negocio.

La fase 6 se focaliza en la operación sostenible de los nuevos o mejorados catalizadores y de la supervisión de la consecución de los beneficios esperados.

Durante **la fase 7**, se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua.

A lo largo del tiempo, el ciclo de vida debería seguirse de modo iterativo, al tiempo que se construye un modelo sostenible de gobierno y gestión de TI corporativa.

5. VENTAJAS Y DIFERENCIAS DE COBIT 5

5.1. Beneficios del COBIT 5

Los beneficios en las organizaciones y sus ejecutivos son los siguientes:

- Mantener información de calidad para apoyar las decisiones del negocio.
- Generar un valor comercial de las inversiones habilitadas por la Tecnología de la Información (TI), o sea: lograr metas estratégicas y mejoras al negocio mediante el uso eficaz e innovador de la TI.

- Lograr una excelencia operativa mediante la aplicación eficiente y fiable de la tecnología.
- Mantener el riesgo relacionado con TI a niveles aceptables.
- Optimizar el costo de la tecnología y los servicios de TI.
- Incrementar la creación de valor a través un gobierno y gestión efectiva de la información y de los activos tecnológicos. La función de TI se vuelve más enfocada al negocio.
- Incrementar la satisfacción del usuario con el compromiso de TI y sus servicios prestados – TI es visto como facilitador clave.
- Incrementar del nivel de cumplimiento con las leyes regulaciones y políticas relevantes.

Las personas que participan son más proactivas en la creación de valor a partir de la gestión de TI.

¿Cómo se logran estos beneficios con el fin de crear valor para las partes interesadas de la organización?

- Para lograr valor para las partes interesadas de la Organización, se requiere un buen gobierno y una buena administración de los activos de TI y de la información.

- Los Directivos, Gerentes y Ejecutivos de las Organizaciones deben acoger la TI como cualquier otra parte importante del negocio.

- Cada día aumentan y se complican más los requisitos externos, tanto legales como de cumplimiento regulatorio y contractual, relacionados con el uso de la información y la tecnología en la Organización, amenazando el patrimonio si no se cumplen.

- COBIT5 proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la Organización.

El Marco de COBIT 5

- Dicho en pocas palabras, 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.

- "COBIT 5 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." (ISACA, 2012)

- 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.

5.2. Diferencias del COBIT 5

A continuación se muestra las diferencias entre COBIT 4.1 y COBIT 5

Nuevo Modelo de Referencia de Procesos

El nuevo modelo puede ser utilizado como una guía para ajustar según sea necesario propio modelo de proceso de la empresa (al igual que COBIT 4.1).

Los objetivos de control de alto nivel ahora se llaman "procesos" y los objetivos de control detallados ahora son identificados como "prácticas", ya sea de gobierno o de administración, dependiendo del dominio que, como mencioné antes, son cinco para esta nueva versión: el primero corresponde a gobierno y los siguientes cuatro a administración.

Es importante resaltar que ahora para cada "práctica" se detallan las entradas y salidas, que son los productos de trabajo que toman de otras prácticas, y los entregables que produce o genera dicha práctica, que van hacia otras prácticas de otros procesos respectivamente. En la versión anterior de COBIT solo se definían las entradas y salidas por proceso, lo cual ahora proporciona un desarrollo más detallado de las actividades que se tienen que realizar y sus correspondientes productos a generar.

Se incorporan procesos totalmente nuevos dentro de los que se considera:

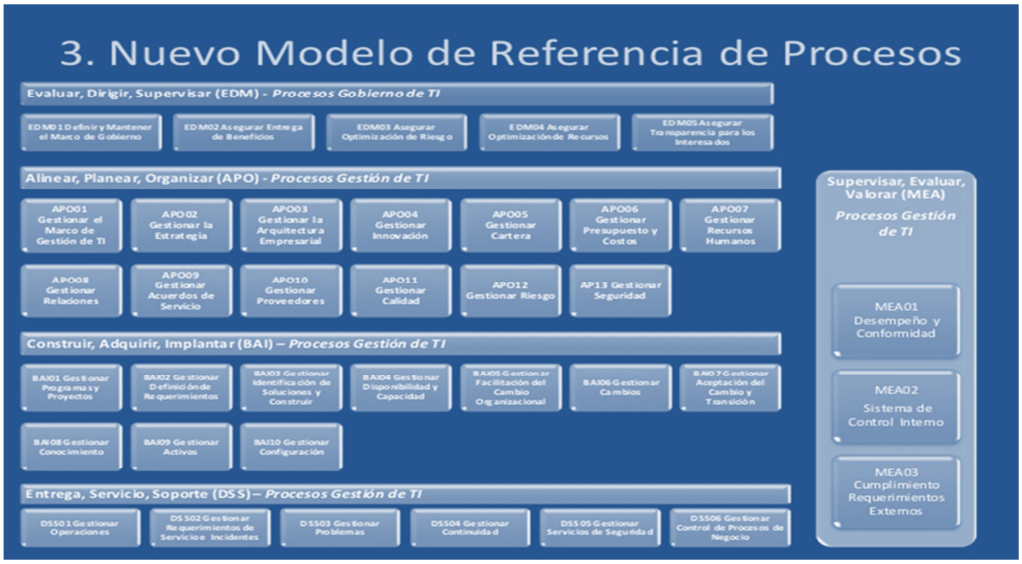
- EDM1 Establecer y Mantener el Marco de Gobierno
- APO1 Administrar el Marco de la Administración de TI
- APO4 Administrar la Innovación (parcialmente PO3)
- APO8 Administrar las Relaciones
- BAI8 Administrar el Conocimiento
- DSS2 Administrar los Activos (parcialmente DS9)
- DSS6 Administrar los Controles en los Procesos de Negocios.

Otro de los cambios importantes respecto a las versiones anteriores de Cobit está en el modelo de nivel de madurez de cada proceso, ahora toma como referencia a ISO/IEC 15504 en lugar del CMM. Para poder identificar el nivel de madurez de cada práctica de gobierno o de administración, se debe utilizar otro documento de ISACA llamado "process assessment model (PAM) using COBIT 4.1", que, a pesar de estar orientado a COBIT 4.1, como es genérico se puede ocupar para COBIT 5.

En resumen, la nueva versión de Cobit busca ser el referente principal para procesos de tecnologías de información, ayudando a diseñar procesos, definir responsabilidades, establecer prácticas y actividades, así como a definir los entregables. Todo con el propósito de contar con una correcta

administración de servicios de tecnología de información, proporcionando con esto una calidad mejorada en la entrega de servicios de TI vía procesos. (ISACA, 2012)

Diagrama de procesos y el mapeo con COBIT 4.1, para que refleje con mayor exactitud la versión de COBIT 5 publicada por ISACA como definitiva y oficial:



Procesos y Dominios:

A nivel de la estructura de Procesos y Dominios esto es lo más relevante del comparativo entre ambas versiones:

Existe un nuevo Dominio (ahora son 5), que se enfoca en aspectos de Gobierno de TI, denominado "EDM – Evaluar, Dirigir & Monitorear" y que cubre el antiguo proceso ME4 de COBIT 4.

La cantidad de procesos se ha incrementado de 34 a 37 (en el draft eran 36, se agregó APO013 "Gestionar Seguridad").

Si bien los objetivos de control que corresponden a cada proceso de COBIT 4, se mantienen mayoritariamente dentro del mismo Dominio, existen excepciones como las siguientes:

1. PO10 – Administrar los proyectos, pasó al Dominio BAI.
2. AI5 – Procurar recursos de IT, pasó al Dominio APO.
3. DS1 – Definir y Administrar los niveles de servicio, pasó al Dominio APO.

4. DS2 – Administrar los servicios de Terceros, pasó al Dominio APO.
5. DS3 – Administrar el desempeño y la capacidad, pasó al Dominio BAI.
6. DS6 – Identificar y asignar costos, pasó al Dominio APO.
7. DS7 – Educar y Entrenar a los usuarios, pasó al Dominio APO.

En el dominio APO – Administrar, Planear y Organizar, es donde se observa mayor reorganización interna de los objetivos de control, es decir que un antiguo proceso de COBIT 4, ahora puede estar distribuido como parte de hasta 5 procesos del mismo dominio en COBIT 5.
El proceso DS12 – Administrar el Ambiente Físico ahora forma parte del DSS5 – Gestionar los Servicios de Seguridad.

Existen nuevos procesos cuyo contenido es mayormente producto de COBIT 5, destacándose:

1. EDM1 – Definir el Framework para el Governance
2. APO1 – Definir el Framework para el Management
3. APO4 – Gestionar Innovación
4. APO13 – Gestionar Seguridad (también hay un Proceso DSS05 Gestionar los Servicios de Seguridad)
5. BAI8 – Gestión del Conocimiento

A continuación, se expone un cuadro con el mapeo realizado entre los procesos de COBIT 4.1 y su cobertura en COBIT5, destacando que se tomó como fuente el material de ISACA incluido en Anexo de la Guía de Procesos de Referencia, pero dado que estaba desglosado por Objetivo de Control, se lo consolidó a nivel Proceso, destacando como "Primaria" al Proceso de COBIT 5 que mayor cobertura (en %) les brinda a los objetivos de control del antiguo proceso de COBIT 4.1.

COBIT 4.1		COBIT 5 - Cobertura (P)rimaria y (S)ecundaria	
Proceso	Descripción	Primaria	Secundaria
PO	Planear y Organizar	Alinear, Planear y Organizar	
PO1	Definir un plan estratégico de TI	APO02	EDM02 / APO05
PO2	Definir la arquitectura de la información	APO03	APO01
PO3	Definir la dirección tecnológica	APO02 / APO04	EDM01 / APO03 / APO01
PO4	Definir los procesos organización y relaciones de TI	APO01	APO07 / APO11 / DSS06
PO5	Administrar la inversión en TI	APO06	APO05
PO6	Comunicar las metas y la dirección de la gerencia	APO01	EDM03
PO7	Administrar los recursos humanos de TI	APO07	APO01
PO8	Administrar la calidad	APO11	
PO9	Evaluar y administrar los riesgos de TI	APO12	EDM03 / APO01
PO10	Administrar los proyectos	BAI01	
AI	Adquirir e Implementar	Construir, Adquirir e Implementar	
AI1	Identificar las soluciones automatizadas	BAI02	
AI2	Adquirir y mantener software aplicativo	BAI03	
AI3	Adquirir y mantener la infraestructura tecnológica	BAI03	DSS02
AI4	Facilitar la operación y el uso	BAI08	BAI05
AI5	Procurar recursos de TI	APO10	BAI03
AI6	Administrar los cambios	BAI06	
AI7	Instalar y acreditar las soluciones y cambios	BAI07	BAI05
DS	Entregar Servicio	Entregar Servicio y Soportar	
DS1	Definir y administrar los niveles de servicio	APO09	
DS2	Administrar los servicios de terceros	APO10	
DS3	Administrar el desempeño y la capacidad	BAI04	
DS4	Asegurar el servicio continuo	DSS04	
DS5	Garantizar la seguridad de los sistemas	DSS05	APO13
DS6	Identificar y asignar costos	APO06	
DS7	Educar y entrenar a los usuarios	APO07	
DS8	Administrar la mesa de servicio y los incidentes	DSS02	
DS9	Administrar la configuración	BAI10	DSS02
DS10	Administrar los problemas	DSS03	
DS11	Administrar los datos	DSS04	DSS01 / DSS05 / DSS06
DS12	Administrar el ambiente físico	DSS01 / DSS05	
DS13	Administrar las operaciones	DSS01	DSS05 / BAI09
ME	Monitorear y Evaluar	Monitorear y Evaluar	
ME1	Monitorear y evaluar el desempeño de TI	MEA01	
ME2	Monitorear y evaluar el control interno	MEA02	
ME3	Garantizar el cumplimiento regulatorio	MEA03	
ME4	Proporcionar gobierno de TI	EDM01 / EDM02 / EDM03 / EDM04 / MEA02	

Procesos nuevos y modificados

COBIT 5 introduce cinco nuevos procesos de gobernabilidad que han apalancadas y la mejora de COBIT 4.1, Val IT y riesgo que los enfoques de gobernanza.

Esta orientación ayuda a las empresas para perfeccionar y fortalecer las prácticas y actividades GEIT-nivel de gestión ejecutivas.

Soporta integración GEIT con prácticas de gobierno empresarial existentes y está alineado con? La norma ISO / IEC 38500

Risk IT

Hay varios procesos nuevos y modificados que reflejan el pensamiento actual, en particular:

- APO03 Gestione la arquitectura empresarial.
- APO04 Gestione la innovación.
- APO05 Administrar cartera.
- APO06 Administrar el presupuesto y los costos.
- APO08 Administrar relaciones.
- APO13 Administrar la seguridad.
- BAI05 Administrar el cambio organizacional habilitación.
- BAI08 gestionar el conocimiento.
- BAI09 Administrar activos.
- DSS05 Administrar servicio de seguridad.
- DSS06 Administrar controles de procesos de negocio.
- COBIT 5 procesos cubre negocios de extremo a extremo y actividades de TI, es decir, una visión completa de nivel empresarial.

Esto proporciona una cobertura más integral y completa de las prácticas que refleja la naturaleza en toda la empresa dominante de uso de TI.

Esto hace que la participación, las responsabilidades y la rendición de cuentas de accionistas de la empresa en el uso de TI más explícita y transparente**.**

Prácticas y actividades

En COBIT 5 prácticas de gobierno o de gestión son equivalentes a los objetivos de control de COBIT 4.1 y Val IT y riesgo los procesos de TI.

En COBIT 5 actividades son equivalentes a las prácticas de control de COBIT 4.1 y Val IT y Risk IT prácticas de gestión.

COBIT 5 integra y actualiza todos los contenidos de la anterior en el nuevo modelo, por lo que es más fácil para los usuarios a entender y utilizar este material en la aplicación de mejoras.

Objetivos y métricas

COBIT 5 sigue la misma meta y conceptos métricos como COBIT 4.1, Val IT y Risk IT, pero éstos se renombró objetivos de la empresa, los objetivos relacionados con la TI y los objetivos del proceso que reflejan una visión a nivel de empresa.

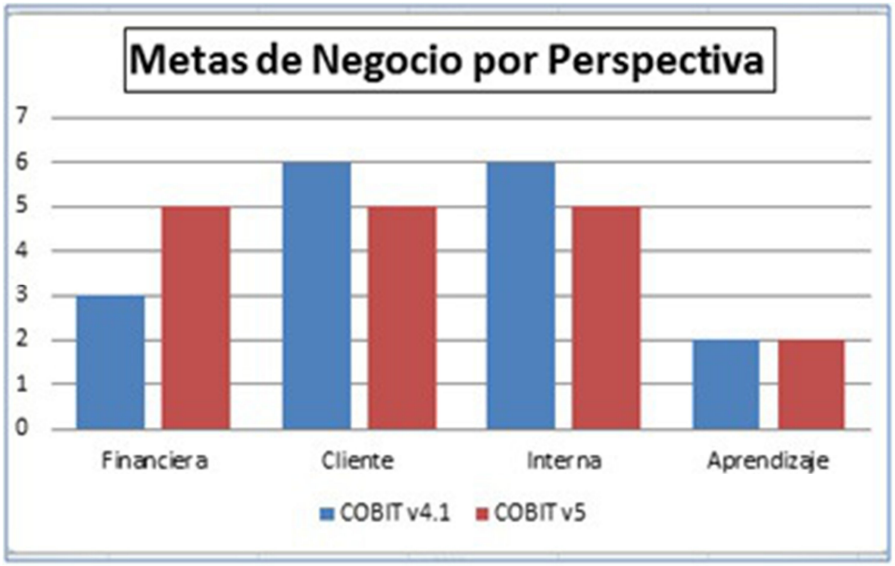
COBIT 5 ofrece una cascada de metas revisado basado en objetivos empresariales que impulsan los objetivos relacionados con la TI y luego con el apoyo de los procesos críticos

COBIT 5 ofrece ejemplos de objetivos y métricas a nivel de empresa, los procesos y prácticas de gestión. Este es un cambio de COBIT 4.1, Val IT y Risk IT, que bajó un nivel inferior.

Metas de Negocio y Metas de TI:

Respecto a la relación habitual entre Metas de Negocio y Metas de TI, COBIT 5 ha mejorado en cuanto a la precisión del grado de relevancia de dicho nexo, dado que ahora se la discrimina en "Primaria" o "Secundaria", mientras que en COBIT 4 sólo se la marcaba con una tilde genérico.

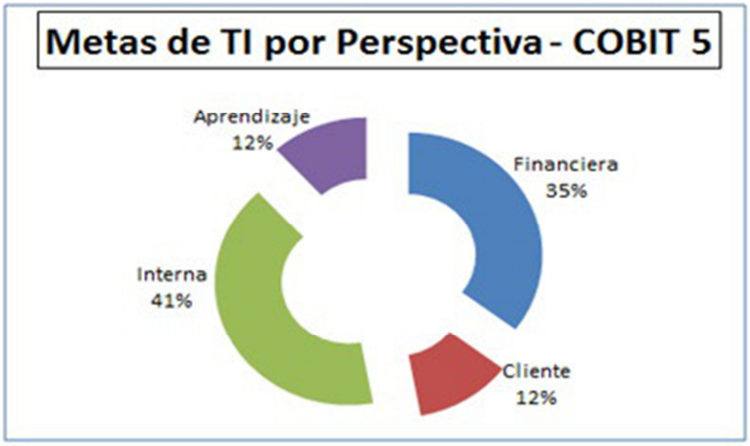
En COBIT 5 se mantiene la cantidad de Metas de Negocio (17) pero ha cambiado de COBIT 4.1 sus contenidos y la distribución respecto a las Perspectivas del Balanced Scorecard, tal como se detalla a continuación:



Con respecto a las Metas de TI, COBIT 5 ha efectuado dos cambios importantes comparativamente con COBIT 4.1:

- Disminuyó la cantidad de 28 a 17 Metas.

Para cada Meta de TI se indica a cuál Perspectivas del Balanced Scorecard corresponde:



Otro de los cambios significativos es el haber transformado el famoso "Pentágono" del Gobierno de TI de COBIT 4.1 prácticamente en el nuevo dominio denominado "EDM – Evaluar / Dirigir & Monitorear":

Pentágono de COBIT 4.1:	Cobertura en COBIT 5:
Alineación Estratégica	Prácticas de Evaluar y Dirigir (Governance) Práctica de Dirigir (Management)
Entrega de Valor	Proceso EDM2
Gestión de Riesgos	Proceso EDM3
Gestión de Recursos	Proceso EDM4
Medición del Desempeño	Proceso EDM5 y Práctica de Monitoreo

COBIT 4.1	COBIT 5
Efectividad	Utilidad
Eficiencia	Usabilidad
Integridad	Libre de error
Confiabilidad	Credibilidad
Disponibilidad	Accesibilidad
Confidencialidad	Seguridad
Cumplimiento	Conformidad

Entradas y salidas

COBIT 5 ofrece entradas y salidas para cada práctica de manejo, mientras que COBIT 4.1 sólo se proporcionó estas otras a nivel de proceso.

Esto proporciona orientación adicional detallada para el diseño de procesos para incluir productos de trabajo esenciales y para ayudar con la integración entre procesos.

Cuadro RACI

COBIT 5 ofrece gráficos RACI que describen las funciones y responsabilidades de una manera similar a COBIT 4.1, Val IT y de riesgos de TI.

COBIT 5 ofrece una gama más completa, detallada y clara de negocio y de TI jugadores y gráficos que COBIT 4.1 para cada práctica de gestión de roles genéricos, lo que permite una mejor definición de las responsabilidades de rol jugador o nivel de participación en el diseño e implementación de procesos. A continuación, se expone el mapeo oficial de ISACA entre ambos modelos de madurez:

COBIT 4. 1

RACI Chart — **Functions**

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain a technology infrastructure plan.		I	I	A		C	R	C	C		C
Create and maintain technology standards.				A		C	R	C	I	I	I
Publish technology standards.		I	I	A		I	R	I	I	I	I
Monitor technology evolution.		I	I	A		C	R	C		C	C
Define (future) (strategic) use of new technology.		C	C	A		C	R	C		C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

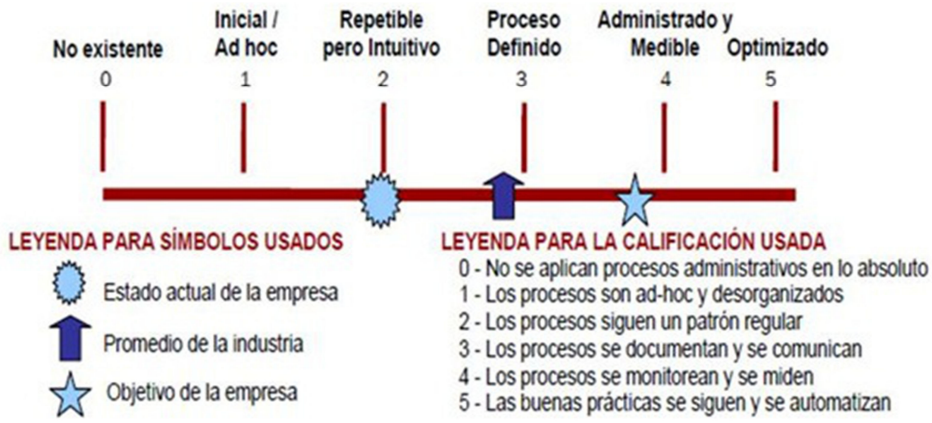
COBIT 5

RACI Chart

Key Governance Practice		Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01	Evaluate the design of the enterprise governance of IT.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02	Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03	Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

COBIT 5

Modelos de Madurez de Capacidad de Procesos y Evaluaciones



COBIT 5 interrumpe el COBIT 4.1, Val IT y Risk IT la capacidad de enfoque de modelado basado en la madurez CMM.

COBIT 5 será apoyado por un nuevo enfoque de evaluación de la capacidad del proceso basado en la norma ISO / IEC 15504, y el Programa de Evaluación de COBIT ya ha sido establecido para COBIT 4.1 como alternativa al enfoque CMM.

El COBIT 4.1, Val IT y Risk IT enfoques basados en CMM no se consideran compatibles con el enfoque de la norma ISO / IEC 15504, porque los métodos utilizan diferentes atributos y escalas de medición.

El enfoque del Programa de Evaluación de COBIT es considerado por ISACA para ser más robusto, fiable y repetible como un método de evaluación de la capacidad del proceso.

El Programa de Evaluación de COBIT es compatible con:

Las evaluaciones formales de los evaluadores acreditados (formación evaluador se está desarrollando).

Menos rigurosos autoevaluaciones para el análisis de brecha interna y la planificación de la mejora de procesos.

El Programa de Evaluación de COBIT, en el futuro, será también, potencialmente, permitir a una empresa para obtener una evaluación independiente y certificados alineados con la norma ISO / IEC.

Este nuevo modelo plantea las siguientes diferencias:

Al estar basado en ISO/IEC 15504 es más exigente respecto a lo que debe cumplir cada proceso para ascender de nivel, dado que este estándar plantear que se deben cumplir los 9 atributos definidos para cada proceso, como requisito para acreditar dicho grado de madurez.

Una evaluación realizada bajo este nuevo modelo no es comparable y no puede ser mezclada con evaluaciones realizadas bajo el modelo de COBIT 4.1, dado que se distorsionarían los resultados por ser distintas las exigencias.

Generalmente, aplicando este modelo de COBIT 5, deberían dar resultados de niveles más bajos de madurez.

A continuación, se expone el mapeo oficial de ISACA entre ambos modelos de madurez:

<table>
<tr><th>COBIT 4.1</th><th>COBIT 5
ISO 15504</th><th>Contexto</th></tr>
<tr><td>5. Optimizado</td><td>5. Optimizado</td><td rowspan="3">Empresa / Conocimiento Corporativo</td></tr>
<tr><td>4. Gestionado</td><td>4. Predecible</td></tr>
<tr><td>3. Definido</td><td>3. Establecido</td></tr>
<tr><td>N/A</td><td>2. Gestionado</td><td rowspan="3">Individual / Conocimiento Individual</td></tr>
<tr><td>N/A</td><td>1. Alcanzado</td></tr>
<tr><td>2. Repetible
1. Ad Hoc
0. No Existente</td><td>0. Incompleto</td></tr>
</table>

6. CONCLUSIONES

Ya entrada la segunda década del siglo XXI, la relevancia de TI en el funcionamiento de cualquier organización, sin importar su tamaño, es absolutamente incuestionable e indiscutida. Sin embargo, y en nuestra extensa experiencia como consultores y asesores de áreas de sistemas, no son pocos

los responsables de áreas de TI que manifiestan su dificultad al momento de mostrarle al negocio su aporte de valor.

Hace unos años se ha realizado un aporte ampliamente reconocido a través **del modelo de medición de la contribución del valor de TI al negocio.**

Complementariamente, también se ha promocionado desde 2007 el re-posicionamiento del CIO, Gerente de Sistemas o Gerente de TI como máximo responsable de la nueva Oficina de Procesos de Negocio.

Cinco años después, y en total sintonía con la visión de la evolución del CIO, ISACA publica la nueva versión de COBIT íntegramente enfocada a procesos, como Estratega sabe que es la mejor manera de abordar esta temática.

Así que estamos absolutamente convencidos que este enfoque está más cerca del negocio que el resto de los estándares y modelos que recomiendan mejores prácticas para la gestión interna de las áreas de Sistemas.

Conclusión del Comparativo entre ambos Modelos de Madurez:

Según indica ISACA en sus papers "COBIT 5, que saldría para los inicios del 2012, es la mayor evolución estratégica de COBIT 4.1, el único framework globalmente aceptado para el IT Governance y brinda a los interesados la guía más completa y actualizada para un mejor gerenciamiento de IT."

Sin embargo, el proceso de migración hacia COBIT 5 puede revestir cierta complejidad para aquellas organizaciones que han implementado oportunamente COBIT 4. En este sentido, es importante destacar que aquellas organizaciones que ya habían alcanzado bajo COBIT 4 un nivel de madurez mínimo de 2 (según el criterio de la ISO 15504), encontrarán el upgrade relativamente fácil, mientras que para el resto puede significar un verdadero desafío que justificará evaluar la conveniencia de directamente comenzar con COBIT 5 "desde cero" como nuevo Framework.

Asimismo, cuando una organización ya ha hecho importantes inversiones en implementar COBIT 4.1 y se encuentra a mitad del proyecto, es recomendable que complete dicha iniciativa en lugar de mezclar las 2 versiones.

En conclusión, con la salida de COBIT 5 se abre una nueva etapa para el gobierno y el management de TI, que implicará que todos los involucrados, más allá del rol (CEO, CIO, CRO, CISO, CCO, Advisor, Auditor, etc), evolucionemos estratégicamente sincronizados con este nuevo estándar.

7. GLOSARIO

- **Actividad.-** En COBIT, la acción principal tomada para operar el proceso. Directrices para alcanzar prácticas de gestión para un gobierno y gestión de TI exitoso en la empresa. Actividades:

1. Describe un conjunto de tareas orientadas a la acción necesaria y suficiente para alcanzar una Práctica de Gobierno o una Práctica de Gestión.
2. Considerar las entradas y salidas del proceso.
3. Se basan en estándares y buenas prácticas aceptados de forma generalizada.
4. Apoyan el establecimiento de roles y responsabilidades claros.
5. No son prescriptivas y deben adaptarse y desarrollarse en procedimientos apropiados.

- **Alineamiento.-** Un estado en el que los elementos facilitadores del gobierno y la gestión de TI de la empresa contribuyen a las metas y las estrategias de la misma.

- **Aplicación TI.-** Funcionalidad electrónica que constituye una parte de los procesos de negocio que se realizan por o mediante la ayuda de TI.

- **Arquitectura de aplicación.-** Descripción de las capacidades de agrupación lógica de las capacidades de gestión de los objetos necesarios para procesar la información y contribuir a las metas corporativas.

- **Arquitectura Empresarial.-** Es una metodología de mejora continua a mediano plazo, que basada en una visión integral, permite mantener actualizada la estructura de información organizacional alineando procesos, datos, aplicaciones e infraestructura tecnológica en cuatro dimensiones: negocios, datos/información, aplicaciones y tecnología.

- **Atributo (de capacidad) de un proceso.-** ISO/IEC 15504: Una característica medible de una capacidad de proceso aplicable a cualquier proceso.

- **Autenticación.-** El acto de verificar la identidad de un usuario y sus derechos de acceso a información en los sistemas.

- **Buena práctica.-** Nota de alcance: Aseguramiento: la autenticación se diseña para prevenir inicios de sesión fraudulentos. También se puede referir a la verificación de exactitud de algún dato.

- **Calidad.-** Una actividad o proceso probado que se ha puesto en práctica con éxito por múltiples empresas y se ha demostrado que produce resultados fiables.

- **Capacidad de un proceso.-** Ser adecuado para un propósito (conseguir el valor deseado).

- **Cartera de inversión.-** ISO/IEC 15504: Una caracterización de la capacidad de un proceso para alcanzar las metas del negocio sean actuales o proyectadas.

- **Ciclo de vida.-** Es un concepto que remite a la aparición, desarrollo y finalización de la funcionalidad de un determinado elemento. Para la ingeniería y la informática, el ciclo de desarrollo es el periodo que comienza con la implementación de un estándar tecnológico y finaliza con el desarrollo de nuevas herramientas más eficientes.

- **COBIT.- COBIT 5:** Conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT); usado actualmente solo como un acrónimo en su quinta revisión. Un marco completo, internacionalmente aceptado, para el gobierno y la gestión de la información de la empresa y la tecnología de la información (TI) que soporta a los ejecutivos de la empresa y los gestores en la definición y consecución de las metas de negocio y las metas de TI relacionadas. COBIT describe cinco principios y siete facilitadores que dan soporte a las empresas en el desarrollo, implementación y mejora continua y supervisión de buenas prácticas relacionadas con el gobierno y la gestión de TI.

- **COBIT 4.1 y anteriores.** Conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT). Un marco completo, internacionalmente aceptado para TI que apoya el negocio y los ejecutivos y gestores de TI en la definición y consecución de las metas de negocio y las metas de TI relacionadas, a través un modelo extenso de gobierno, gestión, control y aseguramiento. COBIT describe los procesos de TI y objetivos de control asociados, directrices de

gestión (actividades, responsabilidades sobre ejecución, otras responsabilidades, métricas de rendimiento) y modelos de madurez. COBIT da soporte a los gestores de la empresa en el desarrollo, implementación, mejora continua y supervisión de buenas prácticas relacionadas con TI.

COBIT ha sido mapeado otros marcos y estándares para ilustrar el cumplimiento completo del ciclo de vida de gestión de TI y para dar soporte para su uso en empresas que adopten múltiples marcos y estándares relacionados con TI.

- **Código de ética.-** Un documento diseñado para influir en el comportamiento individual y en el organizativo de los empleados al definir los valores organizativos y las reglas que se aplican en ciertas situaciones. Se adopta para ayudar a aquellos que dentro de la organización son llamados a tomar decisiones de forma que puedan entender la diferencia entre decisiones 'correctas' e 'incorrectas' y aplicar esta comprensión a sus decisiones.

- **Competencia.-** La habilidad de realizar una tarea, acción o función específicas con éxito

- **Consecución de beneficios.-** Uno de los objetivos del gobierno. La obtención de nuevos beneficios para la empresa, el mantenimiento y extensión de cualquier tipo de beneficio existente y la eliminación de aquellas iniciativas o activos que no crean suficiente valor.

- **Control.-** Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal. También usada como sinónimo de salvaguarda o contramedida.

- **Creación de valor.-** El objetivo principal del gobierno de una empresa, conseguido cuando los tres objetivos subyacentes (consecución de beneficios, optimización de riesgo y optimización de recursos) están en equilibrio.

- **Entradas y Salidas.-** Los elementos/productos del trabajo en un proceso que se consideran necesarios para soportar la operación de un proceso. Son los que posibilitan la toma de decisiones clave, proveen un registro y traza de auditoría de las actividades

del proceso y posibilitan el seguimiento en caso de un incidente. Se definen al nivel de práctica de gestión clave y pueden incluir algunos productos de trabajo usados únicamente dentro del proceso y son, comúnmente, entradas esenciales para otros procesos. Las entradas y salidas de COBIT 5 son ilustrativas y no deben considerarse como una lista exhaustiva ya que se pueden definir flujos de información adicionales dependiendo del entorno particular de una empresa y de su marco de procesos.

- **Estructura organizativa.-** Un catalizador del gobierno y de la gestión. Incluye la empresa y sus estructuras, jerarquías y dependencias.

- **Facilitadores.-** Es la persona que ayuda a un grupo a entender los objetivos comunes y contribuye a crear un plan para alcanzarlos sin tomar partido, utilizando herramientas que permitan al grupo alcanzar un consenso en los desacuerdos preexistentes o que surjan en el transcurso del mismo. Hay muchos tipos de facilitadores, en función del tipo de ámbito en el que se desarrollen las actividades de los grupos.

- **Gestión.-** Incluye el uso juicioso de medios (recursos, personas procesos, prácticas, etc.) para conseguir un fin identificado. Es un medio o instrumento mediante el cual el grupo que gobierna consigue un resultado u objetivo. La gestión es responsable de la ejecución dentro de la dirección establecida por el grupo que gobierna. La gestión se refiere a las actividades operacionales de planificación, construcción, organización y control que alinean con la dirección que establece el grupo que gobierna y la información sobre dichas actividades.

- **Gestión de riesgos.-** Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa.

- **Gobierno.-** El marco, principios y políticas, estructuras, procesos y prácticas, información, habilidades, cultura, ética y comportamiento que establecen la dirección y verifican que cumplimiento y rendimiento de una empresa están alineados con el propósito general y los objetivos definidos.

- **Gobierno de TI empresarial.-** Un enfoque de gobierno que garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la

empresa y la consecución de las metas corporativas. También incluye el gobierno funcional de TI, por ejemplo, garantizando que las capacidades de TI son provistas de forma eficiente y efectiva.

- **Habilitadores.-** Dar a una cosa las condiciones necesarias para que desempeñe una función que no es la que tiene habitualmente. Dar capacidad legal a una persona para hacer una cosa.

- **Holística.-** Alude a la tendencia que permite entender los eventos desde el punto de vista de las múltiples interacciones que los caracterizan; corresponde a una actitud integradora como también a una teoría explicativa que orienta hacia una comprensión contextual de los procesos, de los protagonistas y de sus contextos.

- **Información.-** Un activo que, como cualquier otro activo importante de negocio, es esencial para el negocio de una empresa. Puede existir de muchas formas: impreso o escrito en papel, almacenado electrónicamente, transmitido por correo o de forma electrónica, mostrado en películas o hablado durante una conversación.

- **Intrínseca.-** que es propio o característico de la cosa que se expresa por sí misma y no depende de las circunstancias.

- **Mejora continua.-** Es una filosofía que intenta optimizar y aumentar la calidad de un producto, proceso o servicio. Es mayormente aplicada de forma directa en empresas de manufactura, debido en gran parte a la necesidad constante de minimizar costos de producción obteniendo la misma o mejor calidad del producto, porque como sabemos, los recursos económicos son limitados y en un mundo cada vez más competitivo a nivel de costos, es necesario para una empresa manufacturera tener algún sistema que le permita mejorar y optimizar continuamente.

- **Objetivo de TI.-** Una declaración describiendo el resultado deseado de las TI empresariales como soporte a los objetivos de la empresa. Un resultado puede ser un elemento, un cambio significativo de estado o una mejora de capacidades significativa.

- **Partes interesadas.-** Son las personas que importan en un Sistema. El análisis de poder de las partes interesadas es una herramienta que ayuda al entendimiento de cómo las

personas afectan a las políticas e instituciones, y de cómo las políticas e instituciones afectan a las personas.

- **Plan de negocio.-** El plan de negocios es el ingrediente clave para un negocio exitoso y con frecuencia es ignorado. Es una declaración formal de un conjunto de objetivos de una idea o iniciativa empresarial, que se constituye como una fase de proyección y evaluación. Se emplea internamente por la administración para la planificación de las tareas, y se evalúa la necesidad de recurrir a bancos o posibles inversores, para que aporten financiación al negocio.

- **Política.-** Es una rama de la moral que se ocupa de la actividad, en virtud de la cual una sociedad libre, compuesta por personas libres, resuelve los problemas que le plantea su convivencia colectiva. Es un quehacer ordenado al bien común.

- **Predecible.-** Es aquello que, por sus características, está en condiciones de ser predicho. La acción de predecir, por otra parte, consiste en anticipar algo que ocurrirá en el futuro. Por ejemplo: "Era predecible que las calles de la ciudad se iban a inundar: llovió copiosamente durante tres horas", "Aunque el triunfo del equipo local fue predecible, sorprendió la abultada diferencia en el marcador", "Los inversores sólo depositan su dinero en países cuyas economías resultan predecibles".

- **Principio.-** Es una ley o regla que se cumple o debe seguirse con cierto propósito, como consecuencia necesaria de algo o con el fin de lograr cierto propósito. Las leyes naturales son ejemplos de principios físicos, en matemáticas, algoritmia y otros campos también existen principios necesarios o que se cumplen sin más o que deberían cumplirse si se pretende tener cierto estado de hechos.

- **Proceso.-** Generalmente, una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de fuentes (incluyendo otros procesos), manipula esas entradas y genera salidas (por ejemplo, productos, servicios).

- **Responsabilidad de gobierno.-** El gobierno asegura que los objetivos de la empresa son alcanzados a través de la evaluación de las necesidades, condiciones y opciones de las partes interesadas; estableciendo las directrices a través de la priorización y toma de

decisiones; y la supervisión del rendimiento, cumplimiento y progreso respecto del planeamiento.

- **Riesgo.-** Es una medida de la magnitud de los daños frente a una situación peligrosa. El riesgo se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro. El término hace referencia a la proximidad o contingencia de un posible daño.

- **Rol.-** El concepto está vinculado a la función o papel que cumple alguien o algo. Por ejemplo: "El delantero le planteó al entrenador que no entiende cuál es su rol en el equipo", "El vicepresidente debería aceptar el rol que tiene en el Gobierno y no tomarse atribuciones que no le corresponden", "Mi primo cumple un rol muy importante dentro de una empresa multinacional".
- **Servicio TI.-** La provisión diaria a clientes de la infraestructura y de las aplicaciones TI y del soporte para su uso.

- **Sistema de control interno.-** Las políticas, estándares, planes y procedimientos y las estructuras organizativas diseñadas para proveer una garantía razonable de que los objetivos de la empresa van a conseguirse y de que los eventos no deseados serán evitados o detectados.

- **Soporte.-** Dentro de la informática, representa la acción de solucionar problemas de una aplicación.

- **Tecnología de la información.-** Se refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

8. BIBLIOGRAFÍA

Henri, F. (1879). *Las Bases de la Administración.* París: Dunod, OCLC.

ISACA. (2012). *COBIT 5 - Framework.* Rolling Meadows,USA: ISACA.

Montgomery, D., & Runger, G. (2002). *Probabilidad y estadística aplicadas a la Ingeniería.* México: Limusa Wiley.