Escuela Superior de Redes RED CEDIA

# GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

**VERSIÓN ORIGINAL:**
Edson Roberto Gaseta
Alexandre Cesar Motta
Jacomo Dimmit Boca Piccolini

**VERSIÓN ADAPTADA AL ECUADOR**
A partir de la versión de
ESR RENATA -Colombia

redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

# Gobierno de las Tecnologías de la Información


Versión original:
Edson Roberto Gaseta
Alexandre Cesar Motta
Jacomo Dimmit Boca Piccolini

Versión adaptada al Ecuador
A partir de la versión de
ESR RENATA - Colombia



redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Escuela Superior de Redes RED CEDIA

## Red Nacional de Tecnología Avanzada - RENATA

Director Ejecutivo
Lucas Giraldo Rios

Gerente de Comunicaciones
Camilo Jaimes Ocazionez

Gerente Administrativo y Financiero
Jader Alexis Castaño

Gerente de Tecnología e Información
Javier Enrique Lizarazo Rueda

## Escola Superior de Redes - RNP Brasil

Título original "Governança de TI"
Versión portuguesa RNP ©

Autores versión portuguesa
Edson Roberto Gaseta
Alexandre Cesar Motta
Jacomo Dimmit Boca Piccolini

## Universidad Nacional de Colombia Facultad de Ingeniería

Decano
José Ismael Peña Reyes

Vicedecano Académico
Oscar Germán Duarte

Director Instituto de Extensión e Investigación
Carlos Cortés

Coordinadora Académica
Jenny Marcela Sánchez-Torres

Autor versión adaptada y ampliada
Hernando Peña Villamil

Traductor
Oscar Edwin Piamba Tulcán

Profesionales de apoyo
Ana Carolina Gómez Parra

Diseño y diagramación
Andrés Camilo Gantiva Rueda

**ISBN:** (ebook)




## Comentarios y preguntas (versión ESR - Colombia)


Envíe sus comentarios y preguntas sobre esta publicación a:
RENATA - Escuela Superior de Redes – ESR Colombia.
E-mail: esrcolombia@renata.edu.co
www.renata.edu.co
Bogotá D.C. - Colombia

# Prólogo a la versión portuguesa

La Escuela Superior de Redes, ESR, es una unidad de la Rede Nacional de Ensino e Pesquisa, RNP, responsable por la difusión del conocimiento en Tecnologías de la Información y Comunicación, TIC. La ESR nace con la propuesta de ser formadora y diseminadora de las competencias en TIC para el cuerpo técnico – administrativo de las universidades federales, escuelas técnicas y unidades federales de investigación. Su misión fundamental es realizar la capacitación técnica del cuerpo funcional de las organizaciones usuarias de la RNP, para el ejercicio de las competencias aplicables al uso eficaz y eficiente de las TIC.

La ESR ofrece decenas de cursos en áreas temáticas como: administración y proyecto de redes, administración de sistemas, seguridad, medios de soporte a la colaboración digital de gobierno de TI.

La ESR también participa en diversos proyectos de interés público, como la elaboración y ejecución de planes de capacitación para la formación de multiplicadores para proyectos educativos como: formación en el uso de video conferencia para la Universidad Abierta de Brasil, UAB, formación de soporte técnico de laboratorios del Proinfo y creación de un conjunto de cartillas sobre redes inalámbricas para el programa Un Computador por Alumno, UCA.

# Prólogo a la versión en castellano

La Red Nacional Académica de Tecnología Avanzada, RENATA, tiene el gusto de presentarle a la comunidad académica, científica, tecnológica y empresarial del país, la Escuela Superior de Redes (ESR) RENATA Colombia, esfuerzo de colaboración con la Rede Nacional de Ensino y Pesquisa, RNP Brasil e Instituciones de Educación Superior en Colombia, como parte de nuestra estrategia STAR (Servicios de Tecnología Avanzada RENATA).

Nuestro objetivo es la formación de alto nivel en competencias TIC para todo el personal técnico, administrativo y académico del país, tanto de instituciones conectadas como no conectadas a RENATA de modo tal que se permita incrementar y mejorar la eficiencia en el uso de las tecnologías de la información y las comunicaciones para el trabajo colaborativo en Colombia.

Es también este el espacio para agradecerle a RNP y las universidades del país que han participado en la construcción de este programa académico, junto con los profesores y técnicos que pusieron todo de sí para llevar a buen puerto esta iniciativa.

RENATA los invita a todos a sacarle el mayor provecho a este proceso formativo y a beneficiarse de todo el potencial y los Servicios de Tecnología Avanzada RENATA, STAR.

RENATA es la red nacional de investigación y educación de Colombia que conecta, articula e integra a los actores del Sistema Nacional de Ciencia Tecnología e Innovación (SNCTI) entre sí y con el mundo, a través del suministro de servicios, herramientas e infraestructura tecnológica para contribuir al mejoramiento del nivel de productividad, efectividad y competitividad de la producción científica y académica del país.

# Metodología de la ESR

La filosofía pedagógica y la metodología que orientan los cursos de la ESR están basadas en el aprendizaje como construcción del conocimiento por medio de la resolución de problemas típicos de la realidad del profesional en formación. Los resultados obtenidos en los cursos de naturaleza teórico-práctica son optimizados, pues el instructor, ayudado por el material didáctico, actúa no solo como un expositor de conceptos e información, sino principalmente como orientador del alumno en la ejecución de las actividades contextualizadas en las situaciones de su cotidiano profesional.

El aprendizaje es entendido como una respuesta del alumno al desafío de situaciones-problemas semejantes a las encontradas en la práctica profesional, que son superadas por medio del análisis, síntesis, juzgamiento, pensamiento crítico y construcción de hipótesis para la solución del problema, en abordajes orientadas al desarrollo de competencias.

Así, el instructor tiene participación activa y dialogada, como orientador del alumno para las actividades en el laboratorio. Inclusive la presentación de la teoría al inicio de la sesión de aprendizaje no es considerada una simple exposición de conceptos e información. El instructor busca incentivar la participación de los alumnos continuamente.

Las sesiones de aprendizaje, en las que se realizan la presentación de contenidos y la realización de las actividades prácticas, tienen formato presencial y esencialmente práctico, utilizando técnicas de estudio dirigido individual, trabajo en equipo y prácticas orientadas al contexto de actuación del futuro especialista que se pretende formar.

Las sesiones de aprendizaje se desarrollan en tres etapas, con mayor dedicación a las actividades prácticas, conforme a la siguiente descripción:

**Primera etapa: presentación de la teoría y solución de dudas (de 60 a 90 minutos).**
El instructor presenta, de manera sintética, los conceptos teóricos correspondientes al tema de la sesión de aprendizaje, con ayuda de diapositivas en formato Power Point. El instructor formula interrogantes sobre el contenido de las diapositivas en lugar de solo presentarlas, animando al grupo a la participación y la reflexión. Eso evita que las presentaciones sean monótonas y que el alumno se coloque en actitud pasiva, lo que reduciría el aprendizaje.

**Segunda etapa: actividades prácticas de aprendizaje (de 120 a 150 minutos)**
Esta etapa es la esencia de los cursos de la ESR. La mayoría de las actividades de los cursos es asincrónica y realizada en grupos de dos alumnos, que siguen el ritmo de la guía de actividades propuesta en el libro de apoyo. El instructor y el monitor circulan entre los grupos para solucionar las dudas y ofrecer explicaciones complementarias.

**Tercera etapa: discusión de las actividades realizadas (30 minutos)**
El instructor comenta cada actividad, presentando una de las soluciones posibles, prefiriendo aquellas que generan mayor dificultad y polémica. Los alumnos son invitados a comentar las soluciones encontradas y el instructor retoma tópicos que hayan generado dudas, estimulando la participación de los alumnos. El instructor siempre estimula a los alumnos a encontrar soluciones alternativas a las sugeridas por él y por sus colegas, en caso que existan, y a comentarlas.

## Sobre el curso

El objetivo del curso es capacitar a los participantes para la implementación de buenas prácticas de gobierno de las TI con enfoque en CobiT 4.1 y el comparativo frente a los desarrollos de CobiT 5 También es su propósito contribuir para que el planeamiento, la gestión y el control de los procesos de las TI de las organizaciones estén alineados estratégicamente a los objetivos del negocio.

## A quién se dirige

Gestores técnicos de las TI que deseen implementar buenas prácticas de gobierno de las TI basadas en CobiT 4.1 y CobiT 5 Se recomienda que el participante tenga conocimientos sólidos de planeación y gestión estratégica de las TI, dominio de los fundamentos de gobierno de las TI y de la perspectiva de su utilización en su ambiente organizacional.

## Convenciones utilizadas en el libro

Las siguientes son convenciones tipográficas usadas en este libro:

*Itálico*

Indica los nombres de archivos y referencias bibliográficas relacionadas a lo largo del texto.

Indica una advertencia o precaución a tener en cuenta.

Indica preguntas que animen a la reflexión o presenta contenido para apoyar la comprensión del tema en cuestión.

Abc

Párrafo de texto con fondo azul
Indica la entrada de glosario o definición de términos que deben estar claros para la comprensión de la temática estudiada.

Abc

Párrafo de texto con fondo naranja
Destaca las actividades o ejercicios de nivelación

http://

Texto azul oscuro
Representa las direcciones electrónicas o URL.

# Sobre los autores de la versión portuguesa

**Edson Roberto Gaseta**, MBA en Gestión Empresarial de la ESAMC, Especialista en redes de computación del Instituto de computación de la UNICAMP, especialista en CobiT e ITIL, especialista en infraestructura ambiente Microsoft, especialista en seguridad en ambiente Microsoft ( Las Colinas – Texas – USA), Analista de Sistemas de la Fundación CPqD, desde hace 26 años, gerente de proyectos de tecnologías de información, profesor del curso de posgrado en seguridad de la información de laq Facultad IBTA, profesor académico que ha impartido clases en la Facultad de Hoyler, Universidad de SAO Marcos y Facultad Fleming.

**Alexandre Cesar Motta,** Magíster en Administración con énfasis en planeación organizacional y gestión de recursos humanos de la PUC- Rio. MBA en Gerencia de Proyectos de la FGV-RJ. Economista de la PUC-Rio con más de 10 años de experiencia profesional en cargos de coordinación y dirección de importantes Instituciones de Educación Superior. Profesor de cursos de pregrado y posgrado en las áreas de marketing, recursos humanos, planeación organizacional y gerencia de proyectos. Cuenta con experiencia como facilitador en programas de entrenamiento y desarrollo de competencias, habilidades técnicas y gerenciales en la implementación de proyectos de consultoría en gestión de recursos humanos, gerencia de proyectos y organización de empresas.

**Jacomo Dimmit Boca Piccolini,** Con estudios de postgrado en el Instituto de Computación y Economía de UNICAMP e Ingeniero de la Universidad Federal de São Carlos. Sirve como Coordinador Académico de las áreas de Seguridad y Gobierno de TI de la Escuela de Redes, ESR, de la Red Nacional de Investigación y Educación, RNP. Con más de 12 años de experiencia en seguridad, tiene certificaciones en materia de seguridad y gobernanza de TI. También es director de investigación de Dragon Research Group, Coordinador de Capacitación de FIRST.org, miembro del Consejo de ISACA Brasilia y profesor invitado en los cursos de postgrado en las disciplinas de la ciencia forense, sistemas de seguridad, manejo de incidentes, la creación y gestión CSIRT.

# Sobre los autores de la versión adaptada y ampliada

**Hernando Peña Villamil,** Magíster en Teleinformática de la Universidad Distrital Francisco José de Caldas e Ingeniero Electrónico. Directivo de Tecnología con más de 20 de años de experiencia, liderando proyectos de las TICs con certificaciones internacionales PMP, CobIT FC, ITIL FC e ISO 27001 IA. Vicepresidente Financiero del PMI-Colombia y Director de Membresía de ISACA-Colombia. Catedrático de posgrado en Gobierno de Tecnología de la Información y Gerencia de Proyectos de las Universidades Nacional, ICESI de Cali, Autónoma de Manizales, EAN, Militar y de La Salle. Miembro de los grupos de investigación TGI (Tendencias en Gestión e Innovación) y G3Pymes de la Universidad EAN. Desde el 2011 se desempeña como Consultor de Gobierno de las TI.

# Sobre la traducción para la versión adaptada y ampliada

**Oscar Edwin Piamba Tulcán,** Doctor en Ingeniería Mecánica de la Universidad Federal Fluminense, Magíster en Ingeniería Mecánica de la Universidad de los Andes con Especialización en Ciencias: Física de la misma Universidad e Ingeniero Mecánico de la Universidad Nacional de Colombia. Vinculado como profesor a la Facultad de Ingeniería de la Universidad Nacional de Colombia desde el año 2000, se desempeña como Director Nacional de Información Académica desde 2010. Participa como docente en los programas de Doctorado en Ingeniería Mecánica, en el Doctorado en Ciencia y Tecnología de Materiales y en los programas de maestría y pregrado en Ingeniería Mecánica y Mecatrónica.

# Tabla de contenido

Capítulo

01

# Alcance del gobierno de las Tecnologías de la Información

**Objetivos**

Garantizar la continuidad de los negocios a través del alineamiento estratégico, gestionar y monitorear la disponibilidad, el desempeño y la capacidad de los recursos de las Tecnologías de la Información, TI, y gestionar los riesgos.

**Conceptos**

Gobierno de las TI, gestión de recursos, de riesgos y de seguridad de la información, alineamiento estratégico y continuidad del negocio.

# Introducción

El gobierno de las TI de una organización pública o privada debe prestar atención a los siguientes propósitos:

- Alinear las TI a los negocios de la organización
- Gestionar los recursos de las TI
- Garantizar la seguridad de la información
- Gestionar los riesgos
- Monitorear los recursos de las TI

El gobierno de las TI es una práctica que las organizaciones públicas y privadas buscan implementar, con el objetivo de proveer más control de la estructura de las TI y buscando garantizar la sostenibilidad y la competitividad, por medio del alineamiento entre los objetivos de las TI y los objetivos estratégicos de la organización. Se trata del ampliamente conocido alineamiento de las TI con el negocio.

El gran desafío de las organizaciones públicas y privadas es gestionar adecuadamente la estructura de las TI y direccionar las inversiones en las TI de forma adecuada, buscando alcanzar los mejores resultados de los servicios prestados por las TI, por medio de un adecuado gobierno de las TI.

Para que el gobierno de las TI atienda plenamente la organización es necesario:

- Realizar el alineamiento estratégico para garantizar la continuidad de los negocios;
- Gestionar adecuadamente los recursos de las TI;
- Garantizar que los recursos de las TI y la información generada por ellos esté soportadas por una adecuada gestión de seguridad de la información;
- Gestionar los riesgos de las TI asociados a los negocios;

» Monitorear constantemente la disponibilidad, el desempeño y la capacidad de los recursos de las TI asociados a los principales negocios de la organización.

Esta sesión tiene como objetivo mostrar los principales fundamentos de gobierno de las TI.

## 1.1 Tendencias del desarrollo del módulo "gobierno de TI con CobiT"

El gobierno de TI se apoya principalmente en el marco de referencia CobiT, *Control Objectives for Information and Related Technology* (objetivos de control para la información y la tecnología relacionada) de ISACA cuya versión anterior (4.1) de mayo de 2007 se estructura en cuatro dominios (Planificar, Adquirir e Implementar, Entregar y dar Soporte, y Monitorear y Evaluar) y 34 procesos.

La última versión de CobiT (5.0) de mayo del 2012 lo amplía hacia una visión empresarial haciendo claramente la separación entre gobierno de TI y gestión de TI e integrando a otros dos marcos denominados VAL IT (para gestión de las inversiones de TI) y a RISK IT (para gestión del riesgo de TI) en un marco de referencia que se describe en 37 procesos.

Aunque CobiT 5.0 en la capa de gestión de TI discrimina 32 procesos, varios de ellos se apoyan en *Information Technology Infrastructure Library, ITIL*, para su implementación.

La *International Standarization for Organizations*, ISO, publicó en el año 2008 la ISO 38500 que pretende proporcionar un marco de principios para que los Directores de TI lo utilicen para evaluar, dirigir y monitorear el uso de tecnologías de la información en sus organizaciones. Esta norma recoge en gran parte el esquema del marco de referencia CobiT 4.1.

Recientemente, ha tomado auge la arquitectura empresarial como un marco de referencia más amplio cubriendo aspectos de gobierno de TI y de igual manera elementos de los procesos de negocio, de las aplicaciones, de la información en sí y de la infraestructura tecnológica. Este marco, aunque novedoso, también se apoya en CobiT para la implementación del dominio de gobierno de TI.

## 1.2 Alineamiento estratégico y continuidad del negocio

El gobierno de las TI integra e institucionaliza buenas prácticas para garantizar que el área de las TI de la organización soporte los objetivos del negocio.

- Permite a la organización obtener ventajas con la gestión adecuada de su sistema de información
- Hace explícitos los objetivos de las TI
- Garantiza que la TI soportará todas las actividades del negocio

Es importante que la organización defina claramente sus procesos y objetivos de negocio para que la TI soporte adecuadamente las actividades de la organización. La armonía entre los procesos de negocio y los procesos de las TI garantizan el alineamiento entre el gobierno corporativo y el gobierno de las TI.

La necesidad de un buen gobierno de las TI, con los controles adecuados, garantiza que cualquier cambio en los procesos de negocios sea fácilmente evaluado, para que las decisiones necesarias se puedan tomar. Es común que el área de tecnología no tenga ningún control de gobierno, implicando la falta de preparación para una respuesta adecuada a las nuevas demandas. El gobierno de las TI es parte integral del gobierno corporativo de toda organización. De acuerdo con el *IT Governance Institute*, ITGI, (www.itgi.org).

"El gobierno de las TI es responsabilidad de los ejecutivos y de la alta dirección, involucrando aspectos de liderazgo, estructura organizacional y procesos que garanticen que el área de las TI de la organización soporte y mejore los objetivos y las estrategias de la organización".

ITGI fue creado en 1998 debido al creciente avance de la TI. Realiza investigaciones sobre prácticas globales y percepciones de gobierno de las TI para la comunidad empresarial. Busca ayudar a los líderes empresariales a entender cómo el gobierno de las TI puede apoyar las organizaciones en el alcance sus objetivos.

El gobierno de las TI integra e institucionaliza buenas prácticas para garantizar que el área de las TI de la organización soporte los objetivos de los negocios. Además de eso, el gobierno de las TI permite a la organización obtener todas las ventajas de su sistema de información, maximizando los beneficios, capitalizando las oportunidades y ganando en poder competitivo

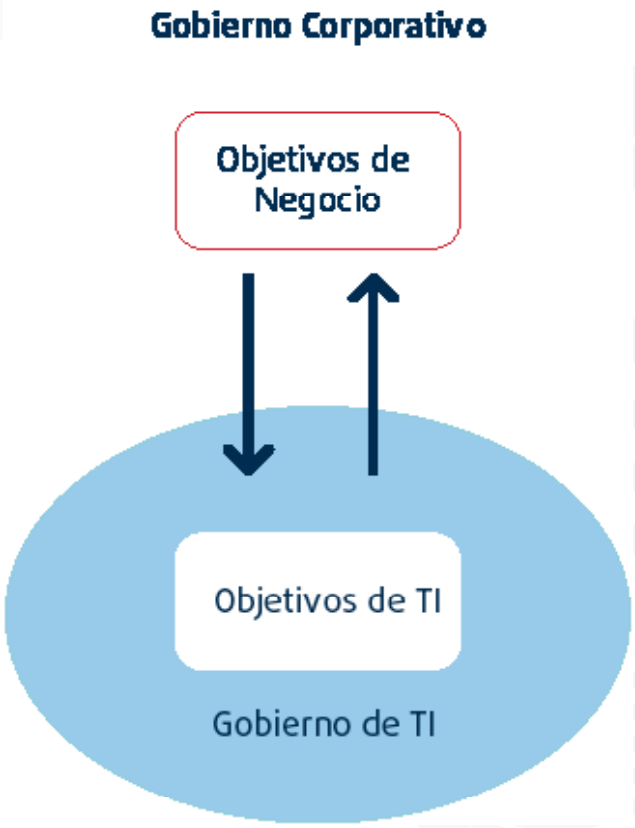



**Figura 1.** Alineamiento entre el gobierno corporativo y el gobierno de las TI

Las organizaciones documentan sus objetivos por medio de documentos y procesos de negocios. A su vez, el gobierno de las TI debe hacer explícito los objetivos de las TI y garantizar que ellos soportarán todas las actividades del negocio. El alineamiento estratégico trabaja para garantizar la relación entre los planes de negocio y los de las TI, definiendo, manteniendo y validando la propuesta de valor de las TI, alineando las operaciones de las TI con las operaciones de la organización.

Para garantizar un alineamiento satisfactorio es necesario que las organizaciones tengan mapeados sus procesos de negocio. Un error común en las organizaciones es que muchas veces ellas no tienen definido claramente sus procesos de negocio, ocasionando un descontrol en la propia organización y desviando las acciones de expansión y mejora continua. Por lo tanto, es importante que la organización defina claramente sus procesos y objetivos de negocio para que la TI soporte adecuadamente sus actividades.

## 1.3 Procesos de CobiT 4.1 asociados al alineamiento estratégico y a la continuidad de los negocios

Como premisa es importante que el área de las TI desarrolle e implemente una Planeación Estratégica de Tecnología de la Información, PETI, implementando el proceso de CobiT 4.1:

- PO1:Definir una PETI y sus objetivos de control
  - Descrito en el modelo CobiT 4.1

También es importante que los procesos de negocio tengan una garantía de continuidad en caso de algún problema en la TI. Por tal razón es importante implementar el proceso de CobiT 4.1:

- DS4. Asegurar la continuidad de los servicios
  - Descrito en el modelo de CobiT 4.1

### 1.3.1 PO1: Definir una Planificación Estratégica de las TI

La PETI es necesaria para gestionar todos los recursos de las TI en alineamiento con las prioridades y estrategias de negocio. La función de las TI y las partes interesadas del negocio son responsables de garantizar la optimización del valor a ser obtenido del portafolio de proyectos y servicios. La planificación estratégica debe mejorar el entendimiento de las partes interesadas en relación con las oportunidades y limitaciones de las TI, evaluando el desempeño actual y definiendo el nivel de inversión requerido. La estrategia y las prioridades de negocios deben ser reflejadas en los portafolios y ejecutadas por medio de planes tác-

ticos de las TI que establezcan objetivos concisos, tareas y planes bien definidos y aceptados por ambos, el negocio y TI.

### 1.3.2 DS4: Asegurar la continuidad de los servicios

Proveer la continuidad de los servicios de las TI requiere el desarrollo, mantenimiento y prueba de un plan de continuidad de las TI, almacenamiento de copias de seguridad *(backup)* en instalaciones remotas (*offsite*) y la realización de entrenamientos periódicos del plan de continuidad. Un proceso eficaz de continuidad de servicios minimiza la probabilidad y el impacto de una interrupción de un servicio clave de las TI en las funciones y procesos críticos de negocio. Implementar e instrumentalizar los procesos de gobierno de las TI es de suma importancia para todas las organizaciones que se comprometen con eficiencia y resultados.

**Ejercicio de refuerzo - alineamiento estratégico y continuidad de los negocios**

» ¿Cómo debe ser realizado el alineamiento entre TI y el negocio?

## 1.4 Gestión de recursos

Los recursos de las TI identificados en CobiT pueden ser definidos así:

» Los aplicativos son los sistemas automatizados para usuarios y los procedimientos manuales que procesan la información.
» Información se refiere a los datos en todas sus formas, la entrada, el procesamiento y la salida brindada por el sistema de información, en cualquier formato para ser utilizado en los negocios.
» La infraestructura se refiere a la tecnología y a los recursos que hacen posible el procesamiento de los aplicativos:
  - *Hardware*, sistemas operacionales, sistemas de gestión de bases de datos, redes y multimedia, además de los ambientes que abrigan y dan soporte a ellos.
» Recursos humanos, propios o externalizados, para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas de información y servicios.

La gestión de recursos en el gobierno de las TI se refiere a garantizar el mejor uso posible de las inversiones y la gestión adecuada de los recursos críticos de las TI, como: aplicativos, informaciones, infraestructura y personas. Las cuestiones relevantes se refieren a la optimización del conocimiento y de la infraestructura de las TI.

EL área de las TI entrega los servicios de acuerdo con los objetivos del negocio y de las TI por medio de un conjunto claramente definido de procesos, que emplean la experiencia de las personas y la infraestructura tecnológica para procesar aplicativos de negocios de manera automatizada, mejorando la información del negocio. Esos recursos, utilizados en conjunto con los procesos constituyen la arquitectura de las TI de la organización.

Para atender los requisitos del negocio, la organización necesita invertir los recursos de las TI necesarios para la creación de una adecuada capacidad técnica (ejemplo: un sistema de gestión), que atienda una necesidad de negocios (ejemplo: aumentar el recaudo), generando un retorno esperado (ejemplo: aplicar adecuadamente los valores recaudados).

La siguiente figura, extraída de CobiT 4.1, muestra los recursos de las TI.

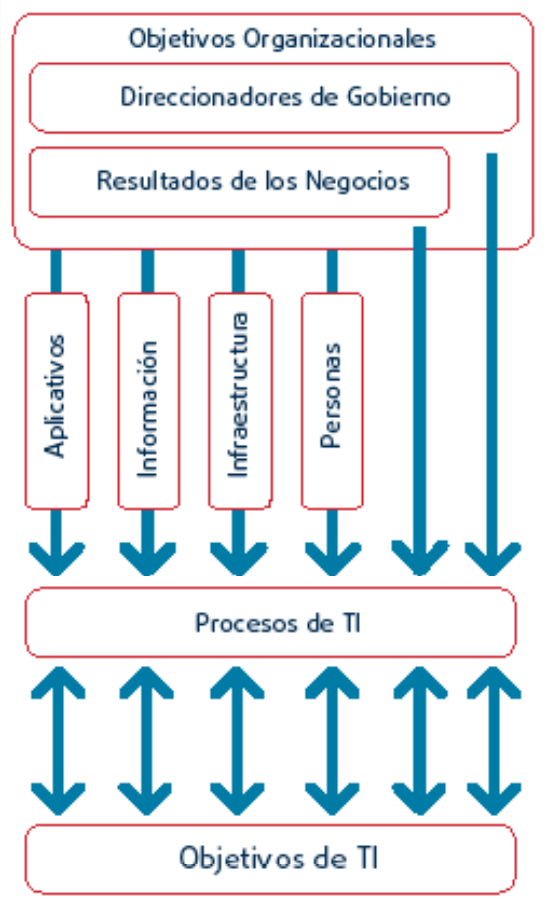



**Figura 2.** Recursos de las TI

Una gestión adecuada de los recursos de las TI tiene como objetivo ampliar el conocimiento y perfeccionar la infraestructura de tecnología de la organización, ya sea por medio de las inversiones realizadas, por la utilización de las TI y por la propia asignación de esos recursos (en personal, aplicativos, tecnología, estructura de soporte y datos).

Así, para que la TI pueda apoyar a la organización a alcanzar sus objetivos de negocios, ella necesita contar con una buena infraestructura tecnológica, así como personal técnico capacitado y entrenado, y presupuesto adecuado que garantice el mantenimiento de los servicios de las TI.

En toda organización, pública o privada, es cada vez más importante garantizar la correcta aplicación de los recursos de las TI, ya sea por la necesidad de las organizaciones por alcanzar sus objetivos institucionales y de negocios, o porque los gastos en TI, frecuentemente, no están asociados a una planificación adecuada. En este contexto, para garantizar la adecuada gestión de los recursos es preciso trabajar con las siguientes dimensiones:

» **Información**: es lo que mueve la organización, y debe estar disponible siempre que sea necesario. Para la generación de la información es necesario que los datos sean confiables, siendo importante que las organizaciones:

- Elaboren un Plan de Continuidad de Negocios, PCN, para minimizar los riesgos relacionados a la gestión de la información, garantizando su disponibilidad;
- Garanticen que la información sea clasificada con relación a su grado: confidencial, reservada o pública;
- Establezcan un área específica para tratar la seguridad de la información, garantizando que las acciones relacionadas a la seguridad de la información sean aplicadas de forma organizada y alineada con los negocios;
- Definan e implementen una Política de Seguridad de la Información, PSI, para reconocer la importancia de la seguridad de la información para el negocio.

**PCN**: conjunto de planes de acción aplicados para garantizar que los servicios esenciales de la organización soportados por TI vuelvan al funcionamiento normal después de una situación catastrófica.

» **Aplicativos:** el desarrollo de sistemas de información es una de las principales actividades de las áreas de las TI de las organizaciones, y la calidad de sus desarrollos impacta directamente en la calidad de los servicios que soportan las actividades del negocio. En este contexto, es importante que las organizaciones adopten una metodología de desarrollo de sistemas robustos, con pocas fallas, realizando pruebas, con homologación y documentación adecuadas. Otro factor importante es desarrollar sistemas basados en criterios de seguridad de la información, tal como lo establece la norma ISO/IEC 27034.

» **Infraestructura:** la infraestructura de las TI debe garantizar que todos los cambios necesarios en los activos sean gestionados

por medio de un proceso, con las clasificaciones adecuadas de cada cambio (normal, de emergencia, urgente) y su integración con las fallas que ocurren en la infraestructura (incidentes) y el plan de capacidad.

» En este sentido es necesario que se establezca:

- Un proceso de gestión de cambios para minimizar los riesgos de inestabilidad y fallas técnicas, operacionales y de seguridad, en el tratamiento de la información en el ambiente de las TI, cuando ocurran cambios en la infraestructura;
- Un proceso específico para el tratamiento de incidentes (fallas), minimizando el riesgo de que eventuales incidentes – involucrando la disponibilidad, la integridad la confidencialidad de la información – tengan tratamiento inadecuado e inconsistente;
- Un proceso de gestión de capacidad y desempeño del ambiente de las TI, minimizando la exposición al riesgo de indisponibilidad de información y discontinuidad significativa en la prestación de servicio por falta de capacidad o desempeño para el procesamiento de la información.

» **Personal:** la importancia estratégica de la TI para la organización debe garantizar que el grupo de personal técnico que desarrolla las actividades de las TI posea calificación adecuada. Las organizaciones deben proveer una gestión de recursos humanos de las TI de forma que todos los profesionales desempeñen adecuadamente sus funciones, con programas de entrenamiento para garantizar la evolución técnica e intelectual. Otro factor importante es la creación de un proceso de gestión de base de conocimiento, para que los asuntos referentes a la tecnología de información sean registrados y consultados por todos los profesionales de la organización. Es importante que los profesionales del área de las TI ejecuten sus funciones de forma orientada a procesos, garantizando que la información técnica y de negocios no sea dependiente de una persona específica.

Además de la calificación técnica, la gestión de recurso humano debe garantizar que todos los profesionales de las TI tengan conocimiento de los procesos de negocio de la organización, de forma que sea conocida la influencia de una determinada falla de las TI en los procesos de negocio. El profesional de las TI debe conocer el negocio de los riesgos asociados a las TI.

### Ejercicio de refuerzo - gerencia de recursos

» ¿Por qué es necesaria una adecuada gestión de recursos de las TI?

## 1.5 Gestión de la seguridad de la información

Garantizar la confidencialidad, la integridad y la disponibilidad de los activos de la organización, de los datos y servicios de las TI.

» **Confidencialidad:** proteger información confidencial contra revelaciones no autorizadas, es decir, los datos sólo pueden ser consultados por personas autorizadas.
» **Integridad:** mantener la información y sistemas computarizados, entre otros activos, exactos y completos, garantizando que las modificaciones en los datos y activos de las TI sean realizadas por personas autorizadas.
» **Disponibilidad:** garantizar que la información y servicios vitales estén disponibles cuando sean requeridos.

En general, le corresponde a la gestión de seguridad de la información:

» Desarrollar e implementar políticas, estándares y guías generales para las personas, para la seguridad de los datos, recuperación de desastres y continuidad del negocio.
» Supervisar el continuo monitoreo y protección de la infraestructura y de los recursos de las TI.
» Evaluar posibles brechas de seguridad y recomendar las correcciones necesarias.
» Negociar y gestionar los acuerdos de niveles de servicio con proveedores externos de servicios de protección u hospedaje de datos.

La información es el bien más importante para el negocio de una organización. Para garantizar que la información esté acorde a los procesos de negocios, es necesario que la gestión de seguridad de la información esté alineada con la seguridad del negocio, asegurando que la seguridad de la información sea efectivamente gestionada en todos los servicios y actividades del área de las TI.

La Gestión de la Seguridad de la Información, GSI, hace parte de un enfoque organizacional relacionado a la gestión de la seguridad, que es más amplio e incluye aspectos como:

- Tratamiento de documentos confidenciales;
- Acceso a las instalaciones (edificios, salones, etc.)
- Llamadas telefónicas.

Las necesidades de seguridad y la importancia relativa de cada elemento dependen del negocio de cada organización. La GSI es formada por una estructura básica de políticas, procesos, estándares, guías y herramientas que garantizan que la organización puede realizar de forma amplia la seguridad de la información. Esta estructura básica provee la base para el desarrollo de un programa de seguridad de la información, con costo efectivo y soporte a los procesos y objetivos del negocio.

Toda la información requerida por la gestión de seguridad de la información deben estar en un banco de datos, con todos los controles de seguridad, riesgos, vulnerabilidades identificadas e informes para soportar y mantener una política de seguridad de la información.

## Identificación de las necesidades de seguridad

Las necesidades de seguridad de la información son obtenidas de las siguientes fuentes:

### Evaluación de riesgos

Todo proceso de protección de activos debe estar precedido por la evaluación de riesgos inherentes a cada uno de esos activos, para que se pueda optimizar la aplicación de recursos de protección en el área que ofrezcan mayor riesgo para los negocios. La evaluación de riesgos está definida como proceso de identificación de riesgos de seguridad, determinación de su magnitud e impacto en los negocios. Sus estrategias pueden variar de acuerdo con los objetivos de la organización.

### Necesidades legales, contractuales y estatutarias

La segunda fuente que puede influir en la necesidad de proteger la información se refiere a aspectos legales, estatutarios y contractuales que una organización, sus socios de negocios, contratantes y proveedores deben atender, destacándose entre otros:

- El deber de diligencia de los administradores de la organización en la adopción de medidas necesarias para la consecución de los objetivos de los negocios, evitando la ocurrencia de actos que impliquen prejuicios a la organización;
- El respeto a la legislación de protección de los derechos del consumidor, garantizando la seguridad en la prestación de servicios y en la comercialización de los bienes;
- El respeto a la legislación de protección de los derechos intelectuales, género que incluye los derechos de autor, la protección a la propiedad intelectual de programas de computador y la preservación de la propiedad industrial;
- El cumplimiento de los derechos constitucionales relativos a la confidencialidad de los datos e información;
- Las determinaciones de las normas de las instituciones públicas y privadas.

Por lo tanto, es importante que la implementación o ausencia de controles de seguridad en cada uno de los sistemas de información sea auditada a partir de premisas que permitan a la organización determinar el grado de exposición a los riesgos y sus consecuencias jurídicas.

**Principios, objetivos y necesidades organizacionales**

La tercera fuente que puede influenciar las necesidades de seguridad de información se refiere a los principios, objetivos y necesidades organizacionales de procesamiento de información que soporten sus operaciones de negocios, sobre los cuales la organización decidió aplicar sus sistemas de información. Es importante que la implementación o ausencia de controles de seguridad en cada uno de los sistemas de la organización no impida la eficiencia de las operaciones de negocios.

## Ejercicio de refuerzo - gestión de seguridad de la información

- ¿Cuáles son las principales necesidades de la seguridad de la información?

## 1.6 Gestión del riesgo

El riesgo puede ser definido como la probabilidad de que una amenaza explote vulnerabilidades para causar pérdidas o daños a un activo o grupo de activos de la organización.

Durante el proceso de evaluación de riesgos, es importante entender los daños que los riesgos de seguridad pueden causar a los negocios de la organización. Una posible forma sería responder las siguientes preguntas:

- ¿Cuáles son las partes más importantes de los negocios de la organización (productos, servicios, actividades, etc.)?
- ¿Cómo es soportado el negocio por el uso de tecnología y qué tan esencial es este soporte?
- ¿Cuánto dependen las decisiones esenciales de la actualización, precisión, disponibilidad e integridad de la información?
- ¿Cuál información confidencial necesita ser protegida?
- ¿Cuáles son las implicaciones de los incidentes de seguridad, relacionados a la información, para los negocios de la organización?

La organización necesita analizar cuáles son los controles necesarios para asegurar que los riesgos sean mitigados. Por lo tanto, es importante implementar el proceso de CobiT 4.1:

- PO9. Evaluar y gestionar los riesgos de las TI
  - Descrito en el modelo de CobiT 4.1

De esta forma, los riesgos son determinados por la combinación de las amenazas, vulnerabilidades y valores de los activos. Los valores son medidos con base en el impacto de estos activos en los negocios de la organización, donde el impacto se traduce como los resultados de un incidente inesperado. Como ejemplos de daños podemos citar, entre otros, los siguientes:

- Datos robados o afectados;
- Destrucción de datos;
- Pérdida de la integridad de los datos;
- Pérdida de la integridad de los sistemas o de la red;
- Pérdida de la capacidad de acceso a los sistemas o a la red;
- Pérdida de reputación;
- Implicaciones financieras:
  - Impacto sobre informes financieros;
  - Ventaja competitiva;
  - Exposición al fraude.

- Implicaciones indirectas a la organización:
  - Interés de los funcionarios en descubrir determinada información;
  - Efecto de hacer públicas determinada información por parte de los funcionarios.
- Requisitos por confidencialidad y privacidad:
  - Implicaciones sobre privacidad;
  - Penalidad legal por la divulgación de información.

Es necesario que los procesos de identificación y evaluación del riesgo tengan en consideración las siguientes recomendaciones:

- Adopción de herramientas automatizadas para identificar las vulnerabilidades existentes en la red, sistemas operacionales y bancos de datos; pruebas internas y externas de intrusión;
- Ejecución de revisiones periódicas de seguridad por un auditor o un especialista de seguridad, siguiendo el principio de segregación de función, es decir, no ser el administrador de los sistemas en prueba;
- Elaboración de un plan de acción periódico para el estudio de la viabilidad de corrección de vulnerabilidades, corrección efectiva de vulnerabilidades y creación de controles que minimicen los riesgos provenientes de la imposibilidad de corrección de vulnerabilidades;
- Uso de técnicas y metodologías para medir los riesgos inherentes a los activos de la organización;
- Uso de laboratorios para simulaciones.

**P09- Evaluar y gestionar los riesgos de las TI**

Crear y mantener una estructura de gestión de riesgos. Esta estructura documenta un nivel común y acordado de riesgos de las TI, estrategias de mitigación y riesgos residuales. Cualquier posible impacto en los objetivos de la organización causado por un evento no planeado debe ser identificado, analizado y evaluado. Estrategias de mitigación de riesgos deben ser adoptadas para minimizar el riesgo residual a niveles aceptables. El resultado de la evaluación debe ser entendido por las partes interesadas y se debe expresar en términos financieros para permitir que las partes interesadas reduzcan el riesgo a niveles de tolerancia aceptables.

### Ejercicio de refuerzo - gestión de la seguridad de la información

» ¿Cómo define usted el riesgo? ¿Qué importancia le atribuye usted a la gestión del riesgo?

## 1.7 Desempeño, capacidad y monitoreo de las TI

El gobierno de las TI debe mantener un plan de gestión, desempeño y capacidad alineado al crecimiento de los negocios.

En este contexto, asegura el desempeño y capacidad suficientes para soportar los servicios planeados por el negocio de la organización. Por tanto, es importante implementar los procesos de CobiT 4.1:

» DS3 – Gestión de desempeño y la capacidad
  • Descrito en el modelo de CobiT 4.1

» ME1 – Monitorear y evaluar el desempeño de las TI
  • Descrito en el modelo de CobiT 4.1

El desempeño y la capacidad del ambiente de las TI están directamente relacionados con los procesos y objetivos del negocio. Dentro del gobierno de las TI es importante que existan procesos adecuados para monitorear el uso de recursos de infraestructura, almacenamiento de datos e información de desempeño y capacidad del ambiente tecnológico, en forma tal que se puedan identificar tendencias de desempeño y la variación entre la utilización planeada y real de la capacidad.

El monitoreo de todos los procesos de negocios debe ser responsabilidad del área de las TI, donde las siguientes acciones deben ser seguidas:

» Gestionar el desempeño y la capacidad de la infraestructura de las TI, para brindar un nivel de recursos técnicos de las TI que permita al negocio atender sus objetivos;
» Definir y mantener procedimientos, estándares y criterios de calidad aplicables a la gestión de desempeño y capacidad;
» Realizar reuniones regulares con proveedores de tecnología, con el fin de mejorar conocimientos relacionados a la capacidad y desempeño de los elementos de la infraestructura de las TI;
» Realizar acciones de prospección de herramientas para la gestión de la capacidad y el desempeño;

» Dimensionar los componentes de infraestructura para fortalecer el proceso de contratación;
» Producir regularmente informes estandarizados, relacionados a la capacidad y desempeño de recursos estratégicos, publicando la información a través de los canales adecuados, con visión de infraestructura de las TI y de los negocios.

### 1.7.1 DS3: Gestionar el desempeño y la capacidad

La necesidad de gestionar el desempeño y la capacidad de los recursos de las TI requiere un proceso que realice análisis críticos periódicos del desempeño y la capacidad actual de los recursos de las TI. Ese proceso incluye una previsión de necesidades futuras con base en requisitos de carga de trabajo, almacenamiento y contingencia. Ese proceso asegura que los recursos de información que soportan los requisitos de negocio estén siempre disponibles.

### 1.7.2 ME1 – Monitorear y evaluar el desempeño de las TI

La gestión eficaz del desempeño de las TI exige un proceso de monitoreo. Este proceso incluye la definición de indicadores de desempeño relevantes e informes sistemáticos y oportunos de desempeño, además de una rápida acción en relación a las desviaciones encontradas. El monitoreo es necesario para asegurar que las actividades correctas están siendo desempeñadas en alineamiento con las políticas y directrices establecidas.

## Ejercicio de refuerzo - desempeño, capacidad y monitoreo de las TI

¿Cuáles son las principales acciones del área de las TI para el monitoreo de los procesos de negocios?

Capítulo

02

# Estructura de CobiT 4.1

**Objetivos**

Comprender la estructura de contenidos de CobiT 4.1 y su aplicación como modelo de referencia para el gobierno de las TI en las organizaciones.

**Conceptos**

CobiT 4.1, su resumen ejecutivo, objetivos de controles, estructura de dominios y procesos, y su relación con el gobierno de las TI.

# Introducción

**CobiT** significa *Control Objectives for Information and Related Technology* (objetivos de control para la información y la tecnología relacionada). Fue elaborado por el ITGI, creado en 1998 para contribuir en la mejora de los estándares de dirección y control de la tecnología de la información en las organizaciones.

Para implementar adecuadamente el gobierno de las TI es necesario utilizar un modelo capaz de direccionar la implantación.

CobiT 4.1 es una guía que ofrece a las organizaciones públicas y privadas buenas prácticas para alcanzar el gobierno de las TI, proporcionando:

- La implantación del gobierno de las TI
- El monitoreo del gobierno de las TI
- La auditoría del gobierno de las TI

CobiT 4.1 es una guía que posee una serie de componentes que pueden servir como un modelo de referencia para el gobierno de las TI, incluyendo un resumen ejecutivo, una estructura, control de objetivos, mapas de auditoría, herramientas para su implementación y principalmente, una guía con técnicas de gestión.

Esta sesión tiene como objetivo estudiar los componentes de CobiT 4.1 para la implementación del gobierno de las TI, y será basada en la información contenida en la publicación del ITGI, en la versión traducida en portugués.

## 2.1 Entendiendo el resumen ejecutivo de CobiT 4.1

CobiT 4.1 está enfocado en los procesos de las TI, y tiene la siguiente estructura:

- 4 dominios de conocimiento
- 34 procesos de las TI
- 210 objetivos de control

También es necesario que las organizaciones tengan mecanismos para garantizar que el área de las TI alcance sus objetivos y en consecuencia satisfaga las necesidades del negocio.

- Estos mecanismos son tratados en CobiT 4.1 como objetivos de control.

Un modelo de madurez de los procesos de CobiT 4.1 es fundamental para la implantación del gobierno de las TI, pues permite que las organizaciones tengan una visión clara de cómo los procesos de las TI están implantados, evaluando las deficiencias existentes y creando planes de acción para mejorar el desempeño de los procesos de las TI.

El resumen ejecutivo de CobiT 4.1 consiste en una visión que brinda una comprensión de los principales conceptos claves y de los principios utilizados. En el resumen también es presentada una visión de la estructura, que brinda una comprensión más detallada de estos conceptos y principios, al identificar los dominios y los procesos de CobiT 4.1.

De acuerdo con CobiT 4.1: "las organizaciones deben satisfacer los requisitos de calidad, confianza y seguridad de su información, así como también de todos sus bienes".

Para que eso sea posible, es necesario que las organizaciones públicas y privadas establezcan:

- Mecanismos capaces de entender la situación actual de la arquitectura de las TI, establecer los objetivos y los medios para alcanzarlos, por medio de optimización, mejora y ampliación de los recursos de las TI (aplicativos, información, infraestructura y personas).
- Controles adecuados para el gobierno de las TI, siendo que CobiT 4.1 brinda un conjunto de buenas prácticas, más enfocadas en controles y menos en la ejecución, auxiliando a las organizaciones en la optimización de las inversiones de las TI, garantizando una mejor entrega de los servicios y el monitoreo adecuado de la arquitectura de las TI.

» La adecuación de su área de las TI con el objetivo de entregar los servicios deseados por el negocio. CobiT 4.1 contribuye con los controles necesarios para alcanzar ese objetivo, haciendo posible:
  - Establecer una relación con los requisitos del negocio;
  - Organizar las actividades de las TI con un modelo de procesos que permitan realizar las actividades adecuadamente y con indicadores de medición de estas actividades;
  - Identificar los principales recursos de las TI a ser utilizados para sustentar el negocio;
  - Definir los principales objetivos de control que deben ser utilizados para monitorear el gobierno de las TI.

CobiT 4.1 brinda una visión orientada hacia la integración de los objetivos de negocios con los objetivos de las TI, buscando monitorear la relación entre los procesos de las TI y los procesos de negocios, con métricas y modelos de madurez.

Para que la organización tenga toda la información que necesita para mantener el negocio, es necesario gestionar adecuadamente todos los recursos de las TI que el negocio soporta, por medio de procesos de las TI, en este caso tratados por CobiT 4.1.

Las organizaciones siempre están buscando alternativas para controlar la TI, para que la información necesaria para mantener el negocio sea brindada. Otro asunto importante es garantizar la seguridad de la información y gestionar los riesgos a los que está sometida la TI, y de qué forma afectan los negocios de la organización.

Otro factor importante es que los dirigentes de las organizaciones necesitan información para garantizar la sustentabilidad del negocio, para propiciar una mejor toma de decisiones, de forma rápida y precisa, con la evaluación de los riesgos involucrados.

Así, CobiT 4.1 apoya el gobierno de las TI brindando una metodología para asegurar que:

» El área de las TI esté alineada con los negocios;
» El área de las TI habilite el negocio y maximice los beneficios;
» Los recursos de las TI sean usados responsablemente;
» Los riesgos de las TI sean gestionados apropiadamente.

La siguiente figura presenta las principales áreas de énfasis del gobierno de las TI definidas en CobiT 4.1

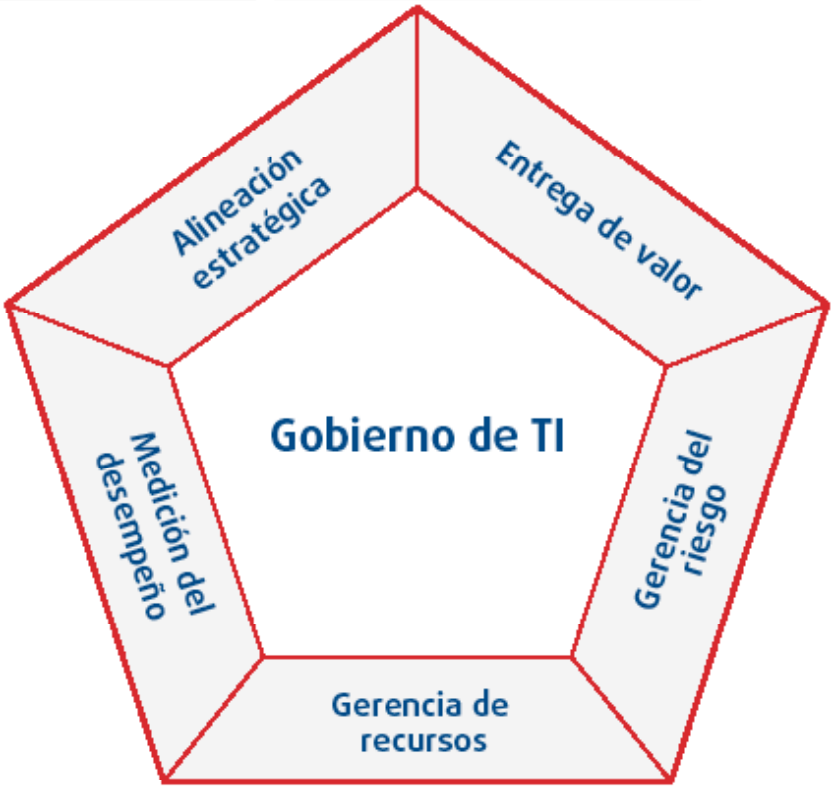



**Figura 3.** Áreas de énfasis del gobierno de las TI

Fuente: CobiT 4.1.

Áreas de énfasis del gobierno de las TI definidas en CobiT:

- Alineamiento estratégico
- Entrega de valor
- Gestión de recursos
- Gestión del riesgo
- Medición del rendimiento

Las áreas de énfasis del gobierno de las TI definidas por CobiT son:

- **Alineamiento estratégico:** se enfoca en garantizar la relación entre los planes de negocio y de las TI, definiendo, manteniendo y validando la propuesta de valor de las TI, alineando las operaciones de las TI con las operaciones de la organización.
- **Entrega de valor:** es la ejecución de la propuesta de valor de las TI a través del ciclo de entrega, garantizando que las TI entregan los beneficios previstos en la estrategia de la organización, concentrándose en optimizar costos y suministrando el valor esencial de las TI.
- **Gestión de recursos:** se refiere a la mejor utilización posible de las inversiones y a la gerencia apropiada de los recursos críticos de las TI: aplicaciones, información, infraestructura y personas. Los asuntos relevantes se refieren a la optimización del conocimiento y de la infraestructura.
- **Gestión del riesgo:** requiere un entendimiento claro del nivel de riesgo que está en capacidad de afrontar la organización y de los requerimientos de conformidad, trasparencia en la evaluación de los riesgos significativos e inserción de la gestión de riesgos en las actividades de la organización.
- **Medición del rendimiento:** acompaña y monitorea la implementación de la estrategia, finalización de los proyectos, uso de los recursos, desempeño y entrega de los servicios, usando, por ejemplo *Balanced Scorecard*, que traducen las estrategias en acciones para alcanzar los objetivos medidos a través de los procesos contables convencionales.

**Balanced Scorecard**
Definición de indicadores de rendimiento utilizados en la organización para el seguimiento de los objetivos estratégicos.

Esas áreas de énfasis en gobierno de las TI describen los aspectos principales relacionados al direccionamiento del área de las TI por las organizaciones. Las operaciones de las TI utilizan procesos para organizar y gestionar sus actividades continuas. CobiT 4.1 provee un modelo que representa todos los procesos encontrados normalmente en las funciones de las TI, brindando así un modelo de referencia común comprendido por toda el área de las TI y por el área de negocio.

## Contenido de CobiT

CobiT 4.1 está enfocado en alcanzar un nivel adecuado de control y gestión de las TI a nivel estratégico. Fue alineado y armonizado con otros patrones y buenas prácticas de las TI, con el fin de actuar como un integrador.

Los productos de CobiT 4.1 fueron organizados en tres niveles para dar soporte a:

- Ejecutivos de la alta dirección
- Gerentes de las TI y de negocios
- Profesionales de evaluación, control y seguridad

Los beneficios de la implementación de CobiT 4.1 como modelo de gobierno de las TI incluyen:

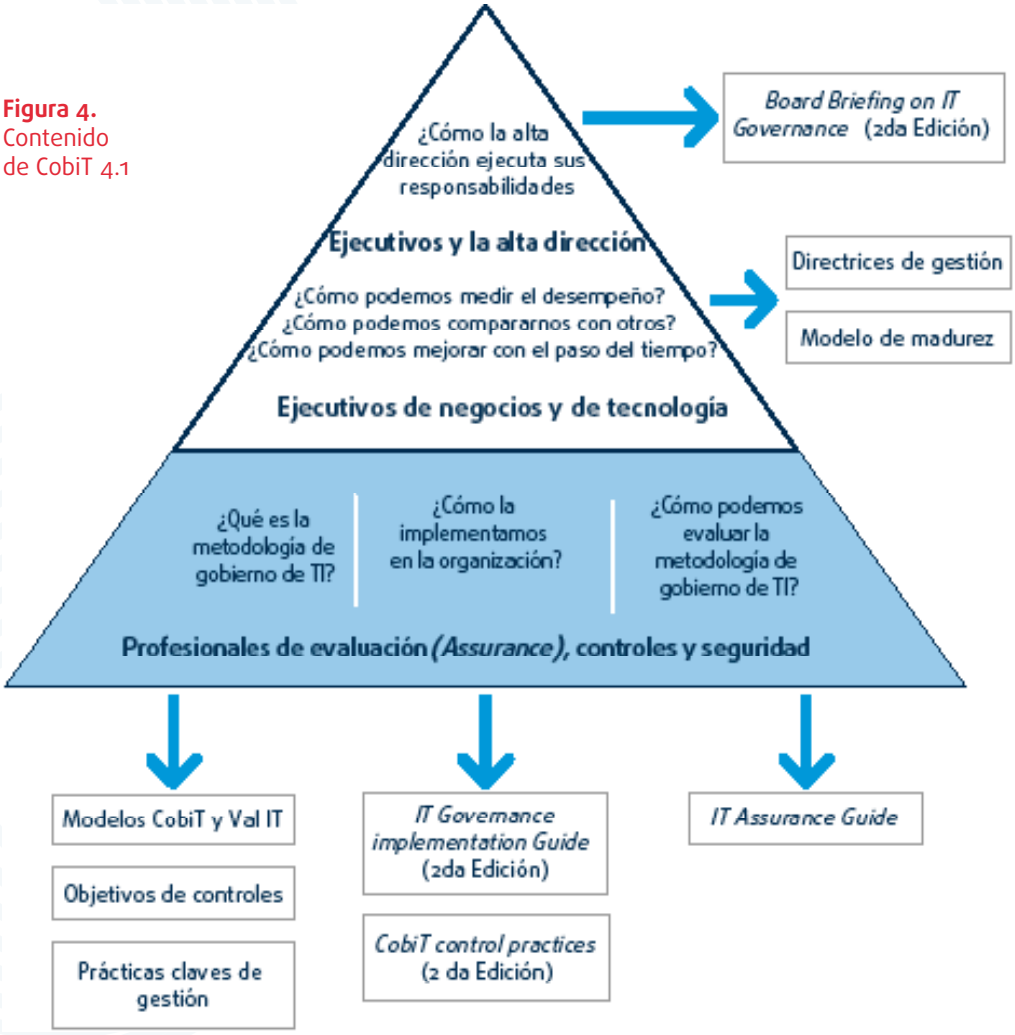
- Mejorar el alineamiento entre las TI y el enfoque del negocio
- Visión clara del papel de las TI para la organización
- División clara de las responsabilidades con base en la orientación para los procesos
- Aceptación general de las prácticas de las TI por terceros y órganos reguladores
- Entendimiento entre las partes interesadas en el negocio, con base en un lenguaje común
- Cumplimiento de los requisitos de los controles internos (COSO) para el ambiente de las TI

De forma resumida, los productos de CobiT 4.1 incluyen:

- *Board briefing on IT Governance* (2a edición): publicación que ayuda a los ejecutivos a entender por qué el gobierno de las TI es importante, cuáles son sus principales asuntos y el papel de ellos en su gestión;
- Directrices de gestión y modelos de madurez: ayudan a la designación de responsabilidades, evaluación de desempeño y *Benchmark*, e incluyen la solución de las deficiencias de capacidad;
- Métodos: organizar los objetivos de gobierno de las TI por dominios y procesos y los relaciona con los requisitos de negocios;
- Objetivos de control: proporcionan conjunto completo de requisitos de alto nivel a ser considerados por los ejecutivos para el control efectivo de cada proceso de las TI;
- *IT Governance Implementation Guide: using CobiT and Val IT TM* (2a. edición):provee un mapa general para implementar el gobierno de las TI usando los recursos de CobiT y del Val IT;

» CobiT ® Control *Practices*: *Guidance to Achieve Control Objectives for Successful IT Governance* (2a edición): explica por qué vale la pena implementar los controles y cómo implementarlos;
» *IT Assurance Guide: Using CobiT* ® - trae orientaciones sobre cómo CobiT puede ser usado para soportar las diferentes actividades de evaluación, además de sugerencias de pruebas para todos los procesos y objetivos de control de las TI.

**Figura 4.**
Contenido
de CobiT 4.1



Todos los componentes de CobiT 4.1 están interrelacionados, proporcionando el soporte para las necesidades de gobierno, gestión, control y evaluación, como se muestra en la Figura 5.

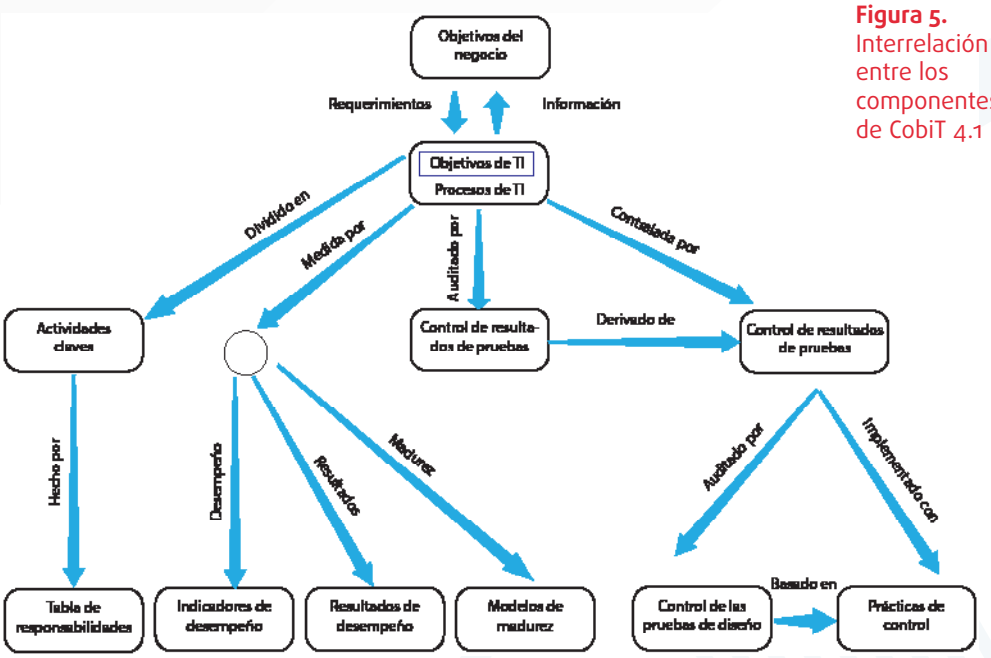



**Figura 5.** Interrelación entre los componentes de CobiT 4.1

## Ejercicio de refuerzo - conociendo el resumen de CobiT 4.1

El resumen ejecutivo de CobiT 4.1 brinda una visión general del gobierno de las TI. Identifique en el resumen ejecutivo cómo CobiT 4.1 trata la gestión de información.

## 2.2 Necesidad de un modelo para el gobierno de las TI

De acuerdo con la definición del ITGI, la misión de CobiT 4.1 es:

» "Investigar, desarrollar, publicar y promover un modelo de control para el gobierno de las TI actualizado e internacionalmente

reconocido para ser adoptado por las organizaciones y utilizado en el día a día por gerentes de negocios, profesionales de las TI y profesionales de evaluación."

Un modelo de control de gobierno de las TI define las razones por las cuales este gobierno es necesario, cuáles son las partes interesadas y lo que el modelo necesita alcanzar.

En este sentido, tres preguntas son aclaradas en CobiT 4.1:

- ¿Por qué implementar el gobierno de las TI?
- ¿Cuáles son las partes interesadas en el gobierno de las TI?
- ¿Que debe contener el gobierno de las TI?

### 2.2.1 ¿Por qué implementar el gobierno de las TI?

Las organizaciones no pueden alcanzar sus objetivos de negocio sin adoptar e implementar un modelo para gobierno y control de las TI que permita:

- Hacer una relación con los objetivos de negocio
- Hacer transparente el desempeño de los negocios comparado con sus objetivos
- Organizar las actividades de las TI de acuerdo con un modelo de procesos
- Identificar los recursos de las TI más importantes que necesitan de actualización
- Definir los objetivos de control gerencial necesarios para evaluar el desempeño de las TI

Son muchos los motivos para la implantación del gobierno de las TI, tales como:

- Desalineamiento entre las necesidades de negocio y la infraestructura de las TI de la organización;
- Decisiones de las TI tomadas de forma aislada;
- La seguridad de la información no existe o no es difundida adecuadamente en la organización;
- La contratación de servicios de terceros no atiende las necesidades del área de las TI.

De acuerdo con CobiT 4.1 las buenas prácticas de gobierno de las TI se tornarán importantes debido a los siguientes factores:

- Los ejecutivos de negocio y la alta dirección están demandando un mejor retorno de las inversiones en TI, esto quiere decir, que el área de las TI soporta las necesidades del área de negocios para aumentar el valor para las partes interesadas;
- Preocupación con el aumento de los gastos en TI;
- Necesidad de atender las exigencias regulatorias de controles de las TI en áreas como privacidad de información e informes financieros (por ejemplo la Ley Sarbanes-Oxley y Basilea II) y reglamentaciones para sectores específicos como las áreas de finanzas, farmacéutica y salud

Basilea III: De acuerdo con el documento de la Asociación Nacional de Instituciones Financieras, ANIF, En 2010, "el Comité de Basilea para la Supervisión Bancaria estableció nuevas normas para fortalecer el capital bancario, teniendo en cuenta el fracaso de Basilea II en contener adecuadamente la grave crisis financiera global de 2007-2009. Su objetivo central es robustecer la disponibilidad del capital, incrementando su cantidad por unidad de negocio y aumentando la calidad del mismo. Para las entidades con potencial riesgo sistémico se adoptaron "colchones de liquidez" adicionales, en función de su tamaño y su papel a nivel global".
http://anif.co/sites/default/files/uploads/Anif-Basilea1112_1.pdf

El Estado colombiano a través del Viceministerio de las Tecnologías de la Información viene diseñando el marco de referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información del Estado Colombiano, que tiene como propósito fortalecer la infraestructura y los procesos de Tecnologías de Información de las entidades públicas, así como organizar orientar la manera de gestionar la Tecnología de Información en todos los sectores, con el propósito de ofrecer mejores servicios a las personas y a las instituciones, maximizar los beneficios hacia el ciudadano y aumentar la eficiencia y transparencia de las entidades del Estado.

- Selección de proveedores de servicios y, la gestión y adquisición de servicios externos;
- Riesgos relacionados a las TI cada vez más complejos, como los de seguridad de la información;
- Iniciativas de gobierno de las TI que incluyen la adopción de metodologías de controles y buenas prácticas que ayuden a monitorear y mejorar las actividades críticas de las TI, para ampliar el valor del negocio y reducir los riesgos;

- Necesidad de optimizar los costos, siguiendo, siempre que sea posible, un enfoque estandarizado en vez de abordajes especialmente desarrolladas.
- Madurez creciente y consecuente aceptación de metodologías exitosas, tales como:
  - CobiT 4.1, ITIL, series ISO 27000 sobre estándares relacionados con la seguridad de la información;
  - ISO 9001: 2000: Requerimientos del Sistemas de Gestión de Calidad;
  - *Capability Maturity Model Integration*, CMMI
  - *Projects in Controlled Environments 2*, PRINCE2
  - *Guide to the Project Management Body of Knowledge,* PMBOK
- Necesidad de las organizaciones de evaluar cómo están en relación a los patrones generalmente aceptados y en comparación con sus socios y organizaciones similares (*benchmarking*).

### 2.2.2 ¿Cuáles son las partes interesadas en el gobierno de las TI?

En relación con la organización, existen varias partes interesadas (*stakeholders*) en la implementación del gobierno de las TI siendo estas internas o externas, con sus necesidades específicas.

*Stakeholders* que procuran generar valor a partir de las inversiones en TI:

- Aquellos que toman decisiones sobre las inversiones
- Aquellos que deciden sobre los requisitos
- Aquellos que usan los servicios de las TI

Partes interesadas dentro y fuera de la organización que proveen servicios de las TI:

- Aquellos que gestionan la organización y los procesos de las TI
- Aquellos que desarrollan las capacidades
- Aquellos que operan los servicios

Parten interesadas dentro y fuera de la organización que tienen responsabilidades sobre controles / riesgos:

- Aquellos con responsabilidad sobre la seguridad, confidencialidad y riesgos
- Aquellos que ejecutan funciones de cumplimiento
- Aquellos que requieren o proveen servicios de evaluación

### 2.2.3 ¿Que debe contener el gobierno de las TI?

Para cumplir los requisitos de una organización, una metodología de gobierno y control de las TI debe:

- Brindar un enfoque de negocios para permitir el alineamiento entre los objetivos de negocios y de las TI;
- Establecer un proceso de orientación para definir el alcance y la extensión de la cobertura, con una estructura definida permitiendo una fácil navegación en su contenido;
- Ser generalmente aceptada por ser consistente con las buenas prácticas y patrones de las TI e independiente de tecnologías específicas;
- Proveer un lenguaje común con un conjunto de términos y definiciones generalmente entendidos por todas las partes interesadas;
- Ayudar a atender los requisitos regulatorios, por ser consistentes con los estándares de gobierno generalmente aceptados y controles de las TI esperados por reguladores y auditores externos.

### Ejercicio de refuerzo - buenas prácticas para el gobierno de las TI

Identifique dos buenas prácticas que pueden ser usadas para cada elemento descrito a continuación:

- Selección de proveedores de servicios y gestión y adquisición de servicios externos.
- Gestión de riesgos relacionados con TI cada vez más complejos, como la seguridad de la información.

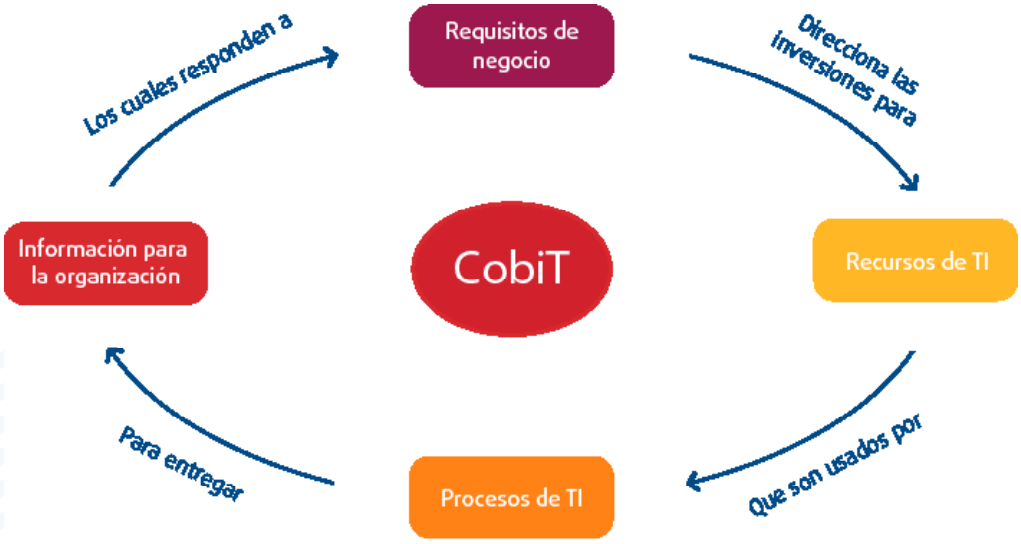
## 2.3 ¿Cómo CobiT 4.1 se relaciona con el gobierno de las TI?

CobiT 4.1 fue creado con las siguientes características principales:

- Enfocado en negocios
- Orientado a procesos

» Basado en controles
» Orientado por mediciones

El modelo CobiT 4.1 está basado en los principios mostrados en la siguiente figura:




La estructura de CobiT 4.1 provee la información que la organización necesita para alcanzar sus objetivos, las necesidades para invertir, gestionar y controlar los recursos de las TI usando un conjunto estructurado de procesos para proveer los servicios que permiten disponer de la información necesaria para la organización.

La gestión y el control de la información están presentes en toda la metodología CobiT 4.1 y ayudan a asegurar el alineamiento con los requisitos de negocio.

### 2.3.1 Requisitos de negocios

Para atender los objetivos de negocios, la información dentro de una organización necesita adecuarse a ciertos criterios de control, los cuales CobiT 4.1 denominan necesidades de información de la organización.

Con base en requisitos más amplios de calidad, confianza y seguridad, siete criterios de información distintos y sobrepuestos son definidos, así:

» **Calidad:**

- **Efectividad:** la información debe ser relevante y pertinente para el proceso de negocio, debe ser entregada a tiempo, de manera correcta, consistente y utilizable.
- **Eficiencia:** la información debe ser brindada mediante el mejor uso de los recursos (más productivos y económicos).

» **Seguridad:**

- **Confidencialidad:** la información debe ser protegida del acceso no autorizado para evitar la divulgación indebida.
- **Integridad:** la información debe ser precisa y completa, así como su validez de acuerdo con los valores y expectativas de negocios.
- **Disponibilidad:** la información debe estar disponible cuando sea requerida por el proceso de negocio, ahora y en el futuro, y de este modo debe ser la salvaguarda de los recursos necesarios y las capacidades asociadas.

» **Confianza:**

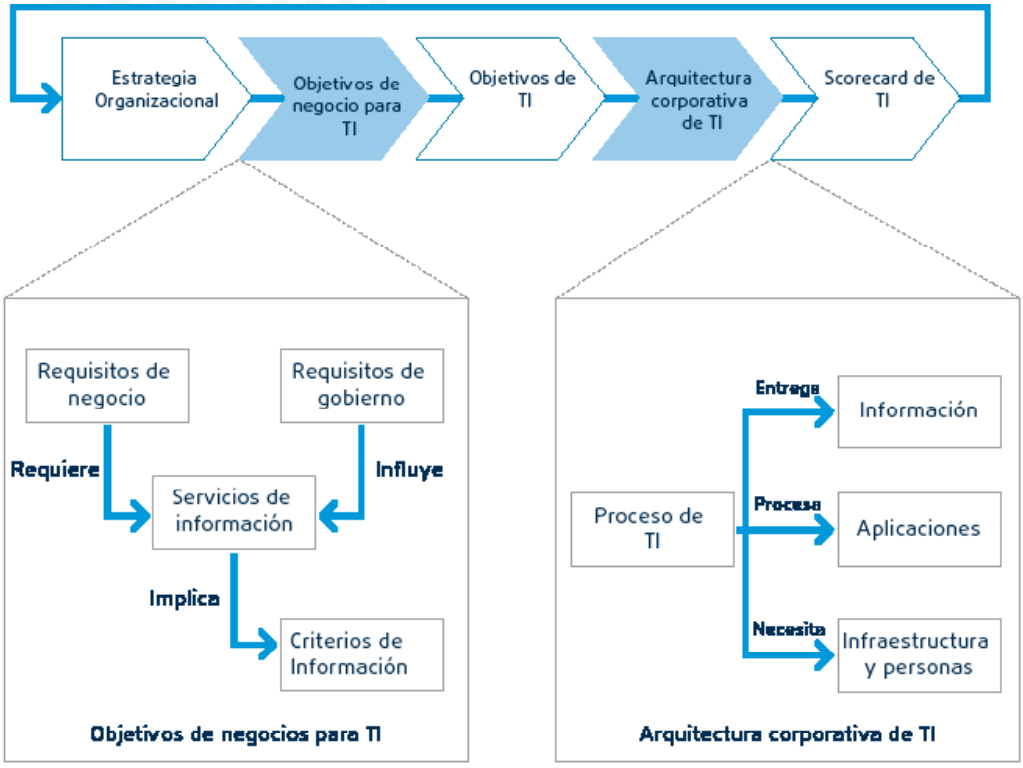
- **Conformidad:** la información debe estar conforme a las leyes, reglamentos y arreglos contractuales a los cuales los procesos de negocio están sujetos, esto es, criterios de negocio impuestos externamente y políticas internas.
- **Confiabilidad:** la información debe ser brindada de forma apropiada, permitiendo su uso en la operación de la organización, en la publicación de informes financieros para sus usuarios y órganos fiscalizadores, conforme a las leyes y a los reglamentos.

### 2.3.2 Objetivos de negocio y objetivos de las TI

De acuerdo con CobiT 4.1, para que el área de las TI entregue de manera exitosa los servicios que soportan las estrategias de negocios, debe existir una definición clara de las responsabilidades y de los requisitos por parte del área de negocios (el cliente), además de un entendimiento preciso acerca de qué y cómo necesita ser entregado por el área de las TI (el proveedor).

La Figura 7 muestra cómo la estrategia de la organización debería ser traducida por el área de negocios en objetivos relacionados a las iniciativas de las TI (objetivos de negocios para TI). Esos objetivos deben llevar a una clara definición de los objetivos propios del área de las TI (los objetivos de las TI), lo que a su vez definirá los recursos y capacidades de las TI (la arquitectura de las TI para la organización) necesarios para ejecutar de manera exitosa la parte que le corresponde a TI en la estrategia de la organización, representando así la relación entre los objetivos de negocio y los objetivos de las TI de una organización.

**Figura 7.** Objetivos y arquitectura de las TI



## Ejercicio de refuerzo - relación de CobiT con el gobierno de las TI

» Con base en la información del *framework* CobiT 4.1, ¿cómo atiende las necesidades de su organización para alcanzar el gobierno de las TI?
» Identifique para su organización:
  - Dos objetivos de negocio
  - Dos objetivos de las TI

## 2.4 Dominios y procesos de CobiT

Los cuatro dominios de CobiT están interrelacionados con la siguiente denominación:

» Planear y Organizar, PO: provee la dirección para la entrega de soluciones (AI) y entrega de servicios (DS)
» Adquirir e Implementar, AI: provee las soluciones y las transfiere para convertirlas en servicios
» Entregar y Soportar, DS: recibe las soluciones y las hace susceptibles de uso por los usuarios finales
» Monitorear y Evaluar, ME: monitorea todos los procesos para garantizar que la dirección definida sea seguida.

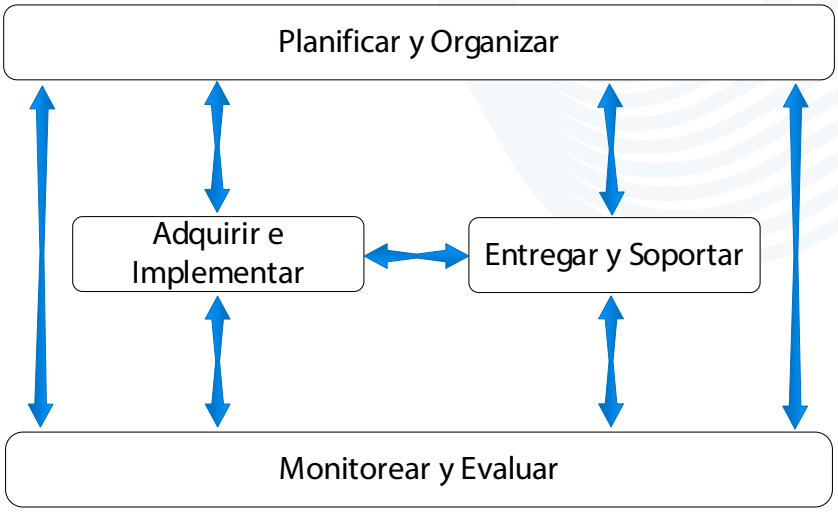
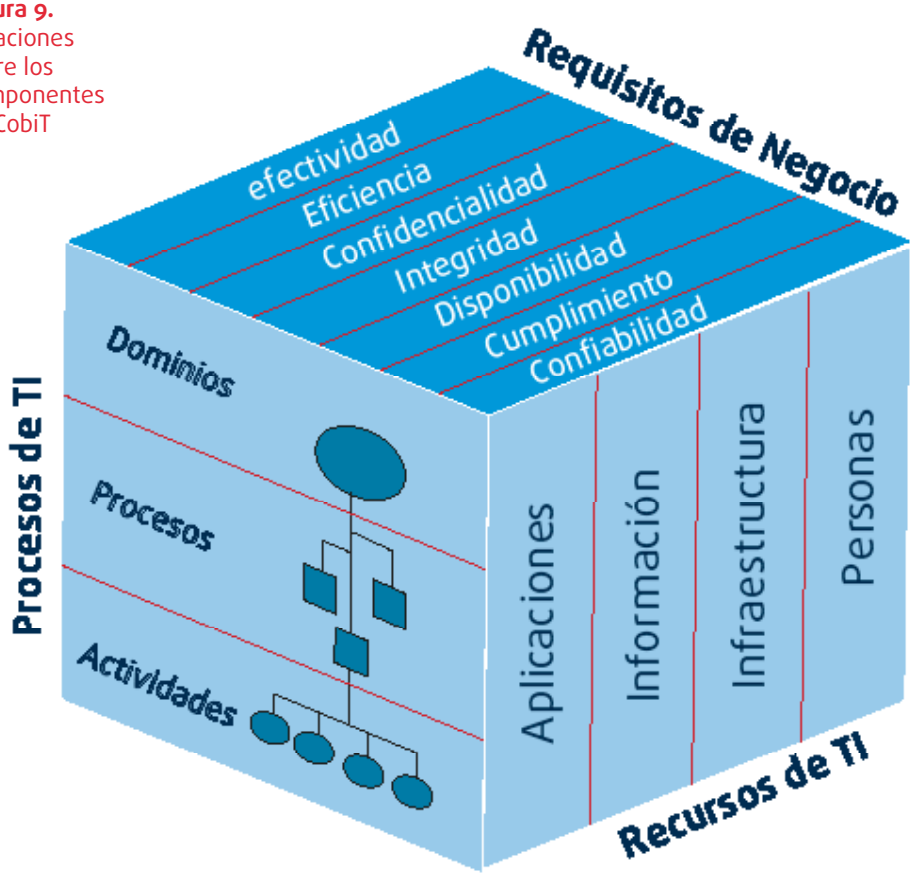



**Figura 8.** Relación entre los cuatro dominios de CobiT

Todos los componentes de CobiT 4.1 están interrelacionados, formando una cadena conjunta de acciones, como puede ser visto en la Figura 9, con el modelo de procesos de CobiT 4.1 de cuatro dominios, conteniendo 34 procesos genéricos de las TI, gestionando los recursos de las TI para la entrega de la información para el área de negocios, de acuerdo con los requerimientos de negocios y gobierno.

**Figura 9.**
Relaciones entre los componentes de CobiT




La implementación de buenas prácticas debe ser consistente con el gobierno y el ambiente de control de la organización, apropiada e integrada a otros métodos empleados para la mejora de los procesos.

Estándares y buenas prácticas no son un remedio para todos los males, dado que su efectividad depende de cómo fueron implementados y si se mantienen actualizados. Son más útiles cuando, aplicados como un

conjunto de principios, son un punto de partida para la producción de procedimientos específicos. Para evitar que las prácticas queden relegadas a la teoría, la gerencia y los funcionarios deben entender lo que deben hacer, cómo hacerlo y por qué eso es importante.

Para alcanzar el alineamiento de las buenas prácticas con los requisitos de negocios CobiT 4.1 debe ser usado en un alto nivel, brindando una metodología de control general con base en un modelo de procesos de las TI que debe servir para cualquier organización. Las prácticas específicas y estándares cubriendo áreas específicas pueden ser mapeados a partir de CobiT 4.1, brindando así un material de orientación.

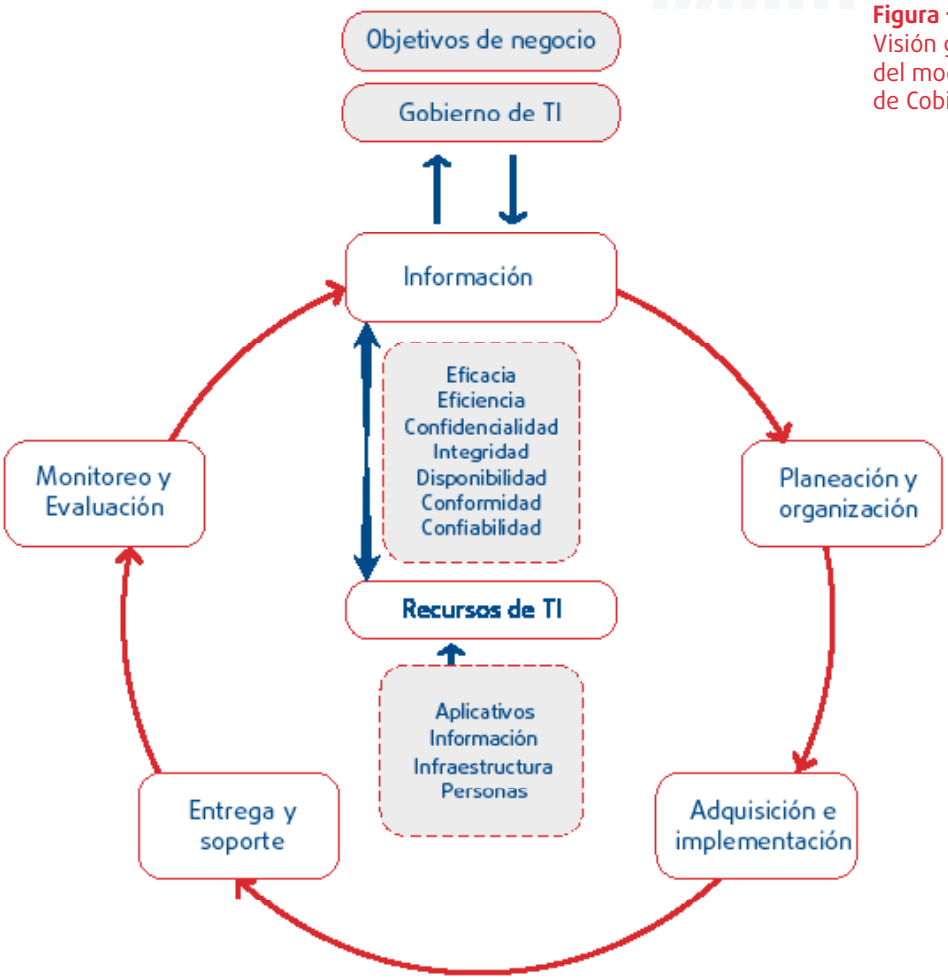



**Figura 10.** Visión general del modelo de CobiT 4.1

Continuación figura 10. Visión general del modelo de CobiT 4.1

| Dominio<br>Planear y Organizar, PO. |
|---|
| Procesos:<br>PO1. Definir la planificación estratégica de las TI<br>PO2. Definir la Arquitectura de información.<br>PO3. Determinar la dirección tecnológica.<br>PO4. Definir los procesos, organizaciones y relaciones de las TI.<br>PO5. Gestionar las inversiones de las TI.<br>PO6. Comunicar los objetivos y la dirección de gestión.<br>PO7. Gestionar los recursos humanos de las TI.<br>PO8. Gestionar la calidad.<br>PO9. Evaluar y gestionar los riesgos de las TI.<br>PO10. Gestionar proyectos. |

| Dominio<br>**Adquirir e implementar, AI.** |
|---|
| Procesos:<br>AI1. Identificar soluciones automatizadas.<br>AI2. Adquirir y mantener el software aplicativo.<br>AI3. Adquirir y mantener la infraestructura tecnológica.<br>AI4. Habilitar la operación y el uso.<br>AI5. Adquirir recursos de las TI<br>AI6. Gestionar cambios.<br>AI7. Instalar y homologar soluciones y cambios. |

| Dominio<br>**Entrega y Soporte, DS.** |
|---|
| Procesos:<br>DS1. Definir y gestionar niveles de servicio.<br>DS2. Gestionar los servicios de terceros.<br>DS3. Gestionar el desempeño y la capacidad.<br>DS4. Asegurar la continuidad de los servicios.<br>DS5. Garantizar la seguridad de los sistemas.<br>DS6. Identificar y ubicar costos<br>DS7. Capacitar y entrenar usuarios.<br>DS8. Gestión del centro de servicios y los incidentes.<br>DS9. Gestionar las configuraciones.<br>DS10. Gestionar los problemas.<br>DS11. Gestionar los datos.<br>DS12. Gestionar el entorno físico.<br>DS13. Gestionar las operaciones de las TI. |

| Dominio<br>**Monitorear y evaluar, ME.** |
|---|
| Procesos:<br>ME1. Monitorear y evaluar el desempeño de las TI.<br>ME2. Monitorear y evaluar los controles internos.<br>ME3. Asegurar la conformidad con los reglamentos.<br>ME4. Proveer Gobierno de las TI. |

### Ejercicio de refuerzo - utilizando el modelo de CobiT

Identifique los componentes de CobiT 4.1 utilizados en su organización.

## 2.5 Objetivos de control

Los controles son un conjunto de políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer una garantía razonable de que los objetivos de negocios serán cumplidos y que eventos indeseables serán prevenidos, detectados y corregidos.

Los objetivos de control de las TI son resultados esperados con la implementación de procedimientos de control en una determinada actividad de las TI.

CobiT 4.1 presenta 34 objetivos de control de alto nivel y 210 objetivos de control detallados.

Básicamente, los objetivos de control son usados para evaluar o auditar los procesos y actividades de las TI, buscando el mejoramiento continuo para que los objetivos de negocio sean alcanzados. Los objetivos de controles son identificados por dos letras para identificar el dominio (PO, AI, DS y ME), un número de proceso y un número de objetivo de control.

Los controles pueden ser divididos en:

- Controles de negocios y de las TI;
- Controles generales de las TI y controles de aplicaciones.

### 2.5.1 Controles de negocios y de las TI

Los sistemas de controles internos de las organizaciones afectan el área de las TI en tres niveles:

- En el nivel de la alta dirección, los objetivos de negocios son definidos y las decisiones son tomadas en relación a cómo entregar y gestionar los recursos de la organización para ejecutar la estrategia. El enfoque general para el gobierno y el control es definido por la alta dirección y comunicado a toda la orga-

nización. El ambiente de control de las TI es direccionado por estos objetivos y políticas de alto nivel.

» En el nivel de los procesos de negocios, los controles son aplicados a las actividades específicas de los negocios. La mayoría de los procesos de negocios es automatizada e integrada a los sistemas aplicativos de las TI. Sin embargo, algunos controles existentes en los procesos de negocios permanecen como procedimientos manuales. Por tanto, los controles en el nivel de los procesos de negocios son una combinación de controles manuales y de aplicativos automatizados. Ambos son de responsabilidad del área de negocios en lo que se refiere a la definición y gestión, aunque los controles de los aplicativos exijan la participación del área de las TI en su proyecto y desarrollo.

» Para soportar los procesos de negocios, el área de las TI brinda servicios, usualmente de manera compartida para diversos procesos de negocios, dado que muchos procesos de desarrollo y operacionales de las TI son ofrecidos a toda la organización, y una buena parte de la infraestructura de las TI es brindada como un servicio común, como por ejemplo: redes, bases de datos, sistemas operacionales y de almacenamiento. Los controles aplicados a todas las actividades de servicios de las TI son llamados controles generales de las TI.

### 2.5.2 Controles generales de las TI y controles de aplicativos

Los controles generales son controles incluidos en los procesos de las TI y servicios, como:

» Desarrollo de sistemas;
» Gestión de cambios;
» Seguridad;
» Operación de computadores.

Los controles incluidos en los aplicativos de los procesos de negocios son comúnmente llamados controles de aplicativos, como:

» Totalidad;
» Veracidad;
» Validez;

» Autorización;
» Segregación de funciones.

CobiT 4.1 asume que el proyecto y la implementación de los controles automatizados en aplicativos son de responsabilidad del área de las TI, cubiertos en el dominio Adquisición e Implementación, AI, con base en los requisitos de negocios definidos a partir de los criterios de información de CobiT 4.1. La responsabilidad por el control y la gestión operacional de los controles de aplicativos no es del área de las TI, es del propietario del proceso de negocio.

Así, la responsabilidad por los controles de aplicativos es compartida entre las áreas de negocios y de las TI, pero la naturaleza de las responsabilidades es diferente, así:

» El área de negocios es responsable por:
  • Definir los requisitos funcionales y de controles;
  • Utilizar los servicios automatizados.
» El área de las TI es responsable por:
  • Automatizar e implementar los requisitos funcionales y de controles;
  • Establecer controles para mantener la integridad de los controles de aplicativos.

De esta forma, los procesos de las TI de CobiT 4.1 cubren los controles generales de las TI, pero solamente los aspectos de desarrollo de los controles de aplicativos, y la responsabilidad por la definición y el uso operacional es del área de negocios.

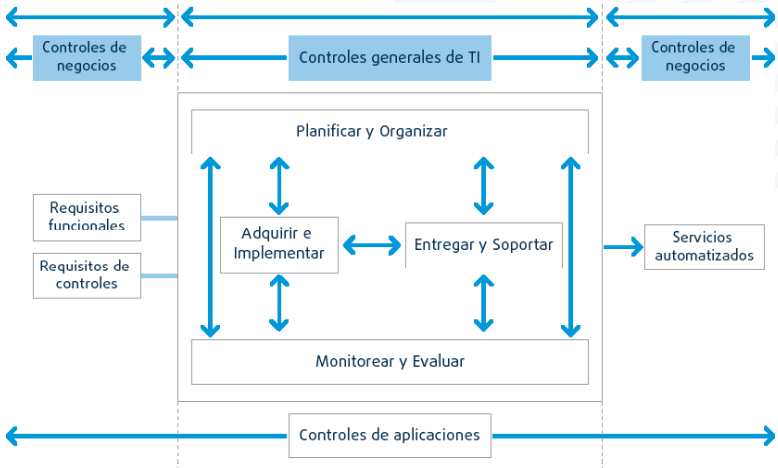



**Figura 11.** Controles de las TI y de negocios

## Ejercicio de refuerzo - controles de negocios y de las TI

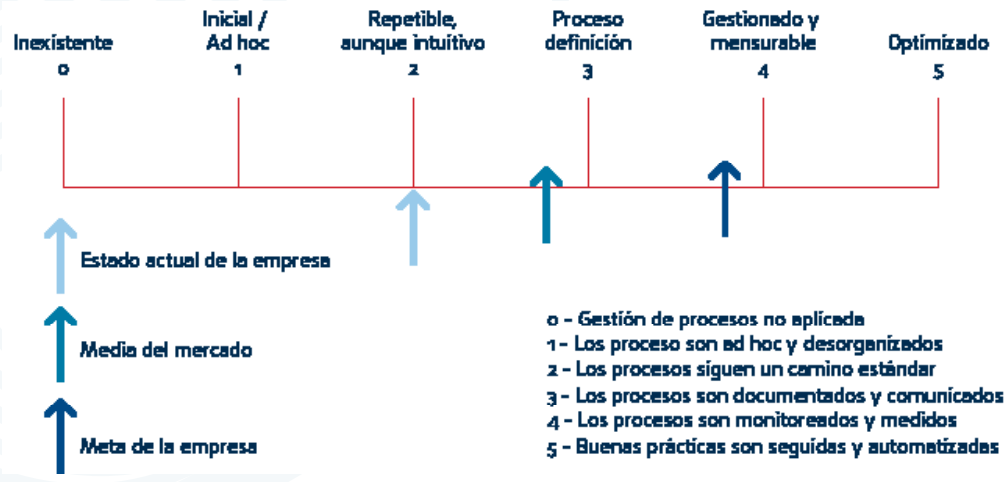
Identificar los controles de negocios y de las TI usados en su organización.

## 2.6 Modelo de madurez de procesos

El modelo de madurez para la gestión y control de procesos de las TI está basado en un método de evaluación de la organización, lo que permite que esta sea calificada desde un nivel de madurez no existente (0) al optimizado (5).

Los niveles de madurez son designados como un modelo inicial, en donde no se puede avanzar a un siguiente nivel sin antes haber cumplido con todas las condiciones del nivel anterior.

**Figura 12.** Modelo de madurez de procesos de CobiT 4.1




Cuando es aplicada una evaluación de madurez de procesos de las TI usando CobiT 4.1 es posible determinar el grado de madurez y crear planes de acción para la evolución del proceso.

### 2.6.1 Niveles de madurez

El nivel de madurez refleja el estado de evolución de un determinado proceso de las TI.

En líneas generales, los niveles de madurez poseen características que pueden ser analizadas, conforme a la información presentada en la siguiente tabla:

Tabla 1. Características de los niveles de madurez

| Madurez | Descripción |
|---|---|
| **Nivel 0** (No existe) | Desconocimiento, por parte de la organización, de los procesos y del problema a ser tratado. |
| Nivel 1 (Inicial/Ad Hoc) | Existe un reconocimiento de los problemas y hasta de los procesos, pero las actividades son ejecutadas de acuerdo con el conocimiento de las personas. |
| **Nivel 2** (Repetible) | Existen procesos informalmente definidos, con resultados previsibles, pero sin ninguna estandarización de las actividades. |
| **Nivel 3** (Procesos definidos) | Los procesos son definidos, formalizados y estandarizados en la organización, los resultados generados son conocidos y las personas son entrenadas cada vez que es necesario. |
| **Nivel 4** (Gestionados y medidos) | Los procesos formalizados son medidos y controlados, generando un ambiente de acompañamiento continúo del desempeño. |
| **Nivel 5** (Optimizado) | Existe una realimentación del desempeño medido, generando un ciclo de mejoramiento continuo. |

### 2.6.2 Criterios de control de procesos

Los criterios de control de procesos son elementos de gestión aplicables a cualquier proceso. A diferencia de los demás criterios de evaluación, los controles de procesos no son mutuamente excluyentes, y sí complementarios. De esta forma, se espera que un proceso controlado, de acuerdo con las prácticas de gobierno de las TI, atienda a todos los criterios de control de procesos. En un escenario en el cual se atienden a todos los criterios de control de procesos, la puntuación máxima de 100% es aplicada a este proceso.

La siguiente tabla presenta los criterios utilizados para evaluar los controles de procesos.

Tabla 2. Criterios utilizados para evaluar los controles de procesos

| Rol del proceso | Descripción |
|---|---|
| Metas y objetivos de los procesos | Consiste en definir y comunicar las metas y objetivos de los procesos de modo específico, medible, responsable de ser alcanzado, realista, orientado a resultados y a temporales, para la efectiva ejecución de cada proceso de TI. |
| Propietarios de los procesos | Consiste en atribuir un propietario para cada proceso de TI, y definir claramente los roles y las responsabilidades del propietario del proceso, como por ejemplo, la responsabilidad por la concepción, la interacción con otros procesos, la prestación de cuentas de los resultados finales, la medición del desempeño y la identificación de oportunidades de mejora del proceso. |
| Repetición de los procesos | Consisten definir e implementar procesos repetitivos y que produzcan consistentemente los resultados esperados. Los procesos deben proporcionar una secuencia de actividades que sea lógica, flexible y escalable, para la obtención de los resultados deseados, y también ser suficientemente ágil para responder con excepciones y emergencias |
| Roles y responsabilidades | Consiste en definir las principales actividades y resultados finales del proceso, además de atribuir y comunicar de modo inequívoco los papeles y responsabilidades para la efectiva ejecución y documentación de las actividades principales, así como el proceso de identificar la responsabilidad por los resultados finales obtenidos en el proceso. |
| Políticas, planes y procedimientos | Consiste en definir y comunicar todas las políticas, planes y procedimientos que orienten un proceso de TI. También se debe atribuir responsabilidades cada una de las actividades y verificar si estas son ejecutadas correctamente, además de asegurar que las políticas, planes y procedimientos sean accesibles y asimilados. |
| Acciones de mejoramiento continuo | Consiste en identificar un conjunto de métricas que brinden indicadores sobre los resultados y sobre el desempeño del proceso. Deben ser establecidas metas que actúen sobre el proceso de metas e indicadores de desempeño y también en la forma de obtener los datos y en su comparación con los objetivos. |

## 2.7 Medición del desempeño

Los objetivos y métricas son definidos en CobiT 4.1 en tres niveles:

- Objetivos y métricas de las TI que definen lo que los negocios esperan de las TI y la forma de realizar la medición.
- Objetivos y métricas de los procesos que definen las entregas de los procesos de las TI para soporte a los objetivos de las TI y la forma de realizar la medición.
- Objetivos y métricas de actividades que establecen lo que necesita ocurrir dentro del proceso para alcanzar el desempeño requerido y la forma de realizar la medición.

Los objetivos son definidos de arriba hacia abajo de manera que los objetivos de negocios determinarán varios objetivos de las TI que los soportaran. Un objetivo de las TI es alcanzado por medio de un proceso o por interacción de un determinado número de procesos.

Por tanto, los objetivos de las TI ayudan en diferentes objetivos de procesos. A su vez, cada objetivo de proceso requiere un determinado número de actividades, estableciendo así los objetivos de actividad.

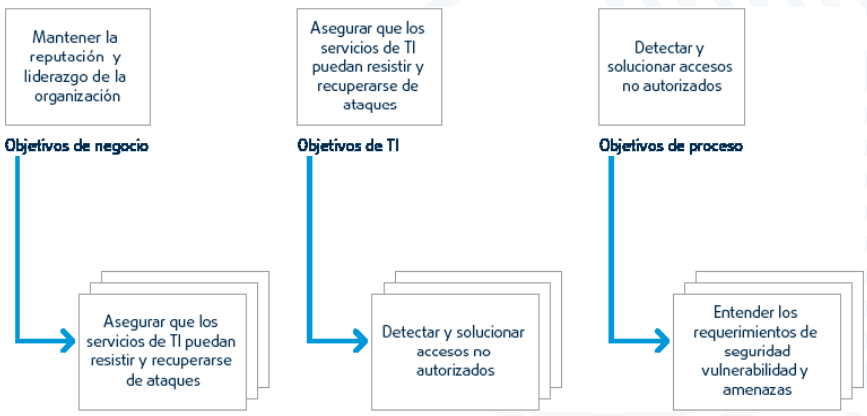


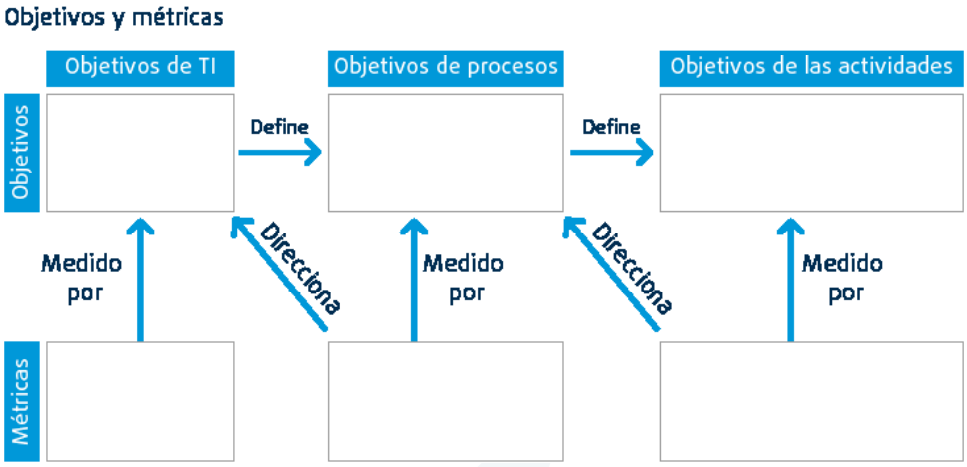

**Figura 13.** Relación de los objetivos de la organización

Para la medición del desempeño de los procesos son usadas dos métricas:

» Medidas de resultados (salidas), anteriormente indicadores clave de objetivos, KGIs "por sus siglas en inglés", indica si los objetivos fueron alcanzados, y debe ser medido solamente después de los hechos, siendo llamados indicadores históricos (*lag Indicators*).

» Indicadores de desempeño, anteriormente indicadores clave de desempeño, KPIs "por sus siglas en inglés",, indican que los objetivos serán posiblemente alcanzados, medidos antes de que los resultados sean claros, y por tanto llamados de indicadores futuros (*lead indicators*)

**Figura 14.**
Relación entre objetivos y métricas




En la parte superior de la figura están representados los objetivos de las TI, los objetivos de proceso y los objetivos de las actividades de proceso. La relación entre ellos va del nivel más alto (objetivos de TI) al nivel más detallado (objetivos de las actividades).

En la parte inferior están representadas las métricas asociadas a cada objetivo, pudiendo ser de resultados o de indicadores de desempeño. De esta forma es posible definir todas las métricas para los objetivos de las TI, pues CobiT 4.1 no brinda métricas para los objetivos de negocios.

## 2.8 Estructura de CobiT 4.1

Para entender mejor CobiT 4.1 es necesario que algunos aspectos sean indicados. Para cada uno de los procesos de CobiT 4.1 es presentada una descripción, en conjunto con los principales objetivos y métricas, además de definir los objetivos de control, así como declaraciones de acciones genéricas con el mínimo de buenas prácticas gerenciales, buscando garantizar el control sobre el proceso. En el inicio de cada proceso de CobiT 4.1, se hace una descripción con los objetivos de control de alto nivel del proceso.

Lo que se aprendió

- ¿Cómo utilizar el marco CobiT?
- ¿Cuál es la estructura del marco CobiT?
- ¿Cuál es la definición de controles de procesos, de las TI y de negocios?
- ¿Cuáles son los niveles de madurez de los procesos?
- Relación entre CobiT y gobierno de las TI
- Áreas de énfasis del gobierno de las TI:
  - Alineamiento estratégico
  - Entrega de valor
  - Gestión de recursos
  - Gestión de riesgos
  - Medición de desempeño
- Criterios de información:
  - Efectividad
  - Eficiencia
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Conformidad
  - Confiabilidad

Capítulo

03

# Estudio de los dominios PO y AI de CobiT

**Objetivos**

Comprender los dominios Planear y Organizar, PO, y Adquirir e Implementar, AI, así como los objetivos de control de sus procesos.

**Conceptos**

Dominio: Planear y Organizar, PO, y sus 10 procesos; Dominio: Adquirir e Implementar, AI, y sus 7 procesos.

# Introducción

El modelo de gobierno de las TI recomendado por CobiT 4.1 es utilizado actualmente para estructurar el área de las TI de las organizaciones, para que ellas sean capaces de soportar adecuadamente los servicios de los cuales dependen sus negocios. La estructura de CobiT 4.1 direcciona el área de las TI para ejecutar sus actividades con orientación a los procesos, proporcionando mejoras en los servicios que las TI brindan a la organización.

En este sentido, el área de las TI debe organizar y planear todas sus actividades, buscando las mejores alternativas de inversión alineadas a los recursos que la TI debe proveer para soportar y entregar los servicios del negocio. También es importante que la organización tenga mecanismos estandarizados para la adquisición e implementación de infraestructura de las TI, procurando siempre la mejor selección para sus negocios, garantizando que todo cambio necesario en el área de las TI no afecte las áreas de negocios.

Esta sesión será sobre los dominios Planear y Organizar, PO, y Adquirir e Implementar, AI, abordando los principales asuntos relacionados, como recursos, criterios de información y áreas de énfasis del gobierno de las TI.

## 3.1 Dominio Planear y Organizar, PO.

Este dominio comprende las estrategias y las tácticas de las TI, buscando identificar cómo el área de las TI puede contribuir para que la organización alcance los objetivos de negocio. La realización de la visión estratégica necesita ser planeada, gestionada y comunicada a toda la organización.

Es necesario que el área de las TI de la organización tenga una infraestructura tecnológica adecuada para dar sustentabilidad a los procesos de negocios.

La planeación cuida del desarrollo de los planes estratégicos de las TI que den soporte a los objetivos de negocio. Esos planes deben contemplar el futuro y estar alineados con los ciclos de tiempo de planeación de la organización, que puede tener proyecciones de dos, tres o cinco años.

El dominio PO puede ayudar a direccionar la participación del área de las TI en la planeación general de la organización en los siguientes aspectos:

- Proveer el alineamiento entre las estrategias de las TI y del negocio.
- Evaluar si la organización está utilizando los recursos de las TI para soportar los negocios.
- Divulgar los objetivos de las TI para toda la organización.
- Entender y gestionar los riesgos de las TI.
- Evaluar si los sistemas de información son adecuados a las necesidades de los negocios.

El dominio Planear y Organizar, PO, es compuesto por diez procesos:

- PO1. Definir un plan estratégico de las TI
- PO2. Definir la arquitectura de la información.
- PO3. Determinar las directrices de tecnología.
- PO4. Definir los procesos, organizaciones y relaciones de las TI.
- PO5. Gestión de la inversión de las TI.
- PO6. Comunicar metas y directrices gerenciales.
- PO7. Gestionar los recursos humanos de las TI.
- PO8. Gestión de la calidad.
- PO9. Evaluar y gestionar los riesgos de las TI.
- PO10. Gestión de proyectos.

### 3.1.1 Proceso PO1. Definir un plan estratégico de las TI

Objetivo: hacer que las áreas de las TI y de negocio trabajen en armonía en la traducción de los requisitos de negocio en oferta de servicios y en el desarrollo de estrategias para la entrega de servicios de manera eficaz y transparente.

Es alcanzado por medio de:

- Compromiso de la dirección de la organización en la alineación de la planeación estratégica de las TI con las necesidades actuales y futuros del área de negocios.
- Conocimiento de la capacidad actual de las TI.
- Establecimiento de un proceso de priorización de objetivos de negocio, que cuantifique los requisitos de negocio.

Es necesario definir y documentar todas las etapas del proceso de planeación estratégica, así como las normas y procedimientos complementarios, inclusive con la definición de roles y responsabilidades, frecuencia y estándares para la planeación, permitiendo una mejor comprensión de los resultados esperados, además de la definición de esfuerzos y herramientas que deben ser utilizadas para la ejecución de la planeación.

Ejemplo: en las organizaciones en las que el área de las TI tiene un papel estratégico, su desafío es no convertirse en la ruta crítica para el desarrollo de los negocios, pues en la mayoría de casos la percepción de los gerentes de negocios, en relación a la calidad de los servicios prestados por TI, es que no atienden la necesidad de evolución de los negocios de la organización.

Así mismo, definir y mantener un plan estratégico de las TI, conforme a lo descrito en PO1, como un proceso continuo, es fundamental para un alineamiento constante con los negocios y para que la organización alcance sus objetivos.

La siguiente tabla muestra los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"definir un plan estratégico de las TI"** busca satisfacer y mantener bajo gestión y control, de manera que garantice que los objetivos de negocio sean alcanzados.

Tabla 3. Requisitos de negocio proceso "definir un plan estratégico de las TI"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | S | Gestión de riesgos | S | Información |
| | | Gestión de recursos | S | Infraestructura |
| | | | | Personas |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"definir un plan estratégico de las TI"**, de tal forma que garantiza que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 4. Objetivos de control proceso "definir un plan estratégico de las TI"

| Objetivos de control |
|---|
| PO1.1 Gestión de valor de las TI: alinear las inversiones del área de las TI con los procesos de negocios de la organización y proveer evaluación de las TI en el sentido de verificar si está entregando los servicios que el negocio necesita. |
| PO1.2 Alineamiento entre TI y negocios: el plan estratégico de negocios debe direccionar la planeación estratégica de las TI, garantizando que las prioridades sean aceptadas por ambas partes. |
| PO1.3 Evaluación de la capacidad y desempeño actual: evaluar la capacidad de las TI para entregar los servicios de negocio esperados y proveer mecanismos para la planeación de la capacidad futura, en alineamiento o con el aumento de la capacidad del negocio. |
| PO1.4 Plan estratégico de las TI: crear y mantener un plan estratégico de las TI alineado a las necesidades y prioridades del negocio, garantizando que las TI contribuyan con los objetivos de negocios de la organización. Debe direccionar los planes tácticos de las TI. |
| PO1.5 Planes tácticos de las TI: deben contener las iniciativas, los recursos necesarios para implementarlas y cómo serán monitoreadas y gestionadas. Los planes tácticos deben direccionar los planes de proyectos que serán incluidos en el portafolio de la organización. |
| PO1.6 Gestión del portafolio de las TI: TI debe gestionar su portafolio de proyectos en alineamiento con los objetivos de negocios y la prioridad que debe ser atribuida a cada proyecto |

La definición de un plan estratégico de las TI necesita varias fuentes de información (entradas), produciendo información de salida.

CobiT 4.1 establece un conjunto amplio de relaciones de entrada y salida del proceso **"definir un plan estratégico de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo para evaluar el nivel de madurez de la organización en relación al proceso **"definir un plan estratégico de las TI".**

### 3.1.2 Proceso PO2. Definir la arquitectura de la información

Establecer un modelo que incorpore un esquema de clasificación de datos para asegurar integridad y la consistencia de todos los datos, alcanzado por:

- Garantías de la precisión de la arquitectura de la información y del modelo de datos.
- Establecimiento de la propiedad de los datos (área de negocio responsable por el dato).
- Clasificación de la información utilizando un esquema acordado entre las áreas de negocio y TI.
- El área de las TI debe crear y mantener un modelo de arquitectura de la información, que comprenda el modelo de datos y los sistemas de información de la organización.
  - Este modelo de arquitectura de la información debe ser consistente con el plan estratégico de las TI.

La información debe ser identificada, estructurada y mantenida de acuerdo con las necesidades del negocio. Para ello, la información debe ser almacenada y estar disponible mediante los mecanismos apropiados y en los momentos adecuados, con el fin de permitir que las personas realicen sus actividades con información confiable.

Ejemplo: es común en las organizaciones el desarrollo de sistemas y aplicaciones sin estándares, en la mayoría de ocasiones para atender una demanda específica, donde la integración entre sistemas y aplicaciones es dejada de lado. En estos casos, la organización, en un corto tiempo, desarrolla una serie de soluciones desintegradas, sin estándar de datos e información. Los ejecutivos y gerentes no consiguen obtener una información de forma rápida y precisa, pues necesitan buscar

la información en fuentes de datos dispersas en varios sistemas transaccionales. Implementar una arquitectura de la información integrada, estandarizada y evolutiva es un factor clave para que los ejecutivos y gerentes puedan tomar decisiones sobre la continuidad de los negocios. Implementar una arquitectura de la información de acuerdo con el proceso PO2 dirige a la organización a resolver los problemas de integración y estandarización de sus sistemas y aplicaciones.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"definir la arquitectura de la información"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 5. Requisitos de negocio proceso "definir la arquitectura de la información"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | S | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | P | Gestión de recursos | P | Información |
| Confidencialidad | S | | | |
| Integridad | P | | | |

Nomenclatura: P: Primario; S: Secundario

CobiT 4.1 define los siguientes objetivos de control para el proceso **"definir la arquitectura de la información",** con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 6. Objetivos de control proceso
"definir la arquitectura de la información"

| Objetivos de control |
|---|
| PO2.1 Modelo de arquitectura de la información de la organización: crear y mantener un modelo de información que permita el desarrollo de aplicaciones de soporte a la toma de decisiones para el área de negocios. Es importante que el modelo soporte toda la seguridad de la información. |
| PO2.2 Diccionario de datos corporativos y reglas de sintaxis de datos: crear y mantener un diccionario de datos y reglas de sintaxis, permitiendo el intercambio en toda la organización, previniendo la duplicidad de elementos de una base de datos. |
| PO2.3 Esquema de clasificación de datos: clasificar los datos según su acceso, como público, confidencial y restringido, y definir quiénes son los dueños de los datos y los permisos de acceso. |
| PO2.4 Gestión de la integridad: definir e implementar procedimientos que aseguren la integridad y consistencia de todos los datos almacenados en forma electrónica, como bancos de datos, bodegas de datos y archivos de datos. |

La definición de la arquitectura de la información de la organización necesita de varias fuentes de información (entradas), produciendo informaciones de salida.

CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"definir la arquitectura de la información"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"definir la arquitectura de la información".**

### 3.1.3 Proceso PO3. Determinar las directrices de tecnología

Definir e implementar un plan de infraestructura, arquitectura y estándares de tecnología y aprovechar las oportunidades tecnológicas, a partir de:

- Establecimiento de un foro para direccionar la arquitectura y verificar su conformidad.
- Establecimiento de un plan equilibrado de infraestructura tecnológica con relación a los requisitos, costos y riesgos.
- Definición de estándares de infraestructura tecnológica con base en los requisitos de la arquitectura de la información.

El plan debe ser actualizado regularmente. Incluye aspectos como arquitectura de sistemas, direccionamiento tecnológico, plan de adquisiciones, estándares, estrategias de migración y contingencia. Esto permite respuestas rápidas a cambios en un ambiente competitivo, economía de escala en equipos y en inversiones de sistemas de información, así como una mejor interoperabilidad entre plataformas y aplicaciones.

Ejemplo: la tecnología se convirtió en un diferencial competitivo para las organizaciones. Explotar la evolución tecnológica y usarla para alcanzar los objetivos de negocio es uno de los factores que lleva a las organizaciones a realizar el alineamiento estratégico entre TI y el negocio. Así, cuando una nueva tecnología pasa a ser adoptada por casi todas las organizaciones de un determinado segmento de negocios, de tal forma que deja de ser factor de ventaja competitiva para quien la usa, pasa a ser un factor de desventaja para las organizaciones que no la usan. Por lo tanto, las organizaciones deben acompañar la evolución tecnológica por medio de acciones que garanticen el uso del mejor patrón de tecnología para el negocio, brindando una visión de futuro, por medio de la implantación de un proceso de acuerdo con el PO3.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"determinar las directrices de tecnología"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

**Tabla 7. Requisitos de negocio proceso "determinar las directrices de tecnología"**

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | P | Entrega de valor | P | Infraestructura |
| | | Gestión de riesgos | S | |
| | | Gestión de recursos | P | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"determinar las directrices de tecnología"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 8. Objetivos de control proceso "determinar las directrices de tecnología"

| Objetivos de control |
|---|
| PO3.1 Planeación de la directriz de tecnológica: planear el direccionamiento tecnológico y analizar las tecnologías existentes y emergentes y planear cual direccionamiento es apropiado para la tecnología que soporta el negocio. El plan debe contemplar la arquitectura de sistemas, el direccionamiento tecnológico, estrategias de migración y contingencia de los componentes de infraestructura. |
| PO3.2 Plan de infraestructura tecnológica: crear y mantener un plan de infraestructura tecnológica basado en el direccionamiento tecnológico. Incluye la contingencia y el direccionamiento para la adquisición de recursos tecnológicos. Considera cambios en el ambiente competitivo, economía de escala en inversiones en personal y sistemas de información, así como mejoras en la interoperabilidad entre plataformas y aplicaciones. |
| PO3.3 Monitoreo de tendencias futuras y regulaciones: establecer un proceso para monitorear las tendencias de las áreas de negocio, tecnología, infraestructura, aspectos legales y regulatorios. Incorporar las consecuencias de esas tendencias al desarrollo del plan de infraestructura de tecnologías de las TI. |
| PO3.4 Estándares tecnológicos: proveer soluciones tecnológicas seguras, eficaces y consistentes, en toda la organización, establecer un foro de tecnología para proveer directrices tecnológicas, aconsejar sobre productos de infraestructura, orientar en la selección de tecnología y evaluar la conformidad con estos estándares y directrices. |
| PO3.5 Comité de arquitectura de las TI: establecer un comité de arquitectura de las TI para proveer directrices de arquitectura, orientar su aplicación y verificar su conformidad, alineada con las estrategias de negocios. |

La definición del direccionamiento tecnológico de la organización necesita de varias fuentes de información (entradas), produciendo informaciones de salida.

CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"determinar las directrices de tecnología"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez desde la organización en relación al proceso **"determinar las directrices de tecnología".**

### 3.1.4 Proceso PO4. Definir los procesos, organización y relaciones de las TI.

Estructurar el área de las TI de forma transparente, flexible y comprometida con el negocio, definiendo e implementando procesos de las TI con roles y responsabilidades definidas e integradas a los procesos de negocio y de toma de decisiones, por medio de:

- Definición de una estructura de procesos de las TI
- Establecimiento de consejos y estructuras organizacionales apropiadas
- Definición de roles y responsabilidades

Los procesos, las políticas administrativas y los procedimientos necesitan estar establecidos para todas las funciones, con especial atención a las de control, garantía de calidad, gestión de riesgos, seguridad de la información, propiedad de sistemas y datos y segregación de funciones.

Ejemplo: el área de las TI de una organización debe ser administrada no solamente teniendo en cuenta los aspectos técnicos. Entre las principales dificultades que se encuentran en la gestión de las TI de las organizaciones, se puede citar la falta de integración con otras áreas internas, de conocimiento de los negocios de la organización, de planeación, de métodos, de procedimientos y procesos de trabajo, de conocimiento de los objetivos de las TI, así como de su divulgación, conocimiento técnico inferior a lo esperado, entre otros factores. Para que el área de las TI pueda tener eficiencia y eficacia en su misión de proveer lo mejor de la tecnología para los negocios, es fundamental que el proceso PO4 sea implantado.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"definir los procesos, organización y relaciones de las TI"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 9. Requisitos de negocio proceso "definir los procesos, organización y relaciones de las TI"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Personas |
| Eficiencia | P | Gestión de riesgos | P | |
| | | Gestión de recursos | P | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"definir los procesos, organización y relaciones de las TI"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 10. Objetivos de control proceso "definir los procesos, organización y relaciones de las TI"

| Objetivos de control |
|---|
| PO4.1 Estructura de procesos de las TI: definir un modelo de procesos de las TI para ejecutar el plan estratégico de las TI. El modelo de procesos de las TI debe estar integrado a un sistema de gestión de calidad y a una estructura de controles internos. |
| PO4.2 Comité estratégico de las TI: establecer un comité estratégico de las TI para asegurar que el gobierno de las TI sea debidamente considerado como parte del gobierno corporativo. Aconsejar sobre el direccionamiento estratégico y analizar las inversiones, priorizando los principales proyectos, en alineamiento con el portafolio de proyectos. |
| PO4.3 Comité ejecutivo de las TI: establecer un comité ejecutivo (o equivalente) compuesto por las direcciones ejecutivas, de negocios y de las TI para: determinar prioridades de los programas de inversiones en TI, alineados con las estrategias y prioridades del negocio; monitorear el estado actual de los proyectos y resolver conflictos de recursos; y monitorear niveles de servicio y sus mejoras. |
| PO4.4 Posicionamiento organizacional del área de las TI: posicionar el área de las TI en la estructura organizacional considerando la importancia de las TI para la estrategia del negocio y el nivel de dependencia operacional. |
| PO4.5 Estructura organizacional de las TI: establecer una estructura organizacional interna y externa de las TI que refleje las necesidades del negocio. Además, implementar un proceso de revisión periódica de la estructura para ajustarla a las necesidades cambiantes de la organización. |
| PO4.6 Definición de roles y responsabilidades: definir y comunicar al personal de las TI y a usuarios finales sus respectivos roles y responsabilidades, que especifiquen la autoridad, responsabilidad, con el objetivo de atender las necesidades de la organización. |
| PO4.7 Responsabilidad del aseguramiento de la calidad: crear la función de aseguramiento de la calidad (QA, *Quality Assurance*) que atienda los requisitos de la organización. |

Continuación tabla 10. Objetivos de control proceso "definir los procesos, organización y relaciones de las TI"

| Objetivos de control |
|---|
| PO4.8 Responsabilidad sobre riesgo, seguridad y conformidad: definir y atribuir roles para la gestión de riesgos de las TI, incluyendo la responsabilidad específica por la seguridad de la información, seguridad física y conformidad. Obtener el direccionamiento de la organización sobre los niveles específicos de riesgo de las TI aceptables y la aprobación de cualquier riesgo residual. |
| PO4.9 Propietarios de datos y sistemas: definir los propietarios de los datos y sistemas de información. Los propietarios toman decisiones sobre la clasificación de la información (pública, confidencial, restringida) y de los sistemas y los protegen de acuerdo con esa clasificación. |
| PO4.10 Supervisión: asegurar que los roles y las responsabilidades de las TI sean adecuadamente ejercidos, evaluar si todo el personal tiene autoridad y recursos suficientes para ejercer sus roles y responsabilidades y revisar de forma general los indicadores claves de desempeño. |
| PO4.11 Segregación de funciones: implementar una separación de roles y responsabilidades que reduzca la posibilidad de que un único individuo tenga el dominio de un proceso crítico. El personal del área de las TI debe ejecutar únicamente tareas autorizadas relacionadas a sus respectivos cargos y posiciones. |
| PO4.12 Dotación de personal de las TI: evaluar regularmente la capacidad de personal con base en cambios mayores en el negocio, en el entorno de las TI, o en la operación para garantizar que el área de las TI tenga cantidad suficiente de personal para soportar de forma adecuada los objetivos y metas de negocios. |
| PO4.13 Personal en clave de las TI: definir e identificar el personal clave de las TI (personal para reemplazo/respaldo) y minimizar la dependencia de un único individuo ejecutando una función crítica. |
| PO4.14 Políticas y procedimientos para personal contratado: garantizar que los consultores y el personal tercerizado que soporta la función de las TI conozca y cumpla con las políticas organizacionales para la protección de los activos de información de la entidad de conformidad con de las exigencias contractuales firmadas. |
| PO15 Relacionamientos: establecer y mantener una estructura optimizada de coordinación, comunicación y conexión entre las funciones de las TI y diversos intereses dentro o fuera del área de las TI: Junta directiva, unidades de negocio, usuarios individuales, proveedores, profesionales de seguridad, gestores de riesgos, gestión de personal tercerizado o externo y el grupo de conformidad corporativa(cumplimiento). |

La definición de los procesos, organización y relaciones de las TI de la organización necesita de varias fuentes de información, produciendo información de salida.

CobiT 4.1 estableció un amplio conjunto de relaciones de entrada y salida del proceso **"definir los procesos, organización y relaciones de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobIT 4.1 incluyó el modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"definir los procesos, organización y relaciones de las TI".**

### 3.1.5 Proceso PO5. Gestionar las inversiones de las TI

Decidir el portafolio de proyectos e inversiones en TI de forma eficaz y eficiente y elaborar los presupuestos de las TI alineados con las estrategias y decisiones de inversiones direccionadas por el área de negocios, por medio de:

- Previsión y asignación de presupuestos
- Definición del criterio de inversión formal (ROI, Retorno sobre la Inversión, período de recuperación de la inversión, VPN, Valor Presente Neto)
- Medición y evaluación del valor de negocio comparado con la predicción.

La planeación de presupuesto y de inversiones en TI debe reflejar toda la necesidad de crecimiento del negocio. El área de las TI no debe planear sola su presupuesto y sus inversiones necesarias para su crecimiento. Si ocurre existirá un desacople entre TI y el negocio, generando conflictos que pueden causar perjuicio para el negocio.

Ejemplo: es común oír que la TI es cara y no entrega lo necesario para el negocio. Este hecho puede ser cambiado si se tiene en cuenta que TI tiene una función estratégica fuerte en la organización. Para eso, es importante que los portafolios de programas, proyectos y servicios estén alineados con los objetivos de la organización, y que las inversiones en TI estén alineadas con estos portafolios, garantizando una relación entre inversiones en TI y desempeño de la organización. La garantía de que las inversiones son adecuadas debe ser brindada por la implementación del proceso PO5.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"gestionar de las inversiones de las TI"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 11. Requisitos de negocio proceso "gestionar las inversiones de las TI"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | P | Entrega del valor | P | Infraestructura |
| Confiabilidad | S | Gestión de recursos | P | Personas |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"gestionar las inversiones de las TI"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 12. Objetivos de control proceso "gestionar las inversiones de las TI"

| Objetivos de control |
|---|
| PO5.1 Estructura de administración financiera: crear y mantener una estructura financiera para gestionar de inversiones y costos de bienes y servicios de las TI por medio de portafolios de inversiones, casos de negocio y presupuestos de las TI. |
| PO5.2 Priorización dentro del presupuesto de las TI: crear y mantener un proceso de toma de decisiones para priorizar la asignación de los recursos de las TI en operaciones, proyectos y en mantenimiento. |
| PO5.3 Proceso de presupuesto de las TI: crear y mantener un proceso para elaborar el presupuesto que refleje las prioridades establecidas por el portafolio de programas de inversiones de las TI de la organización, incluyendo los costos continuos de operación y mantenimiento de la infraestructura actual. |
| PO5.4 Gestión de costo: crear y mantener un proceso de gestión de costo comparando los costos reales con lo presupuestado. Los costos deben ser monitoreados y comunicados. Si hay desviaciones, los impactos deben ser identificados y evaluados oportunamente y deben ser tomadas las acciones correctivas apropiadas |
| PO5.5 Gestión de beneficios: crear y mantener un proceso de monitoreo de los beneficios de proveer y mantener capacidades de las TI apropiadas. Las contribuciones esperadas de las TI sobre los resultados del negocio deben ser identificadas, y acordadas, monitoreadas y reportadas, tanto en programas de inversión en TI como en la operación de soporte regular. |

La definición de gestión de las inversiones de las TI de la organización necesita de varias fuentes de información, produciendo información de salida. CobiT 4.1 estableció un amplio conjunto de relaciones de entrada y salida del proceso **"gestionar las inversiones de las TI"** con otros

procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso.

CobiT 4.1 incluye un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"gestionar las inversiones de las TI".**

### 3.1.6 Proceso PO6. Comunicar aspiraciones y directrices gerenciales

Crear políticas, procedimientos, directrices y otros documentos de forma precisa, comprensible y aprobada por la organización, incorporado a una estructura de controles de las TI, a través de:

- Definición de una estructura de control de las TI
- Desarrollo e implementación de políticas de las TI
- Imposición de políticas de las TI

Todas las acciones del área de las TI deben ser debidamente comunicadas a toda la organización. El área de las TI debe proveer mecanismos para realizar la comunicación de sus objetivos, metas y directrices, mostrando que está alineada a los objetivos de negocio.

Ejemplo: conocer y gestionar los riesgos de las TI es una tarea por la cual todas las organizaciones se deben preocupar. Los riesgos están asociados tanto a las vulnerabilidades tecnológicas como a las humanas. Crear políticas y controles para garantizar la seguridad de la información, definir y comunicar a la organización metas y directrices gerenciales acerca de la actuación de las TI y crear mecanismos de control son factores claves del éxito para los negocios de una organización. En este sentido, las organizaciones deben adoptar una política de control basada en el proceso PO6.

Los requisitos de negocio, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso "comunicar metas y directrices gerenciales" busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados, pueden ser vistos en la siguiente tabla.

Tabla 13. Requisitos de negocio proceso "comunicar aspiraciones y directrices gerenciales"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Información |
| Conformidad | S | Gestión de riesgos | P | Personas |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"comunicar aspiraciones y directrices gerenciales"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 14. Objetivos de control proceso "comunicar aspiraciones y directrices gerenciales"

| Objetivos de control |
|---|
| PO6.1 Política de las TI y ambiente de control: crear y mantener los controles de las TI alineados con la organización y las políticas y reglas para la utilización del ambiente de las TI (control de acceso a los sistemas, política de seguridad de la información). |
| PO6.2 Riesgos empresariales de las TI y estructura interna de control: crear y mantener un marco que defina el enfoque de la organización sobre los riesgos de las TI y el control y que esté alineado con la política de las TI y el ambiente de control y el marco empresarial de riesgos y control. |
| PO6.3 Gestión de políticas de las TI: crear y mantener un conjunto de políticas para apoyar la estrategia de las TI. |
| PO6.4 Distribución de la política, estándares y procedimientos: asegurar que las políticas, estándares y procedimientos de las TI sean impuestos y que todas las personas de la organización tengan conocimiento de ellas. |
| PO6.5 Comunicación de los objetivos y directrices de las TI: divulgar todos los objetivos y directrices de TI asociados a los objetivos de negocio. |

La comunicación de aspiraciones y directrices gerenciales de las TI de la organización necesita de varias fuentes de información produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"comunicar aspiraciones y directrices gerenciales"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso.

CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"comunicar aspiraciones y directrices gerenciales".**

### 3.1.7 Proceso PO7 – Gestionar los recursos humanos de las TI

Admitir y capacitar personal, motivar a través de planes de carrera, atribuir funciones coherentes con las habilidades, establecer un proceso de revisión, crear descripciones de cargos y asegurar la conciencia a la dependencia de los individuos, por medio de:

- Revisión del desempeño del personal.
- Admisión, capacitación, evaluación de desempeño, promoción y desvinculación del personal de las TI.
- Mitigar el riesgo de dependencia excesiva de recursos claves.

La organización debe propiciar en el área de las TI la capacitación y el desarrollo de su personal, con base en la evaluación de desempeño y competencias. Los programas de capacitación y desarrollo deben ser elaborados alineadamente con las estrategias y los objetivos de las TI. Es importante que el área de las TI cree mecanismos para enfrentar las indisponibilidades y la prevención y detección de actividades fraudulentas.

Ejemplo: las áreas de las TI sufren con la rotación de personal especializado. Esta rotación está asociada a la falta de políticas de retención de profesionales en la mayoría de las organizaciones, lo que lleva al profesional de las TI a buscar otras oportunidades en el mercado laboral. La creación de una política de gestión del recurso humano para el área de las TI está totalmente asociada al alineamiento entre el área de las TI y el negocio.

La formación de un profesional de las TI, que además de ejecutar sus funciones técnicas también conozca el negocio de la organización, es construida a lo largo del tiempo. Cualificar y retener este profesional debe ser prioridad del área de las TI, de forma que la aplicación del proceso PO7 es de suma importancia para esto.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"gestionar los recursos humanos de las TI"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 15. Requisitos de negocio proceso "gestionar los recursos humanos de las TI"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Personas |
| Eficiencia | P | Gestión de riesgos | S | |
| | | Gestión de recursos | P | |
| | | Medición del desempeño | S | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"gestionar los recursos humanos de las TI"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 16. Objetivos de control proceso "gestionar los recursos humanos de las TI"

| Objetivos de control |
|---|
| PO7.1 Reclutamiento y retención de personal: asegurar que los procesos de reclutamiento de personal estén alineados con las políticas y los procedimientos de personal de la organización, tales como admisión y ambiente de trabajo positivo. Implementar procesos para asegurar una fuerza de trabajo de las TI apropiada y con las habilidades necesarias para alcanzar los objetivos de la organización. |
| PO7.2 Competencias personales: verificar regularmente si el personal tiene las competencias necesarias para ejercer sus funciones con base en la formación, la capacitación y o la experiencia. Definir los requisitos centrales de competencia en TI y verificar si están siendo cumplidos mediante programas de calificación y certificación. |
| PO7.3 Suplir vacantes: definir, monitorear y supervisar funciones, responsabilidades y la estructura definida de personal. |
| PO7.4 Entrenamiento de personal: proveer al personal de las TI el entrenamiento apropiado para mantener el conocimiento, las especializaciones, las habilidades, la concientización sobre controles internos y la seguridad en el nivel exigido para alcanzar los objetivos organizacionales. |
| PO7.5 Dependencia de individuos: minimizar la exposición a la dependencia crítica de personas claves por medio de captación, documentación e intercambio de conocimiento, desarrollo de posibles substitutos para los roles y funciones claves y planeación de la sucesión. |
| PO7.6 Procedimientos de liquidación de personal: incluir análisis de antecedentes en el proceso de reclutamiento de las TI. La extensión y la frecuencia de revisión periódica de esos análisis dependen de la sensibilidad y de la importancia de la función, debiendo ser aplicadas a los funcionarios, prestadores de servicio y proveedores. |

Continuación tabla 16. Objetivos de control
proceso "gestionar los recursos humanos de las TI"

| Objetivos de control |
| --- |
| PO7.7 Evaluación del desempeño profesional: exigir periódicamente la realización de evaluación de los objetivos individuales derivados de los objetivos de la organización y responsabilidades específicas del cargo. Los funcionarios deben recibir orientación sobre desempeño y conducta en la ejecución de sus actividades. |
| PO7.8 Cambio y desvinculación del cargo: crear acciones para cambio de cargo, especialmente en el caso de desvinculaciones. La transferencia de conocimiento necesita ser facilitada, las responsabilidades redistribuidas y los derechos de acceso eliminados, para que los riesgos sean minimizados y la continuidad de la función sea asegurada. |

La gestión de los recursos humanos de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"gestionar los recursos humanos de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 incluyó el modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"gestionar los recursos humanos de las TI".**

### 3.1.8 Proceso PO8. Gestionar la calidad

- Definir un Sistema de Gestión de Calidad, SGC.
- Monitorear continuamente el desempeño con base en objetivos predefinidos
- Implementar un programa de mejoramiento continuo de los servicios de las TI, mediante:
  - Definición de prácticas y estándares de calidad
  - Monitoreo y revisión de los desempeños interno y externos en comparación con las prácticas y estándares de calidad definidos
  - Mejoramiento continuo del SGC

Un SGC debe ser desarrollado y mantenido, incluyendo estándares y procesos de desarrollo y adquisición por el área de las TI. La gestión de la calidad es esencial para asegurar que la TI esté otorgando valor al negocio, al mejoramiento continuo y a la transparencia de las acciones.

Ejemplo: las organizaciones han dado énfasis a la producción de bienes y servicios de calidad para atender sus necesidades de negocio. La necesidad de una mejor definición del concepto de calidad, principalmente cuando se trabaja con servicios, y una precisa identificación de la dimensión de la calidad por los usuarios son asuntos muy discutidos. En este sentido, definir un proceso de gestión de la calidad es importante para el mejoramiento constante del desempeño organizacional y de sus productos y servicios. Por eso, las organizaciones deben adoptar un proceso de gestión de calidad como el PO8.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"gestionar la calidad"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 17. Requisitos del negocio proceso "gestionar la calidad"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | P | Entrega de valor | S | Información |
| | | Gestión de riesgos | S | Infraestructura |
| | | | | Personas |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"gestionar la calidad"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 18. Objetivos de control proceso "gestionar la calidad"

| Objetivos de control |
|---|
| PO8.1 Sistema de Gestión de Calidad, SGC: establecer y mantener un SGC que brinde un enfoque estandarizado, formal y continuo de gestión de calidad, alineado a los requisitos de negocios. |
| PO8.2 Estándares y prácticas de calidad de las TI: identificar y mantener prácticas, procedimientos y estándares para los procesos claves de las TI, con el fin orientar la organización para alcanzar la calidad definida en el SGC. |
| PO8.3 Estándares de desarrollo y adquisición: adoptar y mantener estándares para todos los desarrollos y adquisiciones, considerando estándares de codificación, convención de nombres, formato de archivos, estándares de diseño de arquitectura y diccionarios de datos, estándares de interface de usuario, interoperabilidad, eficiencia en el desempeño de sistemas, escalabilidad, estándares de desarrollo y pruebas, validaciones comparadas con los requisitos, planes de prueba, pruebas unitarias, pruebas de regresión y pruebas integradas. |
| PO8.4 Énfasis en el cliente: asegurar que la gestión de la calidad tenga como énfasis el cliente externo e interno. Deben ser definidos roles y responsabilidades para la solución de conflictos entre los usuarios/clientes y el área de las TI. |
| PO8.5 Mejoramiento continuo: las acciones del sistema de gestión de la calidad que promueve el mejoramiento continuo es mantenido y comunicado regularmente para toda la organización. |
| PO8.6 Medición, monitoreo y revisión de la calidad: definir, planear e implementar métricas para monitorear continuamente el seguimiento al SGC, así como el valor que el brinda. Medición, monitoreo y almacenamiento de informaciones (registros) deben ser utilizados por el propietario del proceso para tomar medidas correctivas y preventivas. |

La gerencia de la calidad de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"gestionar la calidad"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"gestionar la calidad".**

### 3.1.9 Proceso PO9. Evaluar y gestionar los riesgos de las TI

Desarrollar una estructura de gestión de riesgo integrada a las estructuras corporativa y operacional de gerencia de riesgo, evaluación, mitigación y comunicación del riesgo residual, mediante:

- Garantía de que la gestión del riesgo esté completamente integrada a los procesos gerenciales, interna y externamente, y sea aplicada de forma consistente.
- Realización de evaluaciones de riesgo.
- Recomendación y comunicación de planes de acción de remediación de riesgos.

Cualquier impacto potencial sobre los objetivos de la organización, causado por un evento no planeado debe ser identificado, analizado y evaluado. Estrategias de mitigación del riesgo deben ser adoptadas para minimizar el riesgo residual a niveles aceptables.

Ejemplo: exigencias normativas crecientes, la expansión de los negocios *on-line* 7x24 y la amenaza constante de una economía incierta son factores que aumentan la importancia de la administración de riesgos en todas sus formas – sean estos relacionados a los negocios, datos o eventos. Cada vez más crecen los desafíos inherentes a los riesgos de las TI y las acciones que gerentes y directores de las TI están tomando para entender mejor, confrontar y resolver estos problemas. La administración de riesgos de las TI puede afectar directamente la posición competitiva de una organización, así como su reputación frente a clientes, socios, órganos controladores, sociedad civil y otros grupos de interés. Entender los riesgos y crear mecanismos de respuesta a ellos es fundamental para que las organizaciones se mantengan estables. En el momento en que el avance de los negocios está asociado al mundo digital, las organizaciones públicas y privadas deben adoptar políticas de prevención de riesgos. Adoptar un proceso de evaluación y gestión de riesgos de las TI como el PO9 es de vital importancia en el mundo actual.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"evaluar gestionar los riesgos de las TI"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 19. Requisitos de negocio proceso "evaluar y gestionar los riesgos de las TI"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | S | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | S | Gestión del riesgo | P | Información |
| Confidencialidad | P | | | Infraestructura |
| Integridad | P | | | Personas |
| Disponibilidad | P | | | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"evaluar y gestionar los riesgos de las TI"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 20. Objetivos de control proceso "evaluar y gestionar los riesgos de las TI"

| Objetivos de control |
|---|
| PO9.1 Alineamiento de la gestión de riesgos de las TI y del negocio: crear una estructura de gestión de riesgos de las TI alineada con la estructura de gestión de riesgos de la organización. |
| PO9.2 Establecer el contexto de riesgo: establecer el contexto en que la estructura de evaluación del riesgo es aplicada para asegurar los resultados esperados. Incluye la definición de los contextos interno y externo de cada evaluación del riesgo, el objetivo de la evaluación y los criterios a través de los cuales los riesgos son evaluados |
| PO9.3 Identificación de eventos: identificar eventos (amenaza real que explota vulnerabilidades significativas) con potencial impacto negativo sobre los objetivos o sobre las operaciones de la organización, incluyendo aspectos de negocios, reglamentación, aspectos jurídicos, tecnología, socios de negocio, recursos humanos y operacionales. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener un histórico de riesgos relevantes |
| PO9.4 Evaluación del riesgo: evaluar regularmente la probabilidad y el impacto de todos los riesgos identificados, utilizando métodos cualitativos y cuantitativos. La probabilidad de ocurrencia y el impacto asociado al riesgo (inherente y residual) deben ser determinados individualmente, por categoría y con base en el portafolio de la organización. |

Continuación tabla 20. Objetivos de control
proceso "evaluar y gestionar los riesgos de las TI"

| Objetivos de control |
| --- |
| PO9.5 Respuesta al riesgo: desarrollar y mantener un proceso de respuesta al riesgo para asegurar que los controles mitiguen de forma continua la exposición a los riesgos. El proceso de respuesta al riesgo debe identificar estrategias de riesgo, como evitar, reducir, compartir o aceptar el riesgo, determinar responsabilidades y considerar los niveles de tolerancia definidos. |
| PO9.6 Mantenimiento y monitoreo del plan de acción del riesgo: priorizar y planear las actividades de control en todos los niveles de la organización para implementar las respuestas a los riesgos. Obtener aprobación para acciones recomendadas y aceptación de cualquier riesgo residual y asegurar que las acciones aprobadas sean asumidas por los dueños de los procesos afectados. Monitorear la ejecución de planes y reportar los desvíos a la dirección de la organización. |

La evaluación y la gestión de riesgos de las TI requieren varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"evaluar y gestionar los riesgos de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"evaluar y gestionar los riesgos de las TI".**

### 3.1.10 Proceso PO10. Gestión de proyectos

Aplicar a los proyectos de las TI un programa definido y un enfoque de gestión de proyectos que permita la participación de las partes interesadas y el monitoreo del avance y de los riesgos del proyecto, mediante:

- Definición e implementación de programas, estructuras y enfoques del proyecto.
- Publicación de directrices de gestión del proyecto.
- Realización de la planeación del proyecto para todo el portafolio de proyectos.

La organización debe adoptar una metodología para la gestión de todos los proyectos de las TI. Puede ser creada una oficina de gestión de proyectos, responsable por mantener el portafolio de proyectos y acompañar la ejecución de cada proyecto.

Ejemplo: crear una oficina de proyectos es una de las alternativas que las organizaciones están siguiendo para gestionar la ejecución de los proyectos en desarrollo o futuros, conforme a lo definido en el proceso PO10.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"gestión de proyectos"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 21. Requisitos del negocio proceso "gestión de proyectos"

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | P | Entrega del valor | S | Infraestructura |
| | | Gestión de riesgos | S | Personas |
| | | Gestión de recursos | S | |
| | | Medición del desempeño | S | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"gestión de proyectos"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 22. Objetivos de control proceso "gestión de proyectos"

| Objetivos de control |
|---|
| PO10.1 Estructura de gestión de programas: mantener el programa de proyectos (conjunto de proyectos con un objetivo definido) relacionados al portafolio de programas de inversión en TI identificando, definiendo, evaluando, priorizando, seleccionando, iniciando, gestionando y controlando proyectos. Asegurar que los proyectos apoyen los objetivos de los programas. Coordinar las actividades interrelaciones de múltiples proyectos, gestionar la contribución de todos los proyectos de un programa para los resultados esperados y resolver requisitos y conflictos de recursos. |
| PO10.2 Estructura de gestión de proyectos: crear y mantener una estructura de gestión de proyectos que defina el alcance y la cobertura de los proyectos gestionados, así como los métodos a ser adoptados y aplicados a cada proyecto iniciado. |

Continuación tabla 22. Objetivos de control
proceso "gestión de proyectos"

| Objetivos de control |
|---|
| PO10.3 Enfoque de gestión de proyectos: establecer un enfoque de gestión de proyectos adecuado al tamaño, a la complejidad y a los requisitos de cada proyecto, que debe incluir los roles, las responsabilidades y el acompañamiento de los resultados del patrocinador del programa, patrocinador del proyecto, comité director, coordinador y gerente del proyecto y los mecanismos por los cuales ellos pueden cumplir con esa responsabilidad (como informes y revisiones de etapas del proyecto). Asegurar que todos los proyectos de las TI tengan patrocinadores con autoridad suficiente para ser sus propietarios dentro del programa estratégico general. |
| PO10.4 Compromiso de las partes interesadas: obtener el compromiso y participación de las partes interesadas (para quien el proyecto va a entregar los resultados esperados) afectadas en la definición y en la ejecución del proyecto, dentro del contexto del programa de inversión general de las TI. |
| PO10.5 Declaración del alcance del proyecto: definir y documentar la naturaleza y el alcance del proyecto, buscando confirmar y desarrollar un entendimiento común del alcance del proyecto con las partes interesadas, y también en relación con otros proyectos de un programa de inversiones en TI. La definición debe ser formalmente aprobada por el patrocinador del programa y por el patrocinador del proyecto, antes de su inicio. |
| PO10.6 Fase de inicio del proyecto: asegurar que la fase inicial del proyecto sea formalmente aprobada y comunicada a todas las partes interesadas. La aprobación de la fase siguiente debe ser basada en la revisión y en la aceptación de los resultados entregados de la fase anterior y en la aprobación de un caso de negocio actualizado en la próxima revisión general del programa. En el caso de una superposición de fases, se debe establecer un punto de aprobación por los patrocinadores del programa y del proyecto para autorizar la continuidad. |
| PO10.7 Plan integrado del proyecto: Establecer un plan integrado del proyecto o formalizado y aprobado (que abarque recursos de negocio y de sistemas de información) para orientar la ejecución y el control en todas las etapas del proyecto. Las actividades e interrelaciones de múltiples proyectos dentro de un programa deben ser entendidas y documentadas. El plan del proyecto debe pasar por mantenimiento durante todas las etapas del proyecto. El plan del proyecto y las alteraciones hechas en el deben ser aprobadas de acuerdo con la estructura de gobierno del programa y del proyecto. |
| PO10.8 Recursos del proyecto: definir responsabilidades, relaciones, autoridades y criterios de desempeño para los miembros del equipo del proyecto y especificar la base de adquisición y atribución de funcionarios y/o prestadores de servicio competentes para el proyecto. La contratación de productos y servicios necesarios para cada proyecto debe ser planeada y gestionada para alcanzar los objetivos del proyecto, utilizando las prácticas de contratación de la organización. |
| PO10.9 Gestión del riesgo del proyecto: eliminar o minimizar riesgos específicos asociados a cada proyecto por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de áreas o eventos con potencial para causar cambios indeseados. Los riesgos identificados por el proceso de gestión del proyecto y los resultados esperados del proyecto deben ser establecidos y registrados centralmente. |
| PO10.10 Plan de calidad del proyecto: preparar un plan de gestión de la calidad que describa el sistema de calidad de proyecto y cómo será implementado. El plan debe ser formalmente revisado y aceptado por todas las partes involucradas y debe ser incorporado al plan integrado del proyecto. |

Continuación tabla 22. Objetivos de control
proceso "gestión de proyectos"

| Objetivos de control |
|---|
| PO10.11 Control de cambios del proyecto: establecer un sistema de control de cambios para cada proyecto, de manera que todos los cambios hechos en el alcance original del proyecto (como costo, cronograma, alcance y calidad) sean debidamente revisados, aprobados e incorporados al plan integrado del proyecto, en alineamiento con la estructura de gobierno del programa y proyecto. |
| PO10.12 Planeación de métodos de validación: identificar las actividades necesarias para soportar la validación de nuevos sistemas (o sus modificaciones) durante la planeación del proyecto e incluirlas en el plan integrado del proyecto. Las tareas deben asegurar que los controles internos y aspectos de seguridad atiendan los requisitos definidos. |
| PO10.13 Medición del desempeño, monitoreo y reporte del proyecto: evaluar el desempeño del proyecto en comparación con criterios clave, como: alcance, cronograma, calidad, costo y riesgo. Identificar cualquier desvío del plan. Evaluar el impacto de las desviaciones sobre el proyecto y el programa. Reportar los resultados a las partes interesadas. Recomendar, implementar y monitorear acciones correctivas cuando sean necesarias, en alineación con la estructura de gobierno del programa y proyecto. |
| PO10.14 Cierre del proyecto: exigir que, al finalizar cada proyecto, las partes interesadas evalúen si el proyecto generó los resultados y beneficios planeados. Identificar y comunicar cualquier actividad sobresaliente para obtener los resultados esperados del proyecto y los beneficios del programa. Identificar y documentar las lecciones aprendidas para usarlas en proyectos y programas futuros. |

La gestión de proyectos de las TI requiere varias fuentes de información, que produzcan información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"gestión de proyectos"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla aún el modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"gestión de proyectos".**

## Ejercicio de refuerzo - definiendo el nivel de madurez para los procesos del dominio PO

CobiT 4.1 define para los procesos un modelo de madurez para que sea posible evaluar el nivel de madurez de la organización. Tomando como referencia el modelo de madurez de CobiT 4.1, evaluar el nivel de madurez de los procesos de PO de su organización. Utilice como referencia el marco de CobiT 4.1.

Tabla 23. Ejercicio evaluación nivel de madurez

| | Nivel de madurez | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 |
| PO1 Definir un plan estratégico de TI | | | | | | |
| PO2 Definir la arquitectura de la información | | | | | | |
| PO3 Determinar las directices de tecnología | | | | | | |
| PO4 Definir procesos, la organización y las relaciones de TI | | | | | | |
| PO5 Gestionar la inversión de TI | | | | | | |
| PO7 Gerenciar los recursos humanos de TI | | | | | | |
| PO8 Gerenciar la calidad | | | | | | |
| PO9 Evaluar y gerenciar los riesgos de TI | | | | | | |
| PO10 Gerenciar proyectos | | | | | | |

## 3.2 Dominio Adquirir e Implementar, AI.

Para ejecutar la estrategia de las TI, las soluciones de las TI necesitan ser identificadas, desarrolladas o adquiridas, implementadas e integradas a los procesos de negocio. Además de eso, cambios y mantenimiento de los sistemas existentes son cubiertas por este dominio para asegurar que las soluciones continúen atendiendo los objetivos del negocio.

En este dominio se tratan las decisiones sobre el mejor camino que la organización debe seguir para decidir entre adquirir soluciones de sistemas de información listas o desarrollar sus propios sistemas, con un equipo de desarrollo propio o externo. También son tratados en este dominio los cambios que el ambiente de las TI requiere para atender las mejoras con nuevos servicios para el negocio. Tener la garantía de que los cambios no afecten o afectarán los servicios de negocio, es uno de los factores más importantes de atención para el área de las TI.

El dominio AI ayuda a direccionar las acciones de adquisición e implementación en los siguientes aspectos:

» Garantizar que los nuevos proyectos brindarán soluciones que atiendan a las necesidades de negocios.

- Mantener una gestión activa sobre los proyectos, garantizando que los mismos serán entregados en el tiempo y el presupuesto previstos.
- Garantizar que la implementación de un nuevo sistema y la mejora de los sistemas existentes, así como de la infraestructura, se harán sin afectar los negocios, o que el riesgo sea mínimo y fácilmente solucionado.
- Proveer ambientes de desarrollo, pruebas y homologación de sistemas para tener la garantía de que las implementaciones estarán de acuerdo con lo esperado por los servicios de negocio.

El dominio Adquirir e Implementar, AI, está compuesto por siete procesos:

- AI1 Identificar soluciones automatizadas
- AI2 Adquirir y mantener software aplicativo
- AI3 Adquirir y mantener infraestructura de tecnología
- AI4 Habilitar operación y uso
- AI5 Adquirir recursos de las TI
- AI6 Gestionar cambios
- AI7 Instalar y homologar soluciones y cambios

### 3.2.1 Proceso AI1. Identificar soluciones automatizadas

Identificar soluciones técnicamente viables y con buena relación costo beneficio, mediante:

- Definición de los requisitos técnicos y de negocio.
- Realización de estudios de viabilidad conforme a lo definido en los estándares de desarrollo.
- Aprobación (o rechazo) de requisitos y resultados de estudios de viabilidad.

Este proceso contempla la definición de las necesidades, considera fuentes alternativas, la revisión de la viabilidad económica y tecnológica, la ejecución de los análisis de riesgo y de costo beneficio y la obtención de una decisión final de "desarrollar" o "comprar". Todos esos pasos permiten a las organizaciones minimizar los costos de adquisición e implementación de soluciones y el alcance de los objetivos de negocio.

Ejemplo: adoptar metodologías de desarrollo de sistemas y aplicaciones como CMMI y RUP, o adoptar una metodología propia que cumpla con las definiciones de AI1.

» CMMI, *Capability Maturity Model Integration* es un conjunto de modelos integrados de madurez y capacidad para diversas disciplinas, tales como: ingeniería de software y sistemas y fuentes de adquisición y desarrollo integrado de producto. El CMMI fue creado por *Software Engineering Institute*, SEI, siendo reconocido mundialmente por medir la madurez de los procesos de desarrollo de la organización. Reúne directrices y buenas prácticas, académicas como de mercado, las cuales deben ser incorporadas por las organizaciones en sus procesos. El CMMI ayuda a garantizar y mejorar la calidad de los productos y servicios del área de las TI.

» RUP, *Rational Unified Process* (Proceso Unificado Racional) es un proceso propietario de ingeniería de software. Creado por la *Rational Software Corporation* (adquirida por IBM), dando un nuevo nombre, IRUP, que es un abreviación de IBM *Rational Unified Process,* convirtiéndose en una marca en el área de software y brindando técnicas para ser seguidas por los miembros del equipo de desarrollo de software, con el objetivo de aumentar su productividad en el proceso desarrollo.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"identificar soluciones automatizadas"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 24. Requisitos de negocio proceso identificar soluciones automatizadas

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | S | Entrega de valor | P | Infraestructura |
| | | Gestión de riesgos | S | |
| | | Gestión de recursos | S | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"identificar soluciones automatizadas"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 25. Objetivos de control proceso identificar soluciones automatizadas

| Objetivos de control |
| --- |
| AI1.1 Definición y mantenimiento de los requisitos técnicos y funcionales del negocio: identificar, priorizar, especificar y pactar los requisitos técnicos y funcionales del negocio, cubriendo el alcance de todas las iniciativas necesarias para obtener los resultados esperados del programa de inversiones en TI. |
| AI1.2 Informe de análisis del riesgo: identificar, documentar y analizar los riesgos asociados a los requisitos del negocio y diseño de soluciones como parte del proceso de desarrollo de los requisitos de la organización |
| AI1.3 Estudio de viabilidad y formulación de acciones alternativas: desarrollar un estudio de viabilidad que examine la posibilidad de implementar los requisitos. La gerencia de negocios, soportada por el área de las TI, debe evaluar la viabilidad y las acciones alternativas y hacer recomendaciones al patrocinador del negocio |
| AI1.4 Decisión y aprobación de requisitos y estudio de viabilidad: el patrocinador de negocio aprueba y define los requisitos técnicos y funcionales del negocio, así como los informes de estudio de viabilidad en etapas clave predeterminadas. El patrocinador de negocio toma la decisión final relacionada con la selección de la solución y la forma de adquisición. |

La identificación de soluciones automatizadas de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"identificar soluciones automatizadas"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla aún el modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"identificar soluciones automatizadas"**

### 3.2.2 Proceso AI2 – Adquirir y mantener software al aplicativo

Asegurar la existencia de un proceso de desarrollo que contemple el cumplimiento de plazos y la optimización de costos, mediante:

- Traducción de los requisitos de negocio en las especificaciones del proyecto.
- Adhesión a los estándares de desarrollo en todas las modificaciones.
- Separación de las actividades de desarrollo, pruebas y operación.

Ejemplo: adoptar metodologías de desarrollo de sistemas y aplicaciones, como CMMI y RUP, o adoptar una metodología propia que cumpla con las definiciones de AI2.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"adquirir y mantener software aplicativo"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 26. Requisitos del negocio proceso adquirir y mantener software aplicativo

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | P | Entrega del valor | P | |
| Integridad | S | Gestión del riesgo | S | |
| Confiabilidad | S | | | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso "**adquirir y mantener software aplicativo**" con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 27. Objetivos de control proceso adquirir y mantener software aplicativo

| Objetivos de control |
|---|
| AI2.1 Diseño de nivel macro: traducir los requisitos de negocio en especificaciones de diseño de nivel macro para el desarrollo de sistemas, teniendo en cuenta el direccionamiento tecnológico y la arquitectura de información de la organización. Reevaluar cuando ocurren discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento. |
| AI2.2 Diseño detallado: detallar requisitos técnicos y del proyecto de sistemas. Definir los criterios de aceptación de los requisitos. Aprobar los requisitos para asegurar que estos corresponden al diseño del nivel macro. Reevaluar cuando ocurren discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento |
| AI2.3 Control y auditoría del aplicativo: asegurar que los controles de negocios sean expresados adecuadamente en los controles del aplicativo, de forma que el tiempo de respuesta de procesamiento sea correcto y que el acceso a la información sea exacto, completo, autorizado y auditable. |
| AI2.4 Seguridad y disponibilidad del aplicativo: considerar los requisitos de seguridad y disponibilidad en respuesta a los riesgos identificados alineados con la clasificación de datos, la arquitectura de seguridad de la información y el perfil de tolerancia a los riesgos de la organización. |
| AI2.5 Configuración e implementación de software aplicativo adquirido: personalizar e implementar las funcionalidades automatizadas adquiridas (compradas) para alcanzar los objetivos del negocio. |
| AI2.6 Principales actualizaciones de los sistemas existentes: seguir un proceso similar al de desarrollo de nuevos sistemas cuando ocurran grandes cambios en los sistemas existentes, que pueden resultar en cambios significativos en los diseños y o funcionamientos actuales. |
| AI2.7 Desarrollo de software aplicativo: asegurar que las funcionalidades automatizadas sean desarrolladas de conformidad con las especificaciones del diseño, estándares de desarrollo y documentación y requisitos de calidad y de autorización. Asegurar que todos los aspectos contractuales y legales sean identificados y considerados en el software aplicativo desarrollado por terceros. |
| AI2.8 Garantía de calidad de software: desarrollar y ejecutar un plan de garantía de calidad de software para obtener la calidad especificada en la definición de los requisitos de diseño y en los procedimientos y políticas de calidad de la organización. |
| AI2.9 Gestión de los requisitos de las aplicaciones: acompañar la situación individual de los requisitos (incluyendo todos los requisitos rechazados) durante el diseño, el desarrollo y la implementación, y garantizar que los cambios en los requisitos sean aprobados a través de un proceso de gestión de cambios. |
| AI2.10 Mantenimiento de software aplicativo: desarrollar la estrategia y el plan de mantenimiento de software aplicativo. |

Para adquirir y mantener software aplicativo de las TI son necesarias varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"adquirir y mantener software aplicativo"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso.

CobiT 4.1 contempla aún el modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"adquirir y mantener software aplicativo"**

### 3.2.3 Proceso AI3. Adquirir y mantener infraestructura de tecnología

Disponer plataformas apropiadas a las aplicaciones de negocio, en alineamiento con la arquitectura de las TI definida y los estándares tecnológicos, mediante:

- Preparación de un plan de adquisición tecnológica alineado con el plan de infraestructura tecnológica.
- Planeación del mantenimiento de la infraestructura.
- Implementación de controles internos, medidas de seguridad y de auditoría.

Las organizaciones deben tener procesos de adquisición, implementación y actualización de infraestructura de tecnología. Eso requiere un enfoque planificado de adquisición, mantenimiento y protección de la infraestructura, en alineamiento con las estrategias tecnológicas acordadas y la provisión de ambientes de desarrollo y pruebas. Eso asegura un soporte tecnológico continuo a las aplicaciones de negocio.

Ejemplo: elaboración de un presupuesto para adquisición de infraestructura tecnológica usada en las organizaciones públicas y privadas.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"adquirir y mantener infraestructura de tecnología"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 28. Requisitos de negocio proceso adquirir y mantener infraestructura de tecnología

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Gestión de recursos | P | Infraestructura |
| Eficiencia | P | | | |
| Integridad | S | | | |
| Disponibilidad | S | | | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"adquirir y mantener infraestructura de tecnología"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 29. Objetivos de control proceso adquirir y mantener infraestructura de tecnología

| Objetivos de control |
|---|
| AI3.1 Plan de adquisición de infraestructura tecnológica: preparar un plan de adquisición, implementación y mantenimiento de infraestructura tecnológica que satisfaga los requisitos técnicos y funcionales establecidos por el negocio y que esté de acuerdo con la dirección tecnológica de la organización. |
| AI3.2 Infraestructura de recursos, protección y disponibilidad: implementar controles internos, medidas de seguridad y auditoría durante la configuración, integración y mantenimiento de hardware y software de la infraestructura para proteger los recursos y asegurar disponibilidad e integridad. Las responsabilidades por la utilización de componentes críticos deben ser claramente definidas y entendidas por aquellos que desarrollan e integran los componentes de infraestructura. Su uso debe ser monitoreado y evaluado. |
| AI3.3 Mantenimiento de la infraestructura: desarrollar una estrategia y un plan para mantenimiento de la infraestructura y asegurar que los cambios sean controlados y alineados con los procedimientos de gestión del cambio de la organización (ventana de mantenimiento). Incluir la revisión periódica con base en las necesidades de los negocios, gestión de correcciones y estrategias de actualización, análisis de riesgos, vulnerabilidades y requisitos de seguridad. |
| AI3.4 Viabilidad del ambiente de pruebas: establecer un ambiente de desarrollo y de pruebas para proporcionar eficiencia y eficacia en las pruebas de viabilidad e integración de los componentes de la infraestructura. |

Adquirir y mantener la infraestructura de tecnología de las TI requiere varias fuentes de información, que producen información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"adquirir y mantener infraestructura de tecnología"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"adquirir y mantener infraestructura de tecnología"**

### 3.2.4 Proceso AI4 – Habilitar operación y uso

Brindar manuales de usuario, manuales operacionales y materiales de capacitación eficaces para transferir el conocimiento necesario a la operación y uso exitoso del sistema, mediante:

- Desarrollo y distribución de documentación de trasferencia de conocimiento.
- Comunicación y entrenamiento de usuarios, gerentes de negocio, equipos de soporte y equipos de operación.
- Producción de materiales de capacitación.

El conocimiento sobre nuevos sistemas debe estar disponible. Este proceso requiere la elaboración de documentación y manuales para usuarios y para la TI, y también capacitaciones para asegurar la operación apropiada de las aplicaciones y de la infraestructura.

Ejemplo: creación de una gestión de conocimiento con base en productos de GED, Gestión Electrónica de Documentos, y adopción de una estructura de capacitación para los productos y servicios de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"habilitar operación y uso"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 30. Requisitos de negocio proceso habilitar operación y uso

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | P | Entrega del valor | P | Infraestructura |
| Integridad | S | Gestión del riesgo | S | Personas |
| Disponibilidad | S | Gestión de recursos | S | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"habilitar operación y uso"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 31. Objetivos de control proceso habilitar operación y uso

| Objetivos de control |
|---|
| AI4.1 Planeación para soluciones operacionales: desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad operacional y los niveles de servicios necesarios para que todos los que van a operar, utilizar y mantener las soluciones automatizadas puedan ejercer sus responsabilidades (creación de procesos y procedimientos operacionales). |
| AI4.2 Transferencia de conocimiento a la gerencia de negocio: transferir el conocimiento (capacitación) a la gerencia de negocio para permitir que ésta asuma la propiedad del sistema y de los datos, y ejerza sus responsabilidades en los procesos de entrega, calidad de servicio, controles internos y administración de la aplicación. |
| AI4.3 Transferencia de conocimiento a los usuarios finales: trasferir conocimiento (capacitación) y habilidades para permitir a los usuarios el uso efectivo y eficiente de los sistemas y aplicativos que sustentan los procesos de negocio. |
| AI4.4 Transferencia de conocimiento a equipos de operaciones y soporte: transferir conocimiento (capacitación) y habilidades para permitir que los equipos de operaciones y soporte técnico entreguen, soporten y mantengan los sistemas y la infraestructura asociada de forma eficaz y eficiente. |

Habilitar la operación de la TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"habilitar operación y uso"** con otros procesos relacionados a los demás

dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 incluyó el modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"habilitar operación y uso".**

### 3.2.5 Proceso AI5. Adquirir recursos de las TI

Adquirir y mantener habilidades de las TI que respondan a la estrategia de entrega y a una infraestructura de las TI estandarizada e integrada, y reducir el riesgo de adquisición de recursos de las TI, mediante:

- Obtención de un concepto profesional para aspectos legales y contractuales.
- Definición de procedimientos y estándares de adquisición.
- Adquisición de hardware, software y servicios requeridos en alineamiento con los procedimientos definidos.

Las organizaciones públicas colombianas deben seguir las orientaciones de la Ley 80 de 1993 modificada por la Ley 1150 de 2007 que regula las adquisiciones de la administración pública. Otra disposición del gobierno nacional muy relacionada es la Ley 1474 de 2011 (Estatuto Anticorrupción), así mismo el Estado colombiano ha venido desarrollando los lineamientos para que las entidades puedan realizar las adquisiciones de recursos de TI a través de mecanismos colectivos entre los que se destacan los Acuerdos marco de precios y adquisiciones en modalidad de servicio y/o por demanda.

Ejemplo: estas actividades son ejecutadas por las áreas jurídicas, de compras y de contratos de las organizaciones, con el soporte técnico del área de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"adquirir recursos de las TI"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 32. Requisitos de negocio proceso adquirir recursos de las TI

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | S | Entrega del valor | S | Aplicaciones |
| Eficiencia | P | Gestión de recursos | P | Información |
| Conformidad | S | | | Infraestructura |
| | | | | Personas |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"adquirir recursos de las TI"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 33. Objetivos de control proceso adquirir recursos de las TI

| Objetivos de control |
|---|
| AI5.1 Control de adquisición: desarrollar y acompañar un conjunto de procedimientos y estándares consistentes con el proceso y la estrategia corporativa de adquisición para asegurar que la adquisición de infraestructura, instalaciones, hardware, software y servicios satisfagan los requisitos de negocio. |
| AI5.2 Gestión de contratos de proveedores: instituir un procedimiento para establecer, modificar y finalizar contratos con todos los proveedores. Todos los contratos y las respectivas modificaciones deben ser revisados por consultores legales. |
| AI5.3 Selección de proveedores: seleccionar proveedores de acuerdo con la práctica formal y con las leyes y reglamentos, con base en los requisitos definidos a partir de la información dada por proveedores en potencia y acordadas entre proveedores y clientes. |
| AI5.4 Adquisición de recursos de las TI: garantizar que los intereses de la organización sean protegidos en todos los contratos de adquisición. Incluir e imponer los derechos y las obligaciones de todas las partes, en los términos contractuales de adquisición de software, desarrollo de recursos, infraestructura y servicios. |

Adquirir recursos de las TI de la organización requiere varias fuentes de información, que producen información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"adquirir recursos de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"adquirir recursos de las TI".**

### 3.2.6 Proceso AI6. Gestión de cambios

Controlar la evaluación de impacto, la autorización y la implementación de todas las modificaciones en la infraestructura, en las aplicaciones y en las soluciones técnicas de las TI, minimizar errores debido a especificaciones incompletas de requisitos e interrumpir la implementación de cambios no autorizados, mediante:

- Definición y comunicación de procedimientos de cambio, incluyendo cambios de emergencia.
- Evaluación, priorización y autorización de cambios.
- Seguimiento al estado de los cambios y a los reportes presentados sobre los cambios.

Todos los cambios, incluyendo mantenimientos y correcciones de emergencia, relacionados con la infraestructura y las aplicaciones en el ambiente de producción son formalmente gestionados de manera controlada. Los cambios (incluyendo procedimientos, procesos, parámetros de sistemas y de servicio) deben ser registrados, evaluados y autorizados antes de su implementación y posteriormente revisados, teniendo como base los resultados efectivos contra los planeados. Esto asegura la mitigación de riesgos de impacto negativo en la estabilidad o en la integridad del ambiente de producción.

Ejemplo: reuniones periódicas para priorizar las solicitudes de cambios, de acuerdo con la realidad de los negocios y conforme a lo definido en el proceso de gestión de cambios AI6.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"gestión de cambios"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 34. Requisitos de negocio proceso gestión de cambios

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Entrega del valor | S | Aplicaciones |
| Eficiencia | P | Gestión de recursos | P | Información |
| Integridad | P | | | Infraestructura |
| Disponibilidad | P | | | Personas |
| Confiabilidad | S | | | |

Nomenclatura: Primario P; Secundario S

CobiT 4.1 define los siguientes objetivos de control para el proceso "**gestión de cambios**" con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 35. Objetivos de control proceso gestión de cambios

| Objetivos de control |
|---|
| AI6.1 Estándares y procedimientos de cambio: crear procedimientos formales de gestión de cambios (SDC, Solicitud de Cambio) para actuar de modo estandarizado con todas las solicitudes de cambio en aplicaciones, procedimientos, procesos, parámetros de sistema y de servicio y plataformas subyacentes (inclusive solicitudes de mantenimiento y reparación). |
| AI6.2 Evaluación de impacto, priorización y autorización: evaluar todas las solicitudes de cambio de modo estructurado, con relación a impactos en el sistema operacional y en la respectiva funcionalidad. Asegurar que todos los cambios sean categorizados, priorizados y autorizados. |
| AI6.3 Cambios de emergencia: crear un proceso especial para definición, solicitud, pruebas, documentación, evaluación y autorización de cambios de emergencia que no sigan el proceso de cambio normal establecido. |
| AI6.4 Seguimiento y reporte del estado de los cambios: crear un sistema de acompañamiento e informe de cambios para documentar cambios rechazados, comunicar el estatus de cambios aprobados y en trámite y ejecutar cambios. Garantizar que los cambios autorizados sean implementados conforme a lo planeado |
| AI6.5 Finalización de cambios y documentación: actualizar la documentación y los procedimientos de sistemas y usuarios, siempre que sean implementados cambios en el sistema y en el ambiente tecnológico. |

Gestionar cambios en el ambiente de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del

proceso **"gestión de cambios"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"gestión de cambios".**

### 3.2.7 Proceso AI7. Instalar y homologar soluciones y cambios

Probar que las aplicaciones y las soluciones de infraestructura se ajustan al propósito pretendido y están libres de errores, y planear la implementación y la migración para producción, mediante:

- Establecimiento de una metodología de pruebas.
- Realización de la planeación de liberación para producción.
- Evaluación y aprobación de los resultados de las pruebas por los responsables de la gerencia del negocio.
- Realización de revisiones después de la implementación.

Nuevos sistemas necesitan ser colocados en operación, una vez concluye su desarrollo. Es necesario realizar pruebas apropiadas en un ambiente dedicado, con datos de prueba relevantes, la definición de instrucciones de implantación y migración, la planeación de liberación y de cambios en el ambiente de producción, además de una revisión pos implementación. Estas medidas aseguran que los sistemas operacionales estén alineados con las expectativas y los resultados acordados.

Ejemplo: actividad ejecutada por el área técnicas de las TI, de acuerdo con el proceso AI7

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"instalar y homologar soluciones y cambios"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos de negocios sean alcanzados.

Tabla 36. Requisitos de negocio proceso instalar y homologar soluciones y cambios

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | S | Entrega del valor | P | Información |
| Integridad | S | Gestión de riesgos | S | Infraestructura |
| Disponibilidad | S | Gestión de recursos | S | Personas |
| | | Medición del desempeño | S | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 define los siguientes objetivos de control para el proceso **"instalar y homologar soluciones y cambios"** con el fin de garantizar que los objetivos de negocios sean alcanzados y los eventos indeseables sean tratados de forma adecuada.

Tabla 37. Objetivos de control proceso instalar y homologar soluciones y cambios

| Objetivos de control |
|---|
| AI7.1 Capacitaciones: capacitar el equipo de los departamentos, usuarios involucrados y los equipos de operaciones de las TI sobre todos los cambios que ocurren en el ambiente de las TI y que están asociados o no a los servicios del negocio. |
| AI7.2 Plan de pruebas: crear un plan de pruebas para los cambios implementados y asegurar que sea aprobado por todos los que soliciten cambios, por el área de negocios y por el área de las TI. |
| AI7.3 Plan de implementación: crear un plan de implementación y de retorno a la configuración anterior. Obtener aprobación de todos los involucrados en los cambios. |
| AI7.4 Ambiente de pruebas: crear un ambiente de pruebas seguro que refleje el ambiente de operaciones en lo relacionado a la seguridad, controles internos, prácticas operacionales, exigencias de calidad y confidencialidad y cargas de trabajo. |
| AI7.5 Conversión de datos y sistemas: planear la conversión de datos y la migración de la infraestructura como parte de los métodos de desarrollo de la organización, incluyendo pistas de auditoría, procedimientos de retorno a la situación anterior y de recuperación de fallas. |
| AI7.6 Prueba de cambios: asegurar que los cambios sean probados de manera independiente y de acuerdo con el plan de pruebas definido antes de la migración al ambiente de producción. |

Continuación tabla 37. Objetivos de control proceso instalar y homologar soluciones y cambios

| Objetivos de control |
|---|
| AI7.7 Prueba de aceptación final: asegurar que el área usuaria del área de las TI evalúe los resultados del proceso de pruebas, conforme a lo determinado en el plan de pruebas. Corregir errores significativos identificados en el proceso de pruebas, ejecutar todas las pruebas listadas en el plan de pruebas, así como cualquier prueba de regresión necesaria. Después de la evaluación, aprobar la liberación para la producción. |
| AI7.8 Liberación para producción: después de la conclusión de las pruebas, controlar la transferencia de los sistemas modificados hacia la operación, de acuerdo con el plan de implementación. Obtener la aprobación de todos los involucrados, tales como usuarios, propietarios de sistema y gerencia operacional. Cuando sea apropiado, ejecutar el sistema en paralelo con el antiguo sistema durante un periodo y comparar comportamiento/resultados |
| AI7.9 Revisión pos implementación: crear procedimientos alineados con la gestión de cambios organizacionales, para garantizar la realización de la revisión pos implementación, conforme a lo definido en el plan de implementación. |

Instalar y homologar soluciones y cambios de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio conjunto de relaciones de entrada y salida del proceso **"instalar y homologar soluciones y cambios"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 contempla un modelo de madurez para evaluar el nivel de madurez de la organización en relación al proceso **"instalar y homologar soluciones y cambios".**

## Ejercicio de refuerzo - definiendo el nivel de madurez para los procesos de dominio AI

CobiT 4.1 define un modelo de madurez para los procesos, haciendo posible la evaluación del nivel de madurez de la organización. Tomando como referencia el modelo de madurez de CobiT 4.1, evalúe el nivel de madurez de los procesos AI de su organización. Utilice como referencia el marco de CobiT 4.1.

| | Nivel de madurez | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 |
| AI1 Idetificar soluciones automatizadas | | | | | | |
| AI2 adquirir y mantener software aplicativo | | | | | | |
| AI3 adquirir y mantener infrastructura de tecnología | | | | | | |
| AI4 Habilitar operación y uso | | | | | | |
| AI5 Adquirir recursos de las TI | | | | | | |
| AI6 Gestionar cambios | | | | | | |
| AI7 Instalar y homologar soluciones y cambios | | | | | | |

## Lo que se aprendió

- Procesos de dominio PO
  - PO1. Definir un plan estratégico de las TI
  - PO2. Definir la arquitectura de la información.
  - PO3. Determinar las directrices de tecnología.
  - PO4. Definir los procesos, organizaciones y relaciones de las TI.
  - PO5. Gestión de la inversión en TI.
  - PO6. Comunicar metas y directrices gerenciales.
  - PO7. Gestionar los recursos humanos de las TI.
  - PO8. Gestión de la calidad.
  - PO9. Evaluar y gestionar los riesgos de las TI.
  - PO10. Gestión de proyectos.
- Procesos de dominio AI
  - AI1 Identificar soluciones automatizadas
  - AI2 Adquirir y mantener software aplicativo
  - AI3 Adquirir y mantener infraestructura de tecnología
  - AI4 Habilitar operación y uso
  - AI5 Adquirir recursos de las TI
  - AI6 Gestionar cambios
  - AI7 Instalar y homologar soluciones y cambios

Capítulo

04

# Estudio de los dominios DS y ME de CobiT

**Objetivos**

Comprender los dominios: Entregar y Soportar, DS y Monitorear y Evaluar, ME y los procesos involucrados.

**Conceptos**

Dominio: Entregar y Soportar, DS, y sus 13 procesos y dominio: Monitorear y Evaluar, ME y sus cuatro procesos.

# Introducción

El modelo de gobierno de las TI recomendado por CobiT 4.1 es utilizado actualmente por las organizaciones para estructurar el área de las TI y para que ésta soporte adecuadamente servicios del negocio. La estructura de CobiT 4.1 direcciona el área de las TI para ejecutar su actividad orientada a los procesos, proporcionando mejora en los servicios que TI brinda a la organización.

Así, el área de las TI debe entregar y soportar todos los servicios de negocio de la organización, manteniendo los niveles de operación de la infraestructura de las TI con la disponibilidad y capacidad exigidas por el negocio. Monitorear constantemente los servicios de las TI y los procesos asociados para proveer una mejora constante, debe ser un objetivo alcanzado por la implementación del gobierno TI.

Esta sección trata el tema de los dominios: Entregar y Soportar, DS y Monitorear y Evaluar, ME, abordando los principales asuntos relacionados, como recursos, criterios de información, y áreas de énfasis del gobierno de las TI.

## 4.1 Dominio: Entregar y Soportar, DS.

Este dominio comprende la entrega de los servicios solicitados, lo que incluye entrega de servicio, gestión de la seguridad y continuidad, servicios de soporte para los usuarios y la gestión de datos y recursos operacionales. Todas las actividades operacionales de las TI son contempladas por los procesos del dominio: DS, o sea, nada funciona correctamente si estos procesos no están implementados.

Establecer adecuadamente la entrega y soporte de los servicios que la organización necesita puede ser alcanzado por medio de los procesos del dominio: DS en los siguientes aspectos:

- Entregar los servicios de las TI de acuerdo con las prioridades y las necesidades de los negocios.
- Evaluar si los costos de las TI están optimizados y que no se presente desperdicio o falta de capacidad de recursos de las TI.
- Garantizar que los usuarios de negocio de la organización estén habilitados para utilizar el sistema de las TI de manera productiva segura.
- Evaluar si los aspectos de confidencialidad, integridad y disponibilidad están siendo contemplados para garantizar la seguridad de la información.

El dominio: Entregar y Soportar, DS, es compuesto por 13 procesos:

- DS1 Definir y gestionar niveles de servicios
- DS2 Gestionar servicios tercerizados
- DS3 Gestionar el desempeño y la capacidad
- DS4 Asegurar la continuidad de los servicios
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar los usuarios
- DS8 Gestionar el centro de servicio y los incidentes
- DS9 Gestionar la configuración
- DS10 Gestionar problemas
- DS11 Gestionar los datos
- DS12 Gestionar el ambiente físico
- DS13 Gestionar las operaciones

### 4.1.1 Proceso DS1. Definir y gestionar niveles de servicios

Identificar los requisitos de los servicios, establecer los Acuerdos de Niveles de Servicio, ANS, y monitorear la atención de los niveles de servicio, se alcanza mediante:

- Formalización de los ANS internos y externos alineados con los requisitos y con la capacidad de entrega.
- Comunicar a las áreas de negocio y de las TI sobre los niveles de servicio acordados (reuniones, informes)
- Identificación y comunicación de los requisitos de servicios nuevos y actualización de requisitos de servicios existentes para la planeación estratégica.

La gestión del nivel de servicio es la función central de la gestión de servicios de las TI. Responsable por el control cuantitativo y cualitativo de los servicios prestados a los usuarios de negocio.

El proceso de gestión de niveles de servicio consiste en un conjunto de procesos, procedimientos y herramientas aplicados para:

- Crear el catálogo de servicios
- Planificar los ANS
- Elaborar los ANS
- Monitorear los ANS
- Informar los ANS
- Revisar los ANS

Este proceso también incluye el monitoreo y la elaboración de informes sobre la atención de los niveles de servicio, permitiendo el alineamiento entre los servicios de las TI y los requisitos de negocio.

Los acuerdos de niveles de servicio están compuestos por:

- Acuerdos de Nivel Operacional, OLA (*Operational Level Agreements*): acuerdos con las diferentes áreas de las TI responsables por el servicio.
- Contrato con terceros.

Ejemplo: establecer criterios para el tiempo de atención de solicitudes para los servicios de las TI. El catálogo de servicios debe ser construido con base en el entendimiento de lo que TI puede ofrecer al negocio. También está asociado al nivel de servicio y a la disponibilidad de cada servicio de las TI que se brinda al negocio.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"definir y gestionar niveles de servicio"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 38. Requisitos de negocio proceso definir y gestionar niveles de servicio

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | P | Entrega del valor | P | Información |
| Confidencialidad | S | Gestión de recursos | P | Infraestructura |
| Integridad | S | Medición del desempeño | P | Personas |
| Disponibilidad | S | | | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"definir y gestionar niveles de servicio"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 39. Objetivos de control proceso definir y gestionar niveles de servicio

| Objetivos de control |
|---|
| DS1.1 Estructura de gestión de niveles de servicio: definir un modelo formal de gestión de niveles de servicio entre el cliente y el área de las TI. Este proceso debe mantener un continuo alineamiento entre los requisitos del negocio y sus prioridades. El modelo debe incluir procesos para crear requisitos de servicio, definiciones de servicio, ANS, OLA y recursos financieros, que deberán ser organizados en un catálogo de servicios, contemplando los cargos, las tareas y las responsabilidades de las áreas de las TI y de los proveedores de servicios externos. |
| DS1.2 Definición de servicios: basar la definición de servicios de las TI en las características del servicio y en los requisitos de negocio, organizados y almacenados centralizadamente por medio de la implementación de un enfoque de catálogo/portafolio de servicios. |
| DS1.3 Acuerdos de nivel de servicios, ANS: definir y negociar los acuerdos de nivel de servicios para todos los servicios críticos de las TI, con base en los requisitos del cliente y en la capacidad de entrega por parte de las TI. Esto incluye el compromiso con el cliente, requisitos de soporte para la atención de servicios, métricas cuantitativas y cualitativas de servicios aprobadas por las partes autorizadas, garantía de recursos financieros y acuerdos comerciales (cuando aplica), cargos y responsabilidades, incluyendo la supervisión del ANS. Los elementos a considerar son: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de la continuidad, seguridad y restricciones en cuanto a demanda. |

Continuación tabla 39. Objetivos de control proceso definir y gestionar niveles de servicio

| Objetivos de control |
| --- |
| DS1.4 Acuerdos de Nivel Operacional, OLA: asegurar que los OLAs expliquen la forma en que los servicios serán realizados técnicamente, con el fin de apoyar los Niveles de Servicio Acordados, SLAs, "por sus siglas en inglés", adecuadamente. |
| DS1.5 Monitoreo e informe de las realizaciones de nivel de servicio: monitorear continuamente los criterios de desempeño de los niveles de servicio especificados y crear informes de seguimiento. Las estadísticas de monitoreo son analizadas, y medidas de gestión son tomadas para identificar las tendencias negativas y positivas de cada servicio y de los servicios en conjunto. |
| ADS1.6 Revisión de los ANS y de los contratos: periódicamente realizar un análisis crítico de los acuerdos de nivel de servicios y de los contratos con los proveedores de servicios internos y externos, para asegurarse de que son eficaces y actualizados, y que los cambios en requisitos hayan sido considerados |

La definición y gestión de niveles de servicio de las TI requiere varias fuentes de información, y produce información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada–salida del proceso **"definir y gestionar niveles de servicio"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de evaluación de madurez de la organización, relacionado con el proceso **"definir y gestionar niveles de servicio"**

### 4.1.2 Proceso DS2. Gestionar servicios externalizados

Establecer relaciones y responsabilidades con prestadores externos de servicios y monitorear la entrega de los servicios para verificar y asegurar el cumplimiento de los acuerdos, mediante:

- Identificación y categorización de los proveedores de servicios.
- Identificación y reducción de los riesgos asociados al proveedor.
- Monitoreo y medición del desempeño del proveedor.

Este proceso es realizado definiendo claramente los roles, responsabilidades y expectativas en los acuerdos de externalización, así como revisando y monitoreando tales acuerdos en cuanto a su efectividad y conformidad. La gestión eficaz de los servicios externalizados minimiza los riesgos de negocio asociados a los proveedores que no cumplen el contrato de prestación de servicios.

Ejemplo: las áreas de compras y de contratos de una organización son responsables por la gestión de contratos con terceros. El área de las TI se relaciona con los terceros y proveedores soportados por estas dos áreas.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestionar servicios externalizados"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 40. Requisitos de negocio proceso gestionar servicios externalizados

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Entrega del valor | P | Aplicaciones |
| Eficiencia | P | Gestión de riesgos | P | Información |
| Confidencialidad | S | Gestión de recursos | S | Infraestructura |
| Integridad | S | Medición del desempeño | S | Personas |
| Disponibilidad | S | | | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestionar servicios externalizados"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 41. Objetivos de control proceso gestionar servicios externalizados

| Objetivos de control |
|---|
| DS2.1 Identificación de relaciones con todos los proveedores: Identificar todos los servicios tercerizados y categorizarlos de acuerdo con el tipo, la importancia y la criticidad. Mantener documentos formales de las relaciones técnicas y organizacionales, contemplando roles y responsabilidades, metas, productos esperados y las credenciales de los representantes de los proveedores. |
| DS2.2 Gestión de relaciones con los proveedores: formalizar el proceso de gestión de relaciones con cada proveedor. |
| DS2.3 Gestión de riesgos del proveedor: identificar y minimizar los riesgos relacionados a las capacidades de los proveedores de prestación de servicios de forma continua, segura y eficiente. Garantizar que los contratos estén acordes a los estándares universales del negocio y conforme a las exigencias legales y regulatorias. La gestión del riesgo debe contemplar acuerdos de confidencialidad, condiciones generales y garantías de contrato, viabilidad de continuidad del proveedor, conformidad con requisitos de seguridad, proveedores alternativos, penalidades, gratificaciones etc. |
| DS2.4 Monitoreo del desempeño del proveedor. Establecer un proceso para monitorear la prestación del servicio con el fin de asegurar que el proveedor atienda los requisitos actuales de negocio, obedeciendo los contratos y acuerdos de nivel de servicios firmados, y que su desempeño sea competitivo con otros prestadores y condiciones de mercado |

La gestión de servicios externalizados de las TI requiere varias fuentes de información, y produce información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada–salida del proceso **"gestionar servicios externalizados"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de evaluación de madurez de la organización, relacionado con el proceso **"gestionar servicios externalizados".**

### 4.1.3 Proceso DS3. Gestionar el desempeño y la capacidad

Optimizar el desempeño de la infraestructura, de los recursos y de las capacidades de las TI en respuesta a las necesidades del negocio, atendiendo los requisitos de tiempo de respuesta de los diversos acuerdos de nivel de servicios, minimizando el periodo de indisponibilidad y proporcionando mejoras continuas en el desempeño y en la capacidad de las TI, por medio del monitoreo y la medición, mediante:

» Planeación y oferta de capacidad y disponibilidad de los sistemas.

» Monitoreo e informe del desempeño de los sistemas.
» Modelaje y previsión del desempeño de los sistemas.

La necesidad de gestionar el desempeño y la capacidad de los recursos de las TI requiere un proceso que realice análisis críticos periódicos del desempeño y de las capacidades actuales de los recursos de las TI. Este proceso incluye la previsión de necesidades futuras, con base en requisitos de carga de trabajo, almacenamiento y contingencia. Este proceso asegura que los recursos de información que soportan los requisitos de negocio estén siempre disponibles.

Ejemplo: el monitoreo de las capacidades y del desempeño de la arquitectura de las TI debe garantizar la disponibilidad de los servicios para el negocio. En las organizaciones, las áreas de las TI disponen de grupos de profesionales para realizar este proceso.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestionar el desempeño y la capacidad"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 42. Requisitos de negocio proceso gestionar el desempeño y la capacidad

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | P | Entrega del valor | S | Infraestructura |
| Disponibilidad | S | Gestión de riesgos | S | |
| | | Gestión de recursos | P | |
| | | Medición del desempeño | S | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestionar el desempeño y la capacidad",** con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 43. Objetivos de control proceso gestionar el desempeño y la capacidad

| Objetivos de control |
|---|
| DS3.1 Desempeño y planeación de la capacidad: establecer planificación para la realización de un análisis crítico del desempeño y de la capacidad de los recursos de las TI, con el fin de asegurar que con costos justificables el desempeño y la capacidad estén disponibles para procesar la carga de servicio acordada, conforme a lo determinado en los acuerdos de nivel de servicio. Los planes de capacidad y desempeño deben considerar técnicas de modelaje apropiadas para producir modelos de capacidad y desempeño actuales y futuros de recursos de las TI. |
| DS3.2 Capacidad y desempeño actuales: realizar un análisis crítico del desempeño y de la capacidad actual de los recursos de las TI con el fin de determinar si existe capacidad y desempeño suficientes para la atención conforme a los niveles de servicio acordados. |
| DS3.3 Capacidad y desempeño futuros: realizar regularmente la previsión de desempeño y capacidad de los recursos de las TI con el fin de minimizar el riesgo de interrupción de servicios debido a la capacidad insuficiente o a la degradación del desempeño. Identificar el exceso de capacidad para posible reordenamiento. Identificar las tendencias de carga de trabajo para realizar previsiones para orientar el plan de capacidad y desempeño. |
| DS3.4 Disponibilidad de recursos de las TI: brindar la capacidad y el desempeño necesarios, teniendo en consideración aspectos como cargas normales de trabajo, contingencias, requisitos de almacenamiento y ciclos de vida de recurso de las TI. Se deben ser tomar medidas cuando el desempeño y la capacidad no estén alineados con el nivel necesario (por ejemplo: priorizar tareas, mecanismos de tolerancia a fallas y prácticas de asignación de recursos). La organización debe asegurar que los planes de contingencia viabilicen apropiadamente la disponibilidad, la capacidad y el desempeño de cada recurso de las TI. |
| DS3.5 Monitoreo e informes: monitorear constantemente el desempeño y la capacidad de los recursos de las TI. Los datos acumulados deben atender a dos propósitos:<br>» Mantener y sintonizar el desempeño actual en el entorno de las TI y atender asuntos como la capacidad de recuperación, la contingencia, las cargas de trabajo actual y previsto, la planeación de almacenamiento y la adquisición de recursos.<br>» informar sobre la disponibilidad de servicios prestados al negocio conforme a lo determinado por la SLAs. Acompañar todos los informes de excepciones con recomendaciones de acciones correctivas. |

Gestionar el desempeño y la capacidad del entorno tecnológico de la organización necesita varias fuentes de información, y produce información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"gestionar el desempeño y la capacidad"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de evaluación de madurez de la organización, relacionado con el proceso **"gestionar el desempeño y la capacidad"**.

### 4.1.4 Proceso DS4. Asegurar la continuidad de los servicios

Asegurar un impacto mínimo en los negocios en el caso de una interrupción de los servicios de TI, incorporando la capacidad de recuperación en soluciones automatizadas y desarrollar, mantener y probar los planes de continuidad, mediante:

- Desarrollo, mantenimiento y mejora de la contingencia de las TI.
- Entrenamiento y prueba de planes de contingencias de las TI.
- Almacenamiento de copias de datos y de los planes de contingencia en lugares remotos (*offside*).

El objetivo del proceso, de asegurar la continuidad de los servicios, es soportar el desarrollo de la gestión de la continuidad de los negocios de la organización, garantizando que todas las instalaciones de las TI (técnicas y de servicios) puedan ser recuperadas dentro de los plazos acordados. Un proceso eficaz de continuidad de servicios minimiza la probabilidad y el impacto de una interrupción de un servicio clave de las TI en las funciones y procesos críticos del negocio.

Ejemplo: el plan de contingencia de arquitectura de las TI de las organizaciones es uno de los insumos para garantizar la continuidad de los servicios de las TI y del negocio.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que el proceso **"asegurar la continuidad de los servicios"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados

Tabla 44. Requisitos de negocio proceso asegurar la continuidad de los servicios

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | S | Entrega del valor | P | Información |
| Disponibilidad | P | Gestión de riesgos | P | Infraestructura |
| | | Gestión de recursos | S | Personas |
| | | Medición del desempeño | S | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"asegurar la continuidad de los servicios"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 45. Objetivos de control proceso asegurar la continuidad de los servicios

| Objetivos de control |
|---|
| DS4.1 Estructura de continuidad: desarrollar un modelo de continuidad de las TI con el fin de soportar la gestión de continuidad del negocio de toda la organización por medio de un proceso consistente. El modelo debe orientar a la organización en relación a la gestión de continuidad, contemplando roles, tareas y responsabilidades de los proveedores de servicios internos y externos, sus gestiones, clientes y las reglas y estructuras para documentar, probar y ejecutar planes de recuperación de desastres y continuidad de las TI. El plan también debe tratar factores como identificación de recursos críticos, monitoreo e informes de disponibilidad de recursos críticos, procesamiento alternativo y principios de copia de seguridad (*backup*) y recuperación. |
| DS4.2 Planes de continuidad de las TI: desarrollar planes de continuidad de las TI con base en la estructura y diseñados para reducir el impacto de una gran interrupción de funciones y procesos fundamentales. Los planes deben ser basados en comprender el riesgo de posibles impactos en el negocio, contemplando los requisitos de capacidad de restablecimiento, procesamiento alternativo y capacidad de recuperación de los servicios críticos de las TI. También deben abarcar manuales de uso, roles, responsabilidades, procedimientos, procesos de comunicación y enfoques de pruebas. |
| DS4.3 Recursos críticos de las TI: dar atención especial a los elementos más críticos en el plan de continuidad de las TI para asegurar la capacidad de restablecer y definir prioridades en situaciones de recuperación. Prevenir el desvío de atención hacia los elementos de recuperación menos críticos y asegurar la respuesta y la recuperación en alineamiento con las necesidades del negocio de mayor importancia; al mismo tiempo, asegurar que los costos sean mantenidos en un nivel aceptable y conformes a los requisitos contractuales y regulatorios. Considerar la capacidad de restauración y los requisitos de respuesta y recuperación en diferentes niveles (por ejemplo de 1 a 4 horas, de 4 a 24 obras, más de 24 horas y los periodos operacionales críticos del negocio). |
| DS4.4 Mantenimiento del plan de continuidad de las TI: fortalecer la gestión de las TI para definir y ejecutar procedimientos de control de cambios y asegurar que el plan de continuidad de las TI se mantenga actualizado y refleje siempre los requisitos de negocios actuales. Es esencial que los cambios en los procedimientos y responsabilidades sean comunicados claramente y de forma oportuna. |
| DS4.5 Prueba del plan de continuidad de las TI: probar el plan de continuidad de las TI regularmente para asegurar que los sistemas de las TI puedan ser efectivamente recuperados, que las desviaciones sean tratadas y que el plan se mantenga actualizado. Para esto, son necesarios: preparación cuidadosa, documentación, registro de los resultados de pruebas e implementación de planes de acción de acuerdo con los resultados. También se debe considerar extender las pruebas de recuperación a aplicaciones aisladas en escenarios de pruebas extremo a extremo integrados con los proveedores. |

Continuación tabla 45. Objetivos de control proceso asegurar la continuidad de los servicios

| Objetivos de control |
|---|
| DS4.6 Entrenamiento del plan de continuidad de las TI: asegurar que todas las partes involucradas recibirán entrenamiento regular sobre los procedimientos, roles y respectivas responsabilidades en el caso de un incidente o desastre. Verificar e intensificar el entrenamiento de acuerdo con los resultados de las pruebas de continuidad. |
| DS4.7 Distribución del plan de continuidad: definir y gestionar una estrategia de distribución para asegurar que los planes sean divulgados y que estén apropiadamente disponibles para las partes interesadas y autorizadas, cuando y donde sea necesario. Toda la atención debe ser dirigida para que el plan se encuentre disponible en todos los escenarios de desastre. |
| DS4.8. Recuperación y reanudación de los servicios de las TI: planificar las acciones a ser ejecutadas en los momentos de recuperación y reanudación de los servicios de las TI. Esto puede incluir la activación de sitios alternos, inicio de procesamiento en un centro alterno, comunicación a las partes interesadas y clientes y procedimientos de retorno a la producción. Asegurar que el negocio entienda el tiempo de recuperación de las TI y las inversiones tecnológicas necesarias para sustentar las necesidades de recuperación y retorno a la producción. |
| DS4.9 Almacenamiento de copias de seguridad en lugares remotos: almacenar en sitio remoto todos los medios de copias de seguridad críticas, documentación y otros recursos de las TI, necesarios para la recuperación de las TI y los planes de continuidad de negocio. El contenido almacenado en las copias de seguridad debe ser determinado conjuntamente entre los propietarios de los procesos de negocio y el personal de las TI. La gestión de las instalaciones de almacenamiento remotas debe seguir las políticas de clasificación de datos y prácticas de almacenamiento de medios de la organización. La gestión de las TI debe asegurar que las condiciones de los lugares de almacenamiento remotos sean periódicamente evaluadas, por lo menos anualmente, en los requisitos de contenido, protección ambiental y seguridad. Asegurar la compatibilidad de hardware y software para restaurar los datos archivados y probar y actualizar periódicamente los datos archivados. |
| DS4.10 Revisión posterior a la reanudación de los servicios: con la reanudación exitosa de la función de TI después de un desastre, determinar si la gestión de TI cuenta con procedimientos para evaluar lo adecuado del plan actual y realizar su actualización de ser necesario. |

Asegurar la continuidad de los servicios de las TI de la organización requiere varias fuentes de información, y produce información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"asegurar la continuidad de los servicios"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso.

CobiT 4.1 también presenta un modelo de evaluación de madurez de la organización, relacionado con el proceso **"asegurar la continuidad de los servicios".**

### 4.1.5 Proceso DS5. Garantizar la seguridad de los sistemas

Mantener la integridad de la infraestructura de información y de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad definiendo políticas, procedimientos y estándares de seguridad de las TI, y monitorear, detectar, reportar y solucionar vulnerabilidades e incidentes de seguridad, mediante:

- Comprensión de los requisitos, vulnerabilidades y amenazas de seguridad.
- Gestión estandarizada de las identidades y autorizaciones de los usuarios.
- Pruebas periódicas de seguridad.

La gestión de seguridad incluye el monitoreo, la prueba periódica y la implementación de acciones correctivas de las deficiencias o los incidentes de seguridad. La gestión eficaz de seguridad protege todos los activos de TI y minimiza el impacto sobre los negocios de las vulnerabilidades e incidentes de seguridad.

Ejemplo: las organizaciones implementan la seguridad de TI basadas en una política de seguridad de la información que debe ser implementada en toda la organización, apoyada por la alta dirección.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de TI y los recursos de TI que el proceso **"garantizar la seguridad de los sistemas"** busca satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 46. Requisitos de negocio proceso garantizar la seguridad de los sistemas

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Confidencialidad | P | Gestión de riesgos | P | Aplicaciones |
| Integridad | P | | | Información |
| Disponibilidad | S | | | Infraestructura |
| Conformidad | S | | | Personas |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"garantizar la seguridad de los sistemas"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 47. Objetivos de control proceso garantizar la seguridad de los sistemas

| Objetivos de control |
|---|
| DS5.1 Gestión de la seguridad de las TI: gestionar la seguridad de las TI al más alto nivel organizacional de la organización, de forma tal que la gestión de las acciones de seguridad esté alineada con los requisitos del negocio. |
| DS5.2 Plan de seguridad de las TI: traducir los requisitos del negocio, de riesgo y conformidad, en un amplio plan de seguridad de las TI, que tenga en consideración la infraestructura de las TI y la cultura de seguridad. El plan debe ser implementado en políticas y procedimientos de seguridad, en conjunto con las inversiones adecuadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad deben ser comunicados a los usuarios y partes interesadas. |
| DS5.3 Gestión de identidad: todos los usuarios (internos, externos y temporales) y sus actividades en el sistema de las TI (aplicación del negocio, desarrollo, operación y mantenimiento de sistemas) deben ser identificables de modo exclusivo. Los derechos de acceso de los usuarios a los sistemas y datos deben estar en conformidad con las necesidades del negocio y con los requisitos de función definidos y documentados. Los derechos de acceso deben ser solicitados por la gestión de usuarios, aprobados por el propietario del sistema e implementados por el responsable de la seguridad. Las identidades y los derechos de acceso de los usuarios deben ser mantenidos en un repositorio central. Es necesario implementar y mantener actualizadas las medidas técnicas y de procedimientos con buena relación costo-beneficio para determinar la identidad de los usuarios, implementar la debida autenticación e imponer derechos de acceso. |
| DS5.4 Gestión de cuentas de usuario: asegurar que la solicitud, la emisión, la suspensión, la modificación y el bloqueo de cuentas de usuario y de los respectivos privilegios sean tratados por procedimientos de gestión de cuentas de usuario. Incluir un procedimiento de aprobación de concesión de derechos de acceso por los propietarios de los datos o sistemas. Este procedimiento debe ser aplicado a todos los usuarios, inclusive a los administradores (usuarios con privilegios), usuarios internos y externos, para los casos normales o de emergencia. Los derechos y obligaciones relacionadas al acceso a sistemas e información corporativa deben ser definidos en contratos para todos los tipos de usuarios. Deben ser realizadas revisiones frecuentes de todas las cuentas y de los respectivos privilegios. |
| DS5.5 Prueba de seguridad, vigilancia y monitoreo: garantizar que la implementación de seguridad de las TI sea probada y monitoreada proactivamente. La seguridad de las TI debe ser revalidada periódicamente para garantizar que el nivel de seguridad aprobado sea mantenido. La función de monitoreo y registro de eventos (*logging*) debe hacer posible la prevención y/o detección prematura de actividades anormales o poco comunes que necesitan ser tratadas, así como la subsecuente generación de informes en el tiempo apropiado. |
| DS5.6 Definición de incidentes de seguridad: definir y comunicar claramente las características de incidentes de seguridad potenciales, para que puedan ser tratados adecuadamente por los procesos de gestión de incidentes o gestión de problemas. |

Continuación tabla 47. Objetivos de control proceso garantizar la seguridad de los sistemas

| Objetivos de control |
|---|
| DS5.7 Protección de la tecnología de seguridad: garantizar que las tecnologías de seguridad importantes sean inviolables y que las documentaciones de seguridad no sean reveladas innecesariamente. |
| DS5.8. Gestión de clave criptográfica: asegurar que sean establecidas políticas y procedimientos de generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, inserción, uso y archivo de las claves criptográficas, buscando protegerlas contra modificación o revelación pública no autorizada. |
| DS5.9 Prevención, detección y corrección de software malicioso: asegurar que medidas preventivas, de detección y correctivas sean establecidas corporativamente, en especial correcciones de seguridad (*patches*) y controles de virus, para proteger los sistemas de información y tecnología contra *malwares* como virus, *worms, spyware, spam*, etc. |
| DS5.10 Seguridad de red: garantizar que técnicas de seguridad y procedimientos de gestión relacionados (como *firewalls*, aplicativos de seguridad, segmentación de red y detección de intrusión) sean utilizados para autorizar el acceso y controlar los flujos de información entre redes |
| DS5.11 Comunicación de datos confidenciales: asegurar que las transacciones de comunicación de datos confidenciales ocurran únicamente por un camino confiable o controlado, con el fin de brindar autenticación de contenido, comprobante de envío, comprobante de recibo y no rechazo de origen |

Garantizar la seguridad de los sistemas de las TI de la organización requiere varias fuentes de información, y produce información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"garantizar la seguridad de los sistemas"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de evaluación de madurez de la organización, relacionado con el proceso **"garantizar la seguridad de los sistemas"**.

### 4.1.6 Proceso DS6. Identificar y asignar costos

Brindar trasparencia y comprensión de los costos de las TI y mejoría de la relación costo beneficio por medio del uso de los servicios de las TI.

La identificación y la asignación de costos de los servicios de las TI influyen en el comportamiento del usuario, por medio de la divulgación y concientización de los costos, proporcionando datos de previsión presupuestal para la organización.

La contabilidad de costos tiene como objetivo la justa asignación de costos compartidos y el cobro por los servicios de las TI, mediante:

- Alineamiento de los valores cobrados a la calidad y cantidad de servicios brindados.
- Construcción y concordancia de un modelo completo de costos.
- Implementación del sistema de cobro de valores conforme a la política acordada.

Este proceso contempla la construcción y la operación de un sistema para capturar, asignar y reportar los costos de las TI a los usuarios de los servicios. Un sistema de asignación justo permite a la organización estar más informada y tomar decisiones sobre el uso de los servicios.

Ejemplo: los servicios de las TI deben ser mapeados por medio de un catálogo, con el levantamiento de todos los costos (personas, tecnologías etc.). Una organización que identifica correctamente los costos de las TI consigue mejorar su nivel de inversión y su modelo de costeo.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"identificar y asignar costos"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 48. Requisitos de negocio proceso identificar y asignar costos

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficiencia | P | Entrega de valor | P | Aplicaciones |
| Confiabilidad | P | Gestión de recursos | P | Información |
| | | Medición del desempeño | P | Infraestructura |
| | | | | Personas |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"identificar y asignar costos"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 49. Objetivos de control proceso identificar y asignar costos

| Objetivos de control |
|---|
| DS6.1 Definición de servicios: identificar todos los costos de las TI y asociarlos a los servicios de las TI, sustentando un modelo trasparente de costos. Los servicios de las TI deben ser asociados a los procesos de negocios de forma que permitan identificar los niveles de facturación del servicio correspondiente. |
| DS6.2 Contabilidad de las TI: reunir y asignar los costos vigentes de acuerdo con el modelo de costos definido. Las variaciones entre las previsiones y los costos reales deben ser analizadas e informadas en conformidad con los sistemas corporativos de medición financiera. |
| DS6.3 Modelaje de costos y cobros: con base en la especificación del servicio, definir un modelo de costos que considere los costos directos, indirectos y generales de los servicios, y soporte al cálculo de tasas de cobro por servicio. El modelo de costos debe estar alineado a los procedimientos de contabilidad de costos. El modelo de costos de TI debe asegurar que el cobro por los servicios sea identificable, medible y previsible por los usuarios para incentivar el uso adecuado de los recursos. El gerente de negocios debe ser capaz de verificar el uso real y el cobro de los servicios. |
| DS6.4 Mantenimiento del modelo de costos: realizar periódicamente un análisis crítico y una comparación con referencias de mercado (*benchmarking*) de la adecuación del modelo de costo/cobro buscando mantener la relevancia y la adecuación a los negocios y de las actividades de TI involucradas. |

Identificar y asignar costos de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"identificar y asignar costos"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobIT 4.1 también presenta un modelo de madurez para evaluar el nivel de madurez de la organización, relacionado con el proceso **"identificar y asignar costos".**

### 4.1.7 Proceso DS7. Educar y entrenar a los usuarios

Educar y entrenar a los usuarios para usar las aplicaciones y soluciones tecnológicas, así como las políticas y los procedimientos de la organización.

Este proceso busca entender claramente las necesidades del usuario en términos de entrenamiento en las TI y direccionar la ejecución de una estrategia eficaz de entrenamiento y medición de los resultados, mediante:

- » Establecimiento de un portafolio entrenamiento.
- » Organización del entrenamiento.
- » Disponibilidad del entrenamiento.
- » Monitoreo e informe de la eficacia del entrenamiento.

La educación efectiva de todos los usuarios de los sistemas de las TI, inclusive de aquellos dentro de la propia TI, requiere la identificación de las necesidades de entrenamiento de cada grupo de usuarios. Un programa de entrenamiento eficaz aumenta el uso efectivo de la tecnología a través de la reducción de errores del usuario, aumento de la productividad y de la conformidad con los controles principales (como las medidas de seguridad de usuario)

Ejemplo: las áreas de entrenamiento y capacitación de la organización deben obtener los requisitos necesarios para habilitar a los profesionales a ejercer sus funciones dentro y fuera del área de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"educar y entrenar usuarios"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 50. Requisitos de negocio proceso educar y entrenar usuarios

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficiencia | P | Alineamiento estratégico | S | Personas |
| Eficiencia | S | Entrega de valor | P | |
| | | Gestión de riesgos | S | |
| | | Gestión de recursos | S | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"educar y entrenar usuarios"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 51. Objetivos de control proceso educar y entrenar usuarios

| Objetivos de control |
|---|
| DS7.1 Identificar las necesidades de enseñanza y entrenamiento: establecer y actualizar regularmente un currículo para cada grupo de empleados, considerando:<br>» Las estrategias y necesidades actuales y futuras del negocio;<br>» El valor de la información como un bien;<br>» Los valores corporativos (valores éticos, cultura de seguridad y control etc);<br>» La implementación de nueva infraestructura de las TI y software (paquetes y aplicaciones);<br>» Las habilidades, competencias, certificación y actualizaciones necesarias;<br>» Los métodos de impartir clases (en salones, vía *web*), el tamaño del grupo, accesibilidad y tiempo. |
| DS7.2 Entrega del entrenamiento y enseñanza: con base en las necesidades de enseñanza y entrenamiento identificadas, definir los grupos objetivo y sus miembros, mecanismos adecuados de impartir los entrenamientos, profesores, instructores y monitores. Indicar los instructores y organizar las sesiones de entrenamiento de forma oportuna. Registrar inscripciones (incluyendo los prerrequisitos), frecuencia participación y evaluación de desempeño. |
| DS7.3 Evaluación del entrenamiento recibido: evaluar el contenido de la enseñanza y del entrenamiento recibido, con respecto a la relevancia, calidad, efectividad, absorción y retención del conocimiento, costo y valor. Los resultados de dicha evaluación deben servir de base para definir futuros currículos y sesiones de entrenamiento. |

Educar y entrenar usuarios para el uso de los recursos de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"educar y entrenar usuarios"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo para evaluar la madurez de la organización, relacionado con el proceso **"educar y entrenar usuarios".**

### 4.1.8 Proceso DS8. Gestionar el centro de servicio y los incidentes

Permitir el uso eficaz de los sistemas de las TI por medio del análisis y resolución de consultas, solicitudes e incidentes, creando en la organización un centro de servicios de las TI con respuestas rápidas, procedimientos claros de escalonamiento, análisis de tendencias y resolución de incidentes y problemas, mediante:

- Instalación y operación de un centro de servicios.
- Monitoreo y registro de las tendencias.
- Definición clara de criterios y procedimientos de escalamiento.

Este proceso incluye la implementación de un centro de servicios capacitado para el tratamiento de incidentes, incluyendo registro, enrutamiento, análisis de tendencias, análisis de causa-raíz y resolución.

- Los beneficios al negocio incluyen aumento de la productividad por medio de la resolución rápida de las llamadas de los usuarios.

El incidente es cualquier evento que no hace parte de la operación normal de un servicio y que causa (o puede causar) una interrupción del servicio o una reducción de su calidad.

- Una solución alterna es el método de evitar un incidente o problema.

Principales objetivos de un centro de servicios:

- Restaurar el servicio lo más rápido posible, por lo menos dentro del plazo establecido y documentado en el SLA, mientras algún efecto negativo es minimizado en el proceso de negocio.
- Mantener la comunicación continua entre la organización de las TI y el cliente sobre la situación del evento.
- Evaluar los incidentes para evitar la ocurrencia repetitiva o los problemas crónicos.

Ejemplo: el área de la organización que cuida de todas las solicitudes de las TI debe enfocarse en los servicios de las TI que se encuentran en el catálogo de servicios y a hacer el enlace entre el área de las TI y los usuarios de negocio.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestionar el centro de servicio y los incidentes"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 52. Requisitos de negocio proceso gestionar el centro de servicio y los incidentes

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficiencia | P | Entrega de valor | P | Aplicaciones |
| Eficiencia | P | Medición del desempeño | S | Personas |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestionar el centro de servicio y los incidentes"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 53. Objetivos de control proceso gestionar el centro de servicios y los incidentes

| Objetivos de control |
|---|
| DS8.1 Centro de servicios: establecer un centro de servicio, que es la interfaz entre los usuarios y la TI, para registrar, comunicar, despachar y analizar todos los llamados, incidentes reportados, solicitudes de servicio y demanda de información. Deben existir procedimientos de monitoreo y enrutamiento con base en niveles de servicio acordados relacionados en el SLA adecuado, que permite la clasificación y la priorización de cualquier duda reportada como incidente y solicitud de servicio o de información. Medir la satisfacción de los usuarios finales con la calidad del centro de servicios y de los servicios de TI. |
| DS8.2 Registro de las llamadas de los clientes: establecer una función y un sistema que permita el registro y el rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Deben trabajar de cerca con los procesos de gestión de incidentes, problemas, cambios, capacidad y disponibilidad. Los incidentes deben ser clasificados de acuerdo con las prioridades de negocio y direccionados al equipo de gestión de problemas. Los clientes deben ser informados sobre el estatus de sus llamadas. |
| DS8.3 Escalonamiento de incidentes: establecer los procedimientos de la central de servicio para que los incidentes que no pueden ser solucionados inmediatamente sean enrutados de forma adecuada, conforme los límites definidos en el SLA, y que las soluciones temporales sean aplicadas, si es posible. Asegurar que la propiedad y el monitoreo del ciclo de vida del incidente permanezcan bajo la responsabilidad de la central de servicio, independientes de que grupo de TI esté trabajando en las actividades de solución. |
| DS8.4 Cierre del incidente: establecer procedimientos para monitorear periódicamente el cierre de las llamadas de los clientes. Cuando un incidente ha sido resuelto, asegurar que la central de servicio registre los pasos adoptados para su solución y confirmar que las acciones adoptadas fueron aceptadas por el cliente. También registrar e informar incidentes no solucionados (errores ya conocidos y alternativas existentes de solución) para proveer información buscando la adecuada gestión de los problemas. |

Continuación tabla 53. Objetivos de control proceso gestionar el centro de servicios y los incidentes

| Objetivos de control |
| --- |
| DS8.5 Informes y análisis de tendencias: generar informes de actividades de la central de servicios, permitiendo a los gestores medir el desempeño y el tiempo de respuesta de los servicios e identificar tendencias o problemas recurrentes, para que el servicio pueda ser mejorado siempre. |

Gestionar la central de servicios y los incidentes de las TI de la organización requiere de varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"gestionar el centro de servicio y los incidentes"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo para la evaluación del nivel de madurez de la organización, relacionado con el **"gestionar el centro de servicio y los incidentes".**

### 4.1.9 Proceso DS9. Gestión de la configuración

Establecer y mantener un repositorio preciso y completo de la configuración de activos de las TI y compararlo con la configuración actual, brindando más control sobre los recursos de las TI, mediante:

- Establecimiento de un repositorio central de todos los elementos de la configuración.
- Identificación y mantenimiento de los elementos de la configuración.
- Información precisa y actualizada de todos los componentes que requieren de algún trabajo.
- Revisión de la integridad de los datos de la configuración.

Un Ítem de Configuración, IC, es un elemento de infraestructura de las TI documentado en las categorías de: Hardware, Software, alojamiento, personas y documentación.

Para definir como un IC se requieren cuatro condiciones:

- Ser necesario para la prestación del servicio.
- Ser identificado de forma única.
- Ser objeto de cambios.
- Poder ser gestionado.

Un elemento de configuración debe poseer:

- Una categoría.
- Una situación (*status*).
- Relaciones.
- Atributos.

Este proceso incluye la recolección inicial de la información de configuración, el establecimiento de un perfil básico, la verificación y la auditoría de la información de configuración, y la actualización del repositorio de configuración, conforme a las necesidades. Una gestión de configuración eficaz facilita una mayor disponibilidad del sistema, minimiza las preguntas de producción y soluciona problemas con mayor rapidez.

Un IC es un elemento documentado de la infraestructura de las TI como hardware, software, alojamiento, personas y documentación (categoría). El registro de un IC contiene características como tipo, versión, proveedor, cliente (atributos). La relación entre los ICs es registrada en una base de datos, denominada Banco de Datos de Gestión de Configuración, BDGC, *Configuration Management Data Base*, CMDB.

Ejemplo: es necesario que el área de las TI de una organización tenga el control y la gestión de todos los activos de las TI y su asociación con los servicios de las TI que brinda al negocio. A partir del conocimiento integrado de todos los activos de las TI, será más fácil para la organización invertir adecuadamente, en alineamiento con los procesos de negocio.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestión de la configuración"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 54. Requisitos de negocio proceso gestión de la configuración

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficiencia | P | Entrega de valor | P | Aplicaciones |
| Eficiencia | S | Gestión de riesgos | S | Información |
| Disponibilidad | S | Gestión del desempeño | P | Infraestructura |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestión de la configuración"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 55. Objetivos de control proceso gestión de la configuración

| Objetivos de control |
|---|
| DS9.1 Repositorios de configuración y perfiles básicos: establecer una herramienta de soporte y un repositorio central para almacenar toda la información relevante sobre los ítems de configuración. Monitorear y registrar todos los bienes y los cambios ocurridos en ellos. Mantener un perfil básico de ítems de configuración de todo el sistema y servicio como un punto de verificación seguro para un eventual retorno después de algún cambio. |
| DS9.2 Identificación y mantenimiento de los ítems de configuración: implementar procedimientos de configuración para soportar la gestión y el registro de todas las modificaciones al repositorio de configuraciones. Integrar esos procedimientos con la gestión de cambios, de incidentes y de problemas. |
| DS9.3 Revisión de la integridad de la configuración: periódicamente revisar los datos de configuración para verificar y confirmar la integridad de la configuración actual e histórica. Realizar un análisis crítico periódico de las políticas de uso de software, verificando la eventual existencia de software personal, no autorizado o exceso del contrato de licencias vigente. Los errores y desvíos deben ser reportados, tratados y corregidos. |

Gestionar la configuración de los elementos de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"gestión de la configuración"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo para la evaluación de madurez de la organización, relacionado con el proceso **"gestión de la configuración".**

### 4.1.10 Proceso DS10. Gestión de problemas

- Registrar, rastrear y resolver problemas operacionales
- Investigar la causa raíz de todos los problemas importantes y definir las soluciones para los problemas operacionales identificados, mediante:
  - Realizar análisis de la causa raíz del problema reportado
  - Análisis de tendencias.
  - Propiedad de los problemas y progreso en su solución

El proceso aplica a todos los tipos de servicios en TI que fallen. Su objetivo es identificar las causas principales de falla y recomendar alteraciones en los ítems de configuración.

Principales conceptos asociados al proceso:

- Problema
- Error
- Error conocido

La clasificación de un problema permite que sean designados los recursos apropiados, garantizando que los problemas sean tratados de forma eficiente y efectiva, y la identificación de aquellos con mayor impacto en los negocios.

El proceso de gestión de problemas también contempla la identificación de recomendaciones para mejora, mantenimiento de registros de problemas y revisión de la situación de las acciones correctivas. Un proceso efectivo de gestión de problemas mejora los niveles de servicio, reduce los costos y aumenta la atención y satisfacción del cliente. El proceso aplica a todos los tipos de servicios de las TI que presentan una falla. Su objetivo es identificar las principales causas de fallas y recomendar alteraciones en los, IC.

Principales conceptos asociados al proceso:

- Problema: causa raíz desconocida de uno o más incidentes; también puede ser descrito como la identificación de una condición, resultante de múltiples incidentes que exhiben síntomas comunes. Los problemas también pueden ser identificados a partir de un único incidente significativo.
- Error: un incidente o problema cuya causa raíz es conocida.
- Error conocido: incidente o problema cuya causa raíz es conocida y para el cual fue encontrada una solución de contorno temporal o la solución definitiva.

Ejemplo: las áreas de las TI deben utilizar la gestión de problemas para desarrollar una cultura proactiva para mantener la TI siempre operacional.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestión de problemas"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 56. Requisitos de negocio proceso gestión de problemas

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficiencia | P | Entrega de valor | P | Aplicaciones |
| Eficiencia | P | Gestión de riesgos | S | Información |
| Disponibilidad | S | Gestión del desempeño | S | Infraestructura |
| | | | | Personas |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestión de problemas"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 57. Objetivos de control proceso gestión de problemas

| Objetivos de control |
|---|
| DS10.1 Identificar y clasificar los problemas: implementar procesos para reportar y clasificar los problemas identificados como parte de la gestión de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos de la clasificación de incidentes; sirven para identificar la categoría, el impacto, la urgencia y la prioridad. Los problemas deben ser clasificados en grupos o dominios relacionados (por ejemplo, hardware, software, soporte al software). Esos grupos deben corresponder a responsabilidades operacionales asociados a clientes y usuarios, y servir como base para la asignación de los problemas. |

Continuación tabla 57. Objetivos de control proceso gestión de problemas

| Objetivos de control |
|---|
| DS10.2 Rastreo y solución de problemas: el sistema de gestión de problemas debe brindar recursos de rastros de auditoría adecuados, que permitan el rastreo, el análisis y al identificación de la causa raíz de todos los problemas reportados, considerando:<br>» Todos los ítems de configuración asociados.<br>» Los problemas e incidentes pendientes<br>» Los errores conocidos y sospechosos.<br>» El rastreo de tendencias de problemas.<br>Identificar el problema e iniciar el tratamiento de su causa raíz, presentando solicitudes de cambio de acuerdo con el proceso de gestión de cambio establecido. Por medio del proceso de solución, o gestión de problemas se debe obtener reportes periódicos de gestión de cambios del progreso de la solución de problemas y errores. La gestión de los problemas debe monitorear continuamente el impacto de los problemas y errores conocidos en los servicios a los usuarios. En el caso de impactos severos, la gestión de problemas debe encaminar el problema al grupo apropiado, para aumentar la prioridad de solicitud de cambio (RFC) o implementar cambios urgentes apropiados. El avance de la solución del problema debe ser monitoreado de acuerdo con los SLAs |
| DS10.3 Cierre de problemas: establecer un procedimiento de cierre de registro de problema, tanto en la confirmación de la eliminación exitosa de un error conocido como después de un acuerdo con las áreas de negocio sobre cómo tratar con el problema de manera alternativa. |
| DS10.4 Integración de gestión de cambios, configuración y problemas: integrar los procesos de configuración y gestión de problemas e incidentes para asegurar una gestión efectiva de problemas y facilitar las mejoras en el proceso. |

La gestión de problemas de los servicios de las TI de la organización requiere varias fuentes de información, y produce información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"gestión de problemas"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo para la evaluación de la madurez de la organización, relacionado con el proceso **"gestión problemas"**.

### 4.1.11 Proceso DS11. Gestionar los datos

» Optimizar el uso de la información y garantizar que la información esté disponible cuando sea necesaria, manteniéndola completa, precisa, disponible y protegida, mediante:
  - Realización de copias de seguridad (*backup*) de los datos y pruebas de restauración.
  - Gestión de almacenamiento local y remoto de los datos (*onsite y offsite*)
  - Descarte seguro de datos y equipos.

El proceso de gestión de datos también contempla el establecimiento de procedimientos efectivos para controlar la biblioteca de medios, copia de seguridad (*backup*), recuperación de datos y el almacenamiento de datos de forma adecuada. La gestión efectiva de datos ayuda a asegurar la calidad, la rapidez y la disponibilidad de los datos relacionados con el negocio.

Ejemplo: las áreas operacionales de las TI son responsables por ejecutar las actividades de este proceso.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestionar los datos"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 58. Requisitos de negocio proceso gestionar los datos

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Integridad | P | Entrega de valor | P | Información |
| Confiabilidad | P | Gestión de riesgos | P | |
| | | Gestión de recursos | P | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestionar los datos",** con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 59. Objetivos de control proceso gestionar los datos

| Objetivos de control |
|---|
| DS11.1 Requisitos de negocio para la gestión de datos: verificar que todos los datos esperados sean recibidos, procesados de manera completa, precisa y en el tiempo apropiado, y que toda salida sea entregada de acuerdo con los requisitos de negocio. Soportar las necesidades de reanudación y reproceso. |

Continuación tabla 59. Objetivos de control proceso gestionar los datos

| Objetivos de control |
|---|
| DS11.2 Arreglos de almacenamiento y retención: definir e implementar procedimientos para un efectivo y eficiente almacenamiento de datos, retención y archivamiento para atender los objetivos de negocio, a la política de seguridad de la organización y las exigencias regulatorias. |
| DS11.3 Sistemas de gestión de biblioteca de medios: definir e implementar procedimientos para mantener un inventario de los medios almacenados y archivados, asegurando su usabilidad e integridad. |
| DS11.4 Descarte de datos y equipos: definir e implementar procedimientos para asegurar que los requisitos de negocios sean atendidos en relación a la protección de datos confidenciales y software, cuando los datos y equipos son descartados o transferidos |
| DS11.5 *Backup* y restauración: definir e implementar procedimientos de copia de seguridad (*backup*) y restauración de sistemas, aplicativos, datos y documentación, en alineamiento con los requisitos de negocio y con el plan de continuidad. |
| DS11.6 Requisitos de seguridad para la gestión de datos: definir y establecer políticas y procedimientos para identificar y aplicar requisitos de seguridad aplicables a recepción, procesamiento, almacenamiento físico y salida de datos para atender los objetivos del negocio, la política de seguridad de la organización y las exigencias reglamentarias. |

Gestionar los datos de los sistemas de información de las TI de la organización necesita varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"gestionar los datos"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de madurez para la evaluación del nivel de madurez de la organización, relacionado con el **"gestionar los datos".**

### 4.1.12 Proceso DS12. Gestionar el ambiente físico

» Proteger los activos de las TI y los datos de negocio y minimizar el riesgo de interrupción en los negocios, brindando y manteniendo un ambiente físico adecuado que proteja los recursos de las TI contra el acceso indebido, daños, robo, mediante:

- Implementación de medidas de seguridad física.
- Selección y gestión de instalaciones físicas.

El proceso de gestión del ambiente físico incluye la definición de los requisitos del local físico, la selección de instalaciones apropiadas, el diseño de procesos eficaces de monitoreo de factores ambientales y su gestión de accesos físicos. La gestión eficaz del ambiente físico reduce

las interrupciones en los negocios provocadas por daños causados a equipos o personas.

Ejemplo: garantizar la seguridad patrimonial y el acceso a las áreas restringidas de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestionar el ambiente físico"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 60. Requisitos de negocio proceso gestionar el ambiente físico

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Integridad | P | Gestión de riesgos | P | Infraestructura |
| Disponibilidad | P | Gestión de recursos | S | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestionar el ambiente físico"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 61. Objetivos de control proceso gestionar el ambiente físico

| Objetivos de control |
|---|
| DS12.1 Selección y distribución del centro de datos: definir y seleccionar el local para los equipos de las TI, considerando el alineamiento de la estrategia tecnológica con la estrategia de negocios. La selección y la planeación de la distribución de una instalación física deben tener en cuenta los riesgos asociados a posibles desastres naturales y no naturales, así como las leyes y regulaciones relevantes, tales como reglamentaciones de salud ocupacional y seguridad en el trabajo. |
| DS12.2 Medidas de seguridad física: definir e implementar medidas de seguridad física alineadas con los requisitos del negocio para proteger el centro de datos y los activos físicos. Las medidas de seguridad física deben ser capaces de prevenir efectivamente, detectar y mitigar riesgos relacionados con robo, temperatura, fuego, humo, agua, vibración, terrorismo, vandalismo, cortes de energía, químicos y explosivos. |

Continuación tabla 61. Objetivos de control proceso gestionar el ambiente físico

| Objetivos de control |
|---|
| DS12.3 Acceso físico: definir e implementar procedimientos para conceder, limitar y revocar el acceso a las instalaciones, edificios y áreas, de acuerdo con las necesidades de negocio, inclusive en situaciones de emergencia. Los accesos a instalaciones, edificios y áreas deben ser justificados, autorizados, registrados y monitoreados. Esto se aplica a todas las personas que acceden a las instalaciones, inclusive el personal fijo, funcionarios temporales, clientes, vendedores y visitantes, entre otros. |
| DS12.4 Protección contra factores ambientales: diseñar e implementar medidas de protección contra factores ambientales. Instalar equipos y dispositivos especializados para monitorear y controlar el ambiente. |
| DS12.5 Gestión de instalaciones físicas: gestionar las instalaciones físicas, incluyendo equipos de energía y comunicaciones, en alineamiento con las leyes y regulaciones, requisitos técnicos y de negocio, especificaciones de los fabricantes y distribuidores de equipos y directrices de seguridad y salud ocupacional. |

Gestionar el ambiente físico de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"gestionar el ambiente físico"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo para evaluar el nivel de madurez de la organización, relacionado con el proceso **"gestionar el ambiente físico"**.

### 4.1.13 Proceso DS13. Gestionar las operaciones

» Mantener la integridad de los datos y asegurar que la infraestructura de las TI pueda resistir y recuperarse de errores y fallas, alcanzando los niveles de servicio operacionales para el procesamiento programado de datos, protección de salidas de datos críticos, monitoreo y mantenimiento de la infraestructura, mediante:

- Operación del ambiente de las TI alineado con los niveles de servicio acordados e instrucciones definidas.
- Mantenimiento de la infraestructura de las TI

Este proceso incluye la definición de políticas y procedimientos de operaciones para la gestión eficaz del proceso agendado, protección de resultados sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. La gestión efectiva de operaciones ayuda a mantener la integridad de los datos y a reducir atrasos y costos en la operación de las TI.

Ejemplo: las áreas operacionales de las TI son responsables por ejecutar las actividades de este proceso.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"gestionar las operaciones"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 62. Requisitos de negocio proceso gestionar las operaciones

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Gestión de recursos | P | Aplicaciones |
| Eficiencia | P | | S | Información |
| Integridad | S | | | Infraestructura |
| Disponibilidad | S | | | Personas |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"gestionar las operaciones",** con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 63. Objetivos de control proceso gestionar las operaciones

| Objetivos de control |
|---|
| DS13.1 Procedimientos e instrucciones operacionales: definir, implementar y mantener procedimientos estandarizados para las operaciones de las TI y asegurar que el equipo de operaciones esté familiarizado con todas las actividades operacionales relevantes. Los procedimientos operacionales deben incluir el cambio de turnos (entrega formal de las actividades, actualización de información, problemas operacionales, procedimientos para escalar e informes de responsabilidades actuales) para asegurar el nivel de servicio acordado y la continuidad de las operaciones. |
| DS13.2 Agenda de trabajos periódicos: organizar la agenda de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el procesamiento y la utilización para atender los requisitos del negocio. |

Continuación tabla 63. Objetivos de control proceso gestionar las operaciones

| Objetivos de control |
|---|
| DS13.3 Monitoreo de la infraestructura de las TI: definir e implementar procedimientos para monitorear la Infraestructura de las TI y eventos relacionados. Asegurar que suficiente información cronológica sea almacenada en los registros de la operación para permitir la reconstrucción, la revisión y el análisis de las secuencias de tiempo de las operaciones y otras actividades pertinentes o de apoyo a las operaciones. |
| DS13.4 Documentos confidenciales y dispositivos de salida: establecer protección física apropiada, prácticas de control y gestión de inventario sobre activos críticos de TI, tales como formularios especiales, documentos de Negociación, impresoras de finalidades especiales o *Tokens* de seguridad. |
| DS13.5 Mantenimiento preventivo de hardware: definir e implementar procedimientos para asegurar el mantenimiento periódico de la infraestructura para reducir la frecuencia y el impacto de fallas o la degradación del desempeño. |

Gestionar las operaciones de las TI de la organización requiere varias fuentes produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada–salida del proceso **"gestionar las operaciones"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de madurez para evaluar el nivel de madurez de la organización, relacionado con el proceso **"gestionar las operaciones".**

## Ejercicio de refuerzo - definiendo el nivel de madurez para los procesos del dominio DS

CobiT 4.1 define modelo de madurez para los procesos para que sea posible evaluar el nivel de madurez de la organización. Tomando como referencia el modelo de madurez de CobiT 4.1, evalúe el nivel de madurez de los procesos del dominio DS de su organización. Utilice como referencia el marco de CobiT 4.1

| | Nivel de madurez | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 |
| DS1 Definir y gestionar niveles de servicios | | | | | | |
| DS2 Gestionar servicios extenos | | | | | | |
| DS3 Gestionar el desempeño y la capacidad | | | | | | |
| DS4 Asegurar la continuidad de los servicios | | | | | | |
| DS5 Garantizar la seguridad de los sistemas | | | | | | |
| DS6 Identificar y asignar costos | | | | | | |
| DS7 Educar y entrenar los usuarios | | | | | | |
| DS8 Gestionar la central de servicio y los incidentes | | | | | | |
| DS9 Gestionar la configuración | | | | | | |
| DS10 Gestión de problemas | | | | | | |
| DS11 Gestionar los datos | | | | | | |
| DS12 Gestionar el ambiente físico | | | | | | |
| DS13 Gestionar las operaciones | | | | | | |

## 4.2 Dominio: Monitorear y Evaluar, ME

Todos los procesos de las TI necesitan ser evaluados regularmente con el paso del tiempo para asegurar la calidad y la adherencia a los requisitos de control. Este dominio aborda la gestión del desempeño, el monitoreo del control interno, la adherencia regulatoria y el gobierno.

El dominio ME puede ayudar a la organización en los siguientes aspectos:

- Medir el desempeño de las TI para detectar problemas antes que ellos ocurran.
- Asegurar que los controles internos sean efectivos y eficientes.
- Asociar el desempeño de las TI a los objetivos de negocio.
- Definir los controles adecuados para garantizar confidencialidad, integridad y disponibilidad de la información.

El dominio, ME está compuesto por cuatro procesos:

- ME1 Monitorear y evaluar el desempeño de las TI
- ME2 Monitorear y evaluar los controles internos
- ME3 Asegurar la conformidad con requisitos externos
- ME4 Proveer gobierno de las TI

### 4.2.1 Proceso ME1. Monitorear y evaluar el desempeño de las TI

» Brindar trasparencia y comprensión de costos, beneficios, estrategia, políticas y niveles de servicios de las TI, en conformidad con los requisitos de gobierno, monitoreando y entregando informes sobre las métricas de los procesos de las TI, identificando e implementando acciones de mejora de desempeño, mediante:

- Agrupar y traducir los informes de desempeño de procesos para los informes de gestión.
- Análisis crítico del desempeño frente a metas acordadas y la toma de acciones correctivas necesarias.

Este proceso incluye la definición de indicadores relevantes de desempeño, informes sistemáticos y oportunos de desempeño y una pronta acción en relación a las desviaciones encontrados.

Ejemplo: el centro de control y monitoreo, implementado por medio de herramientas de recolección de eventos, es normalmente utilizado para monitorear el desempeño de los activos y soluciones de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"monitorear y evaluar el desempeño de las TI"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 64. Requisitos de negocio proceso monitorear y evaluar el desempeño de las TI

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | S | Aplicaciones |
| Eficiencia | P | Entrega de valor | S | Información |
| Confidencialidad | S | Gestión de riesgos | S | Infraestructura |
| Integridad | S | Gestión de recursos | S | Personas |
| Disponibilidad | S | Medición del desempeño | P | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"monitorear y evaluar el desempeño de las TI"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 65. Objetivos de control proceso monitorear y evaluar el desempeño de las TI

| Objetivos de control |
|---|
| ME 1.1 Enfoque del monitoreo: establecer un enfoque y un estructura de monitoreo general que definan el alcance, la metodología y el proceso a ser seguidos para evaluar la entrega de soluciones y servicios de las TI y monitorear la contribución de las TI a los resultados del negocio. La estructura se debe integrar con el sistema de gestión de desempeño corporativo. |
| ME 1.2 Definición y recolección de datos de monitoreo: trabajar con el negocio en la definición de un conjunto equilibrado de metas de desempeño que sean aprobadas por las áreas de negocio y demás partes interesadas relevantes. Definir modelos comparativos (*Benchmarks*) para metas e identificar los datos disponibles para la recolección con la intención de la medición de las metas. Establecer procesos para recolectar en el tiempo apropiado y de manera correcta los datos a ser incluidos en informes que muestren el progreso en el alcance de las metas. |
| ME 1.3 Método de monitoreo: implementar un método de monitoreo de desempeño (tal como el *Balanced Scorecard*) que registre las metas, capture las mediciones, presente una visión amplia y sucinta del desempeño de las TI y se ajuste al sistema de monitoreo corporativo. |
| ME 1.4 Evaluación del desempeño: analizar periódicamente el desempeño con base en las metas, ejecutar análisis de la causa raíz de los problemas e iniciar acciones correctivas para tratar las causas ocultas. |

Continuación tabla 65. Objetivos de control proceso monitorear y evaluar el desempeño de las TI

| Objetivos de control |
| --- |
| ME 1.5 Informes para la alta dirección: desarrollar informes para la alta dirección sobre la contribución de las TI para el negocio, especialmente en términos de desempeño del portafolio de la organización, programas de inversión en TI y soluciones y servicios de cada programa. En los informes gerenciales de estado, informar hasta qué punto los objetivos planeados fueron alcanzados, los recursos proyectados fueron utilizados, las metas de desempeño alcanzadas y los riesgos minimizados. Anticipar la revisión de la alta dirección, sugiriendo acciones de remediación en el caso de desvíos importantes. Brindar informes para la alta dirección y solicitar la retroalimentación (*feedback*) de la revisión gerencial. |
| ME 1.6 Acciones de remediación: identificar e iniciar acciones de remediación con base en el monitoreo, en la evaluación y en los informes de desempeño. Incluye el acompañamiento de todo el proceso de monitoreo, informes y evaluaciones con:<br>» Análisis crítico, negociación y establecimiento de respuestas de gestión;<br>» Asignación de responsabilidades en las correcciones;<br>» Verificación de los resultados de las acciones acordadas. |

Monitorear y evaluar el desempeño de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"monitorear y evaluar el desempeño de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo de madurez para evaluar el nivel de madurez de la organización, relacionado con el proceso **"monitorear y evaluar el desempeño de las TI".**

### 4.2.2 Proceso ME2. Monitorear y evaluar los controles internos

» Asegurar que los objetivos de las TI sean alcanzados y asegurar la conformidad con las leyes y los reglamentos relacionados a TI, monitoreando los procesos de control interno de actividades de las TI e identificando acciones de mejora, mediante:

- Definición de un sistema de controles internos integrado a la estructura de procesos de las TI.
- Monitoreo y reporte sobre la eficacia los controles internos de las TI.
- Reporte de las excepciones de los controles internos para que la gerencia tome las medidas necesarias.

Este proceso incluye el monitoreo y reporte de las excepciones de control, de los resultados de autoevaluación y evaluación de terceros. Un beneficio importante del monitoreo de los controles internos es asegurar una operación eficaz y eficiente y la conformidad con las leyes y los reglamentos aplicables.

Ejemplo: definir una estructura que establezca los principales controles que deben ser implementados y auditados para evaluar el desempeño de los procesos de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"monitorear y evaluar los controles internos"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 66. Requisitos de negocio proceso monitorear y evaluar los controles internos

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Entrega de valor | P | Aplicaciones |
| Eficiencia | P | Gestión de riesgos | P | Información |
| Confidencialidad | S | | | Infraestructura |
| Integridad | S | | | Personas |
| Disponibilidad | S | | | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"monitorear y evaluar los controles internos"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 67. Objetivos de control proceso monitorear y evaluar los controles internos

| Objetivos de control |
|---|
| ME 2.1 Monitoreo de la estructura de controles internos: monitorear, comparar y mejorar el ambiente y la estructura de controles de las TI continuamente, para alcanzar los objetivos organizacionales. |
| ME 2.2 Revisión gerencial: monitorear y evaluar la eficiencia y la eficacia de las revisiones gerenciales de los controles internos de las TI. |
| ME 2.3 Excepción a los controles: identificar todas las excepciones a los controles y asegurar que sea hecho un análisis crítico de las causas principal. Escalar y reportar adecuadamente las excepciones a las partes interesadas. Realizar las acciones correctivas necesarias. |
| ME 2.4 Autoevaluación de los controles: evaluar el grado de alcance y la efectividad de los controles internos de la administración sobre los procesos, las políticas y los contratos de las TI por medio de un programa continuo de autoevaluación. |
| ME 2.5 Garantía de los controles internos: conforme a la necesidad, obtener mayor garantía del alcance y la eficacia de los controles internos por medio de evaluaciones de terceros. |
| ME 2.6 Controles internos aplicados a terceros: evaluar el status de los controles internos aplicados a cada proveedor de servicio. Cerciorarse de que los proveedores externos de servicios atienden las exigencias legales y reglamentarias y las obligaciones contractuales. |
| ME 2.7 Acciones correctivas: identificar, iniciar, monitorear e implementar acciones correctivas con base en las evaluaciones y en los informes de control. |

Monitorear y evaluar los controles internos de las TI de la organización necesita varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"monitorear y evaluar los controles internos"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo madurez para evaluar el nivel de madurez de la organización, relacionado con el proceso **"monitorear y evaluar los controles internos".**

### 4.2.3 Proceso ME3. Asegurar la conformidad con requisitos externos

Estar en conformidad con las leyes, reglamentos y requisitos contractuales identificando todas las leyes, reglamentos y contratos aplicables y el respectivo nivel necesario de conformidad de las TI, optimizando los procesos de las TI para reducir el riesgo de no conformidad, mediante:

» Identificación de los requisitos legales, reglamentarios y contractuales relacionados a TI.
» Evaluación del impacto de los requisitos de conformidad.
» Monitoreo y generación de informes sobre la conformidad de esos requisitos.

Este proceso incluye identificar los requisitos de conformidad, optimizar y evaluar la respuesta, asegurarse de que los requisitos se hayan cumplido e integrar los informes de conformidad de las TI con los informes de las áreas de negocio.

Ejemplo: definir una estructura que atienda los principales requisitos legales para la actuación del área de las TI. Se entiende por requisitos legales las leyes y reglamentos que deben ser seguidos por las organizaciones.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"asegurar la conformidad con requisitos externos"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 68. Requisitos de negocio proceso asegurar la conformidad con requisitos externos

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Conformidad | S | Alineamiento estratégico | P | Aplicaciones |
| Confiabilidad | S | Gestión de riesgos | P | Información |
| | | | | Infraestructura |
| | | | | Personas |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"asegurar la conformidad con requisitos externos"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 69. Objetivos de control proceso asegurar la conformidad con requisitos externos

| Objetivos de control |
|---|
| ME 3.1 Identificación de los requisitos de conformidad con leyes, reglamentaciones y contratos externos: identificar continuamente las exigencias locales e internacionales de ley, reglamentaciones y contratos que deben ser cumplidas para su inclusión en políticas, estándares, procedimientos y metodologías de las TI. |
| ME 3.2. Optimización de respuesta a requisitos externos: revisar y ajustar políticas, estándares, procedimientos y metodologías de las TI para asegurar que los requisitos legales, reglamentarios y contractuales sean atendidos y comunicados. |
| ME 3.3 Evaluación de la conformidad con requisitos externos: confirmar la conformidad de políticas, estándares, procedimientos y metodologías de las TI con los requisitos legales y reglamentarios. |
| ME 3.4 Asegurar la conformidad: obtener y asegurar la conformidad y adhesión a todas las políticas internas derivadas de directrices legales, internas o externas, y requisitos regulatorios o contractuales externos, confirmando que acciones correctivas fueron tomadas oportunamente para resolver cualquier desvío de conformidad del proceso. |
| ME 3.5 Informes integrados: integrar los informes de las TI sobre requisitos legales, regulatorios y contractuales a los informes similares de otras funciones del negocio. |

Asegurar la conformidad con requisitos externos de las TI de la organización requiere varias fuentes produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"asegurar la conformidad con requisitos externos"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso. CobiT 4.1 también presenta un modelo para evaluar el nivel de madurez de la organización, relacionado con el proceso **"asegurar la conformidad con requisitos externos".**

### 4.2.4 Proceso ME4. Proveer gobierno de las TI

Integrar el gobierno de las TI a los objetivos de gobierno corporativo y tener conformidad con leyes, reglamentos y contratos, preparando informes gerenciales sobre la estrategia, el desempeño y los riesgos de las TI, y atendiendo los requisitos de gobierno, en alineamiento con las directrices de la alta dirección de la organización, mediante:

- Establecimiento de una estructura de gobierno de las TI integrada al gobierno corporativo.
- Realizar auditoría independiente sobre el estado de gobierno de las TI.

El establecimiento de una estructura efectiva de gobierno involucra la definición de las estructuras organizacionales, de los procesos, del liderazgo, de los roles y respectivas responsabilidades para asegurar que las inversiones corporativas en las TI estén alineadas y sean entregadas en conformidad con las estrategias y los objetivos de la organización.

Ejemplo: la definición de un panel de indicadores debe ser adoptada para proveer el gobierno efectivo de las TI.

La siguiente tabla presenta los requisitos de negocios, las áreas de énfasis del gobierno de las TI y los recursos de las TI que los procesos **"proveer gobierno de las TI"** buscan satisfacer y mantener bajo gestión y control, con el fin de garantizar que los objetivos del negocio sean alcanzados.

Tabla 70. Requisitos de negocio proceso proveer gobierno de las TI

| Requisitos de negocio | | Áreas de énfasis del gobierno de TI | | Recursos de TI necesarios |
|---|---|---|---|---|
| Eficacia | P | Alineamiento estratégico | P | Aplicaciones |
| Eficiencia | P | Entrega de valor | P | Información |
| Confidencialidad | S | Gestión de riesgos | P | Infraestructura |
| Integridad | S | Gestión de recursos | P | Personas |
| Disponibilidad | S | Medición del desempeño | P | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |
| Conformidad | S | | | |
| Confiabilidad | S | | | |

Nomenclatura: Primario: P; Secundario: S

CobiT 4.1 también define los siguientes objetivos de control para el proceso **"proveer gobierno de las TI"**, con el fin de garantizar que los objetivos de negocio sean alcanzados y los eventos indeseables sean tratados adecuadamente.

Tabla 71. Objetivos de control proceso proveer gobierno de las TI

| Objetivos de control |
| --- |
| ME 4.1 Establecer una estructura de gobierno de las TI: definir, establecer y alinear la estructura de gobierno de las TI con el gobierno organizacional y el ambiente de control. Fundamentar la estructura en procesos y modelos de control de las TI adecuados e implementar prácticas y responsabilidades claras para evitar fallas de control interno y supervisión. Cerciorarse de que la estructura de gobierno de las TI asegura la conformidad con leyes y reglamentos, alineada con las estrategias y los objetivos de la organización. Producir informes sobre el status de gobierno de las TI y asuntos relacionados. |
| ME 4.2. Alineamiento estratégico: facilitar a la alta dirección la comprensión de los asuntos estratégicos de las TI, tales como los roles de las TI, las capacidades y los conocimientos tecnológicos. Asegurarse de que existe un conocimiento compartido entre el negocio y la TI relacionada del potencial de la contribución de las TI a la estrategia de negocio. Trabajar con el consejo directivo y los cuerpos de gobierno establecidos, tal como un comité de estrategia de las TI, para dar dirección estratégica a la gestión relacionada con TI, asegurando que la estrategia y los objetivos sean propagados de arriba a abajo a las unidades de negocio y las funciones de las TI, y que la credibilidad y la confianza sean desarrollados entre el negocio y el área de las TI. Permitir el alineamiento de las TI al negocio en lo que concierne a la estrategia y a la operación, incentivando la responsabilidad compartida entre el negocio y TI para tomar decisiones estratégicas y obtener los beneficios de las inversiones en TI. |
| ME 4.3 Entrega de valor: gestionar los programas de inversión y demás recursos y servicios de las TI para asegurar que brinden el mayor valor posible en el soporte a los objetivos y estrategias de negocio. Asegurar que sean alcanzados los resultados esperados por el negocio en relación con las inversiones de las TI, que el alcance completo de esfuerzos necesarios para lograr esos resultados sea entendido, que sean creados y aprobados por las partes interesadas casos de negocio completos y consistentes, que los activos e inversiones sean gestionados durante sus ciclos de vida económicos, y que exista una gestión activa de la realización de los beneficios, tal como contribución a nuevos servicios, ganancias de eficiencia y respuesta rápida a las solicitudes del cliente. Imponer un enfoque disciplinado de gestión de portafolio, programas y proyectos, insistiendo en que el negocio se responsabilice de todas las inversiones habilitadoras de las TI y asegurando que el área de TI optimice los costos de la entrega de capacidades y servicios. |
| ME 4.4 Gestión de recursos: supervisar la inversión, el uso y la asignación de los recursos de las TI por medio de evaluaciones periódicas de las iniciativas y operaciones de las TI, buscando asegurar a la existencia de recursos suficientes y el alineamiento con objetivos estratégicos y necesidades de negocio actuales y futuras. |
| ME 4.5 Gestión de riesgos: trabajar con el consejo directivo para definir el apetito corporativo de riesgo de las TI y obtener una seguridad razonable de que las prácticas de gestión de riesgos de las TI son adecuadas para asegurar que los riesgos actuales de las TI no exceden el apetito de riesgo de la alta dirección. Integrar las responsabilidades de gestión de riesgos con la organización, asegurando que las áreas de negocios y TI evalúan regularmente y reportan los riesgos relacionados con TI y sus impactos, y que la posición de los riesgos de TI de la organización sea transparente para todas las partes interesadas. |

Continuación tabla 71. Objetivos de control proceso proveer gobierno de las TI

| Objetivos de control |
|---|
| ME 4.6 Medición de desempeño: confirmar si los objetivos acordados de las TI fueron alcanzados o excedidos o si el progreso en el logro de los objetivos de las TI satisface las expectativas. Cuando los objetivos acordados no son alcanzados o el progreso no sale como es esperado, es necesario revisar las acciones correctivas de la gerencia. Reportar a la alta dirección los portafolios y programas relevantes y el desempeño de las TI, con base en informes que permitan a la alta dirección revisar el progreso de la organización en lo relacionado con los objetivos definidos. |
| ME 4.7 Evaluación independiente: obtener una evaluación independiente (interna o externa) sobre la conformidad de las TI con leyes y reglamentos relevantes, políticas y procedimientos organizacionales y con prácticas generalmente aceptadas para el efectivo y eficiente desempeño de las TI |

Habilitar la operación y uso de las TI de la organización requiere varias fuentes de información, produciendo información de salida. CobiT 4.1 establece un amplio número de relaciones de entrada – salida del proceso **"proveer gobierno de las TI"** con otros procesos relacionados a los demás dominios de su estructura, así como define las principales actividades y funciones desempeñadas en este proceso.

CobiT 4.1 también presenta un modelo de madurez para evaluar el nivel de madurez de la organización, relacionado con el proceso **"proveer gobierno de las TI".**

## Ejercicio de refuerzo - definiendo el nivel de madurez para los procesos de dominio ME.

CobiT 4.1 define modelo de madurez para los procesos para que sea posible evaluar el nivel de madurez de la organización. Tomando como referencia el modelo de madurez de CobiT 4.1, evalúe el nivel de madurez de los procesos del dominio ME de su organización. Utilice como referencia el marco de CobiT 4.1

| | Nivel de madurez | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 |
| ME1 Monitorear y evaluar el desempeño de las TI | | | | | | |
| ME2 Monitorear y evaliuar los controles internos | | | | | | |
| ME3 Asegurar la conformidad con requisitos | | | | | | |
| ME4 Proveer gobierno de las TI | | | | | | |

## Lo que fue aprendido

» Comprensión de los procesos del dominio DS

- DS1 Definir y gestionar niveles de servicios
- DS2 Gestionar servicios externos
- DS3 Gestionar el desempeño y la capacidad
- DS4 Asegurar la continuidad de los servicios
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar los usuarios
- DS8 Gestionar el centro de servicio y los incidentes
- DS9 Gestionar la configuración
- DS10 Gestión de problemas
- DS11 Gestionar los datos
- DS12 Gestionar el ambiente físico
- DS13 Gestionar las operaciones

» Comprensión de los procesos del dominio ME

- ME1 Monitorear y evaluar el desempeño de las TI
- ME2 Monitorear y evaluar los controles internos
- ME3 Asegurar la conformidad con requisitos externos
- ME4 Proveer gobierno de las TI

Capítulo

05

# Evaluación de la madurez de los procesos de CobiT

**Objetivos**

Capacitar a los alumnos a utilizar los conceptos de CobiT 4.1 por medio de una herramienta de evaluación de nivel de madurez de los procesos de las TI.

**Conceptos**

Madurez de procesos de las TI y herramientas de evaluación.

# Introducción

La implantación de un buen gobierno de las TI exige que la organización tenga conocimiento claro de la madurez de sus procesos de las TI. Para esto es necesario que se realice una evaluación del nivel de madurez de los procesos utilizando el modelo de madurez de CobiT 4.1 como referencia.

El modelo de madurez de los procesos de las TI de CobiT 4.1 está basado en un método para evaluar el área de las TI de una organización, permitiendo que ella sea clasificada desde un nivel de madurez no existente (0) hasta optimizado (5).

Esta sesión mostrará cómo evaluar la madurez de los procesos de las TI de CobiT 4.1 en las organizaciones, por medio de una herramienta capaz de identificar los niveles de madurez y los procesos prioritarios que deberán ser mejorados o implementados.

## 5.1 Evaluación del nivel de madurez

La evaluación del nivel de madurez de los procesos de las TI:

- Ofrece un enfoque para la identificación de los procesos críticos.
- Definir acciones de mejora alineadas con los objetivos estratégicos de las TI y de negocio.

La evaluación del nivel de madurez de los procesos brinda los medios para determinar si los procesos son eficaces en relación a sus objetivos, y para identificar las causas que pueden caracterizar la baja calidad en la ejecución de los procesos. Los resultados pueden ser usados para orientar las acciones de mejora o para determinar la implementación de nuevos procesos.

Los resultados de la evaluación de madurez de procesos de TI basado en CobiT 4.1 brindan información valiosa que pueden ayudar a la organización a planear, ejecutar y monitorear sus iniciativas de mejora y gestión de los procesos.

## 5.2 Beneficios de la evaluación

- Localizar las deficiencias en la estructura y en la gestión de los procesos y, consecuentemente, las causas de desempeño no satisfactorios.
- Mejorar la comprensión de las ganancias potenciales de la mejora de la gestión de procesos.
- Determinar la capacidad del proceso en la realización de sus propósitos.
- Proveer las bases y la orientación para el mejoramiento continuo en la ejecución y gestión de procesos de forma estructurada, priorizada y evolutiva.
- Seleccionar y combinar enfoques y técnicas de mejoramiento y gestión de procesos compatibles con cada etapa de madurez gerencial.
- Monitorear y evaluar los progresos en el mejoramiento de la gestión de procesos mediante evaluaciones sucesivas.

Con relación al mejoramiento continuo, la evaluación de madurez de los procesos permite trazar un camino de mejoras para cada organización y proceso de forma individualizada, seleccionando las técnicas compatibles con su actual estado de madurez.

A medida que la organización avanza en la escala de madurez de sus procesos de las TI, sus habilidades se desarrollan, sus metas de desempeño son redefinidas y ella sofistica sus enfoques, haciendo uso adecuado y de forma progresiva de una gran cantidad de técnicas de gestión y mejoramiento.

## 5.3 Descripción de la herramienta de evaluación

La herramienta de evaluación es utilizada para registrar la información y brindar de forma automática los niveles de madurez de cada proceso de las TI, abordando los cuatro dominios de CobiT 4.1 con sus 34 procesos y 210 objetivos de control.

La herramienta fue desarrollada en hoja de cálculo y puede ser ejecutada por las siguientes aplicaciones:

» MS-Excel 7.0 o superior
» *Open Office* 3.1 o superior

El aplicativo MS-Excel debe tener su licencia de uso de la empresa Microsoft, mientras el *Open Office* puede ser instalado gratuitamente.

Es importante que la información de las sesiones anteriores sea utilizada o el contenido del marco CobiT 4.1 para entender correctamente todos los procesos y los objetivos de control.

## 5.4 Utilización de la herramienta

Los puntos a seguir describen la funcionalidad de cada parte de la herramienta. Para iniciar, ejecute la herramienta utilizando una de las aplicaciones descritas anteriormente.

### 5.4.1 Guía resumida

Esta guía de planilla brinda una visión general de todos los dominios de CobiT 4.1. Los resultados presentados son originados automáticamente por la información ingresada en las demás guías.

La información presentada en esta guía es mostrada en la tabla 72 con la siguiente información:

» Identificación del dominio;
» El total de los objetivos de control del dominio evaluado;
» Madurez total del dominio, indicada por el promedio del nivel de madurez de todos los procesos del dominio;
» Relevancia, Estrategia e Impacto, REI: indica la media de la puntuación del dominio en relación a la relevancia del dominio para la TI, el alineamiento con la estrategia de la organización y el impacto de este dominio sobre los negocios de la organización.

Tabla 72. Guía resumida

| Área de tecnología de la información - madurez actual | | | |
|---|---|---|---|
| Resumen del dominio | | | |
| **BO - Planificar y Organizar** | | **Al - Adquirir e implementar** | |
| Objetivos de control | | Objetivos de control | |
| Total de los objetivos de control de CobiT | 74 | Total de los objetivos de control del CobiT | 40 |
| Modelo de madurez | | Modelo de madurez | |
| Madurez del dominio | 0 | Madurez del dominio | 0 |
| REI | | REI | |
| Media de la puntuación | 1 | Media de la puntuación | 1 |
| **DS - Entrega y Soporte** | | **MO - Monitorear y Evaluar** | |
| Objetivos de control | | Objetivos de control | |
| Total de los objetivos de control del CobiT | 71 | Total de los objetivos de control del CobiT | 25 |
| Modelo de madurez | | Modelo de madurez | |
| Madurez del dominio | 0 | Madurez del dominio | 0 |
| REI | | REI | |
| Media de la puntuación | 1 | Media de la puntuación | 1 |

## 5.4.2 Guía gráfica

Esta guía brinda una visión gráfica en formato de radar con el nivel de madurez de los procesos evaluados para cada dominio de CobiT 4.1.

La Figura 15 muestra el gráfico generado automáticamente con la información ingresada en las demás guías de la planilla.

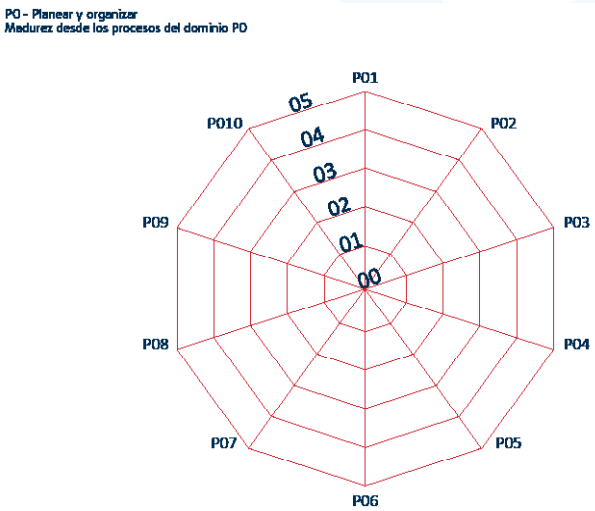



**Figura 15.** Gráficos (Dominio PO)

### 5.4.3 Guía REI: Relevancia, Estrategia e Impacto

En esa guía debe ser ingresada la información para determinar la relevancia, la contribución estratégica y el impacto de cada proceso de CobiT 4.1 para la TI y para la organización.

» Esta guía brinda los nombres de todos los procesos de CobiT 4.1, siendo necesario atribuir para cada proceso la siguiente información:
- Relevancia del proceso: indica qué tan importante es para la organización el proceso a ser evaluado.
- Contribución estratégica: indica cuánto contribuye el proceso evaluado a la estrategia de las TI, y en consecuencia, a la organización.
- Impacto: indica cuánto impacta el proceso ser evaluado sobre la organización en caso tal de que éste no estuviese siendo ejecutado correctamente o no exista en la organización.

El diligenciamiento de esta guía no debe ser simplemente el ingreso de los valores atribuidos a cada proceso evaluado. La selección de los criterios de evaluación debe ser realizado en cada celda de las columnas D, E y F.

La columna "resultado" muestra el resultado relacionado a las opciones seleccionadas para la relevancia, contribución estratégica e impacto.

Cuanto mayor sea el valor calculado para cada celda en este proceso, una prioridad más alta que necesita para tomar dentro de la organización.

Tabla 73. Guía REI

| | Levantamiento REI: Relevancia, Estrategia, Impacto | | | | |
|---|---|---|---|---|---|
| | PO: Planear y Organizar | | | | |
| PO: Planificar y Organizar | PO1 - Definir un plan estratégico de TI | Relevante | Poca contribución | Mucho impacto | 24 |
| | PO2 - Definir la arquitectura de la información | Poca relevancia | Contribuye con la estrategia | sin impacto | 6 |
| | PO3 - Determinar las directrices de tecnología | Relevante | Poca contribución | mucho impacto | 24 |
| | PO4 - Definir los procesos, la organización y las relaciones de TI. | Relevante | Esencial para la estrategia | Algún impacto | 30 |
| | PO5 - Gestionar la inversión en TI. | Irrelevante | No hay contribución | Sin impacto | 1 |
| | PO6 - Comunicar metas y directrices gerenciales. | Irrelevante | No hay contribución | Sin impacto | 1 |
| | PO7 - Gestionar los recursos humanos de TI | Irrelevante | No hay contribución | Sin impacto | 1 |
| | PO8 - Gestionar la calidad. | Irrelevante | No hay contribución | Sin impacto | 1 |
| | PO9 - Evaluar y gestionar los riesgos de TI. | Irrelevante | No hay contribución | Sin impacto | 1 |
| | PO10 - Gestionar proyectos. | Irrelevante | No hay contribución | Sin impacto | 1 |

### 5.4.4 Guía de tecnología de la información

- En esta guía deberá ser registrada la información relacionada a la evaluación de cada proceso de las TI.
- Para obtener el nivel de madurez actual será necesario evaluar cada objetivo de control de cada proceso.
- De esta forma, la evaluación será completa y tendrá mayor alcance.

Para diligenciar la información de esta guía es importante tener a mano el marco de CobiT 4.1 o la información de los objetivos de control de las sesiones 3 y 4.

La información de esta guía debe ser ingresada de la siguiente forma, conforme a la Tabla 74.

- El conjunto de columnas "cobertura" determina los objetivos de control para cada proceso y deberá ser diligenciado con los valores de 0 a 5 de acuerdo con la evaluación de madurez, sustituyendo o manteniendo el valor de (0) presente en cada celda. Para ingresar los valores es necesario leer cada objetivo de control de los procesos e ingresar el valor deseado.
- La columna "madurez evaluada" presente el nivel de madurez evaluado para cada proceso, de acuerdo con la información ingresada para cada objetivo de control.
- La columna "total de objetivos de control" muestra cuantos objetivos de control están siendo evaluados.
- El conjunto de columnas "madurez" es una referencia para diligenciar cada objetivo de control.

Tabla 74. Guía Tecnología de la Información

| Encuesta de madurez de tecnología de la información | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dominio ID | Procesos de TI | Alcance | | | | | | | | | | | | | | | | Madurez | | | | | | | |
| | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | Madurez evaluada | Total de objetivos de control | 0 - Inexistente | 1 - Inicial / 0 | 2 - Repetitivo / Intuitivo | 3 - Definidos | 4 - Gerenciados | 5 - Optimizados |
| PO - Planear y Organizar | | | | | | | | | | | | | | | | | | | | | | | | | |
| PO - Planear y Organizar | PO1 Definir un plan estratégico de TI | 5 | 4 | 3 | 5 | 2 | 0 | | | | | | | | | | 3.2 | 6 | | | | | | | |
| | PO2 Definir la arquitectura de la información | 4 | 5 | 3 | 2 | | | | | | | | | | | | 3.5 | 4 | | | | | | | |
| | PO3 Determinar las directrices de tecnología | 2 | 3 | 5 | 1 | 2 | | | | | | | | | | | 2.6 | 5 | | | | | | | |
| | PO4 Definir los procesos, la organización y las relaciones de TI | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 | 15 | | | | | | | |
| | PO5 Gestionar la inversión de TI | 0 | 0 | 0 | 0 | 0 | | | | | | | | | | | 0.0 | 5 | | | | | | | |
| | PO6 Comunicar metas y directrices gerenciales | 0 | 0 | 0 | 0 | 0 | | | | | | | | | | | 0.0 | 5 | | | | | | | |
| | PO7 Gerenciar los recursos humanos de TI | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | | | 0.0 | 8 | | | | | | | |
| | PO8 Gerenciar la calidad | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | | | | | 0.0 | 6 | | | | | | | |
| | PO9 Evaluar y gerenciar los riesgos de TI | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | | | | | 0.0 | 6 | | | | | | | |
| | PO10 Gerenciar proyectos | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | 0.0 | 10 | | | | | | | |
| | | | | | | | | | | | | | | | | | | 70 | | | | | | | |

### 5.4.5 Guía de Análisis de GAP

Esta guía muestra la brecha, el vacío (GAP), entre el nivel de madurez de cada proceso en la situación actual (columna "madurez evaluada") y la meta deseada para cada proceso (columna "meta deseada para el proceso").

- La meta deseada debe ser establecida y diligenciada en la columna "meta deseada para el proceso" para cada proceso, y puede tener valores diferentes, dependiendo de la estrategia de alcance de la meta.

Los valores de referencia para la evaluación son: 0 – inexistente, 1 – inicial, 2 – repetitivo/intuitivo, 3 – definido, 4 – gerenciado, 5 – optimizado.

- Los valores de la columna "madurez evaluada" son extraídos de la guía "tecnología de la información".
- La columna "GAP" brinda la diferencia entre la madurez evaluada y la meta deseada.

En cuanto mayor sea el GAP, mayor será el esfuerzo para alcanzar la meta

Tabla 75. Guía análisis GAP

| | Análisis de GAP | Madurez evaluada | Meta deseada para el proceso | GAP |
|---|---|---|---|---|
| PO - Planear y Organizar | | | | |
| PO - Planear y Organizar | PO1 Definir un plan estratégico de TI | 3,2 | 5,0 | 1,8 |
| | PO2 Definir la arquitectura de la información | 3,5 | 4,0 | 0,5 |
| | PO3 Determinar las directrices de tecnología | 2,6 | 4,0 | 1,4 |
| | PO4 Definir los procesos, la organización y las relaciones de TI | 0,0 | 0,0 | 0,0 |
| | PO5 Gestionar la inversión de TI | 0,0 | 0,0 | 0,0 |
| | PO6 Comunicar metas y directrices gerenciales | 0,0 | 0,0 | 0,0 |
| | PO7 Gerenciar los recursos humanos de TI | 0,0 | 0,0 | 0,0 |
| | PO8 Gerenciar la calidad | 0,0 | 0,0 | 0,0 |
| | PO9 Evaluar y gerenciar los riesgos de TI | 0,0 | 0,0 | 0,0 |
| | PO10 Gerenciar proyectos | 0,0 | 0,0 | 0,0 |

## 5.4.6 Guía de análisis de prioridad

Esta guía brinda el resultado de la evaluación del nivel de madurez de los procesos de las TI de CobiT 4.1.

La relación entre la columna "REI" y a la columna "GAP" define los procesos que deben ser priorizados para ser implantados o mejorados.

Es necesario establecer cuantos procesos de cada dominio serán priorizados. Una práctica adoptada es priorizar:

- 5 procesos del dominio PO
- 3 procesos del dominio AI
- 5 procesos del dominio DS
- 2 procesos del dominio ME

En cuanto mayor sea el índice REI y GAP, mayor es la prioridad del proceso.

## Lo aprendido

- Uso de herramientas para la evaluación de la madurez de los procesos de Gestión de las TI con base en CobiT 4.1
- Criterios de análisis del nivel de madurez de los procesos de gestión de las TI.

Capítulo

06

# Normas, estándares y reglamentos asociados al gobierno de las TI

**Objetivos**

Comprender la norma ISO/IEC 38500, los modelos Val IT y COSO, y las principales leyes, reglamentos y documentos del gobierno nacional que orientan al gobierno de las TI.

**Conceptos**

La tecnología de la información se ha convertido en un recurso estratégico para cualquier organización que quiera mantenerse competitiva en el mercado. En la mayoría de las organizaciones, muchas de las soluciones adoptadas no poseen estandarización, integración y desempeño satisfactorio, sin procesos de las TI definidos e implementados.

# Introducción

La tecnología de la información se ha convertido en un recurso estratégico para cualquier organización que quiera mantenerse competitiva en el mercado. En la mayoría de las organizaciones, muchas de las soluciones adoptadas no poseen estandarización, integración y desempeño satisfactorio, sin procesos de las TI definidos e implementados.

Por esto existe la necesidad de establecer un gobierno de las TI que identifique:

- La situación actual de la estructura, procesos, recursos, servicios y productos de las TI;
- Las nuevas necesidades de información alineadas a la estrategia de la organización;
- Los objetivos estratégicos y las directrices de las TI.

Además de metodologías y buenas prácticas, la ISO publicó en el 2009 la norma ISO/IEC 38500 para el gobierno de las TI.

Es importante que las organizaciones tengan los modelos y mejores prácticas asociadas con los reglamentos, normas y leyes como base para la implantación, monitoreo y mejora continua del gobierno de las TI.

Determinar el valor de las TI también es un papel importante del gobierno de las TI, de modo que el modelo Val IT establece procesos para ayudar a las organizaciones a dimensionar las inversiones en TI.

El modelo para la auditoría COSO y su relación con los procesos de CobiT 4.1 es indicado para que las organizaciones creen un ambiente de controles internos, proporcionando la evaluación de los riesgos y haciendo la gestión de los ejecutivos más eficiente y la toma decisiones más precisa.

Las organizaciones públicas deben seguir, además de las mejores prácticas de las TI, los reglamentos determinados por la administración pública para implementar efectivamente el gobierno de las TI.

## 6.1 Norma para gobierno de las TI - ISO/IEC 38500

El objetivo principal de la norma es apoyar a las organizaciones con un conjunto de principios para la evaluación, la gestión y el monitoreo del uso de las TI. Estos principios están alineados con los modelos y mejores prácticas al ejemplo de CobiT 4.1.

La norma está estructurada de la siguiente forma:

- Alcance, aplicación y objetivos.
- Estructura para un gobierno corporativo de las TI adecuado.
- Guía para el gobierno corporativo de las TI.

Los modelos y las mejores prácticas son cada vez más adoptados por las organizaciones en todo el mundo para la implementación del gobierno de las TI. En 2008 fue publicada la norma ISO/IEC 38500:2008 para que las organizaciones, además de usar los modelos y mejores prácticas, implementen el gobierno de las TI. En diciembre del 2009 fue ratificada la norma NTC ISO/IEC 38500 por el Consejo Directivo del Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, que es el organismo nacional de normalización, según el Decreto 2269 de 1993.

La norma trata sobre el uso efectivo de las TI para alcanzar los objetivos de negocios de la organización, el retorno de las inversiones en TI que la organización realiza, dónde gasta, cómo gasta y dónde invierte. La aplicación de la norma está destinada a todo tipo de organizaciones, públicas o privadas, de diferentes tamaños (pequeñas, medianas o grandes).

### 6.1.1 Alcance, aplicaciones y objetivos

Principales objetivos de la norma:

- Garantizar a todos en la organización (consumidores, accionistas, funcionarios y otros) que el gobierno de las TI será implementado siguiendo las orientaciones de la norma.
- Informar y orientar a todos en la organización sobre el uso de las TI en la ejecución de sus actividades y la contribución para los negocios.

Entre los principales objetivos de la norma está brindar indicadores para una evaluación objetiva del gobierno de las TI, y brindar a los ejecutivos y dirigentes de las organizaciones un conjunto de principios para el uso efectivo de las TI. La norma se aplica a todos los procesos de las TI definidos en la organización, cómo los procesos de CobiT 4.1, y puede ser usada como orientadora de acciones para:

- Gerentes y ejecutivos;
- Profesionales que hacen parte de grupos de monitoreo de recursos dentro de la organización;
- Especialistas externos, de negocios o técnicos;
- Proveedores de hardware, software e infraestructura de las TI;
- Proveedores internos y externos de servicios y consultores;
- Auditores de las TI.

La búsqueda de la aplicación de la norma, así como los modelos y mejores prácticas, no son privilegios de pocas organizaciones, dado que todas pueden intentar optimizar sus recursos de las TI, invirtiendo adecuadamente en busca de mejores resultados.

### 6.1.2 Beneficios del uso de la norma

La norma proporciona los siguientes beneficios:

- Destaca la importancia del gobierno de las TI para la organización, evaluando los riesgos involucrados y las inversiones en TI exigidas para el soporte de negocio.
- Incentiva a las organizaciones a usar los modelos de mejores prácticas adecuados para sustentar su gobierno de las TI.
- Establece un cuadro de seis principios básicos para que la organización evaluar, orientar y monitorear el uso de las TI.

Siguiendo estos principios los dirigentes de la organización tienen una visión sobre los riesgos y las oportunidades relacionadas a la utilización de las TI, pues la norma:

- Es aplicable para todas las organizaciones, menores o mayores, independientemente del propósito y de la estructura de propiedad (pública o privada).
- Aclara que el gobierno corporativo de las TI ayuda a garantizar la conformidad con las obligaciones (reglamentos, legislación, ley común, contractual), siendo útil para el desempeño de la organización.
- Indica que los sistemas de las TI inadecuados pueden exponer a la organización a los riesgos de no cumplir con la legislación vigente.

### 6.1.3 Definiciones

Las siguientes definiciones son aplicadas a la norma:

- **Aceptable:** atender las expectativas de la organización que pueden ser presentadas como razonables o merecedoras;
- **Gobierno corporativo:** sistema por el cual las organizaciones son dirigidas y controladas;
- **Gobierno corporativo de las TI:** sistema por el cual el uso actual y futuro de las TI es dirigido y controlado; involucra la evaluación y el direccionamiento del uso de las TI para dar soporte a la organización y monitorear su aplicación para alcanzar los objetivos de negocios.
- **Competente:** poseer la combinación de conocimiento, habilidades formales e informales, entrenamiento, experiencia y atributos comportamentales necesarios para desempeñar una tarea o papel.
- **Dirigente:** miembros de la más alta dirección de una organización (propietarios, consejo de administración, socios, ejecutivos y funcionarios designados).
- **Comportamiento humano:** comprensión de las interacciones entre seres humanos y los demás elementos de un sistema, con la intención de garantizar el bienestar y el desempeño de los sistemas. El comportamiento humano incluye cultura, necesidades y aspiraciones de personas como individuos y como grupos.
- **Tecnología de la Información, TI:** los recursos necesarios para adquirir, procesar, almacenar y diseminar información. Este término también incluye "Tecnología de la Comunicación, TC" y el

término compuesto de "Tecnología de la Información y de la Comunicación, TIC".

- **Inversiones:** la asignación de personas, capital y otros recursos para alcanzar los objetivos definidos y otros beneficios.
- **Gestión:** el sistema de controles y procesos necesarios para alcanzar los objetivos estratégicos de la organización.
- **Organización:** cualquier compañía, corporación, gobierno, entidades sin fines de lucro o de cualquier otro tipo, legalmente constituida, incluyendo asociaciones, clubes, sociedades, órganos gubernamentales y organizaciones privadas que tengan sus propias prácticas y administración.
- **Política:** instrucciones claras y medibles de dirección y comportamiento deseado que condicionen las decisiones tomadas dentro de la organización.
- **Propuesta:** compilación de beneficios, costos, riesgos, oportunidades y otros factores aplicables a las decisiones a ser tomadas.
- **Recursos:** personas, procedimientos, software, información, equipos, consumibles, infraestructura, capital y fondos de operación y tiempo.
- **Riesgo:** combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- **Parte interesada** (*stakeholder*): cualquier individuo, grupo u organización que puede afectar, ser afectado o tener la percepción de que será afectado por una decisión o actividad.
- **Estrategia:** plan general de desarrollo de la organización que describe el uso eficaz de los recursos para apoyar a la organización en sus actividades futuras. Involucra el establecimiento de objetivos y propuestas de iniciativas para ejecución.
- **Uso de las TI:** planeación, diseño, desarrollo, distribución, operación, gestión y aplicación de las TI para atender las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios de las TI por las unidades internas de negocio, unidades especializadas en TI o proveedores externos y servicios de utilidad (tales como proveer software como servicio).

## 6.2 Estructura para un adecuado gobierno corporativo de las TI

### 6.2.1 Principios

La norma establece seis principios de buen gobierno corporativo de las TI, siendo aplicados a la mayoría de las organizaciones.

**Principio 1: Responsabilidad**

» Todos en la organización deben comprender y aceptar sus responsabilidades con relación a la oferta y a la demandas de las TI.

Los procesos de negocios de la organización (cliente) y el área de las TI (proveedor) deben trabajar en conjunto, usando una comunicación eficaz con base en una relación positiva y de confianza y demostrando claridad y responsabilidad.

En organizaciones de gran tamaño, un comité ejecutivo de las TI (conocido formalmente como el comité de estrategias de las TI), compuesto por miembros de varios niveles de dirección de la organización, presidido por un miembro del propio comité, es un mecanismo eficaz para evaluar, orientar y monitorear el uso de las TI en asuntos críticos, incluyendo la priorización de demanda e inversiones. Las pequeñas y medianas organizaciones, que poseen una estructura más simple y flujos de comunicación más ágiles, deben adoptar un enfoque más directo para supervisar las actividades de las TI. La responsabilidad debe permear toda la estructura organizacional, iniciando por las capas de más alto nivel.

El ITGI apoya este principio con las siguientes publicaciones:

» La publicación "*Board Briefing on IT Governance and Unlocking Value: an Executive Primer on the Critical Role of IT Governance*" brinda orientación sobre los roles y responsabilidades del gobierno de las TI en los negocios y describe cómo establecer una estrategia de las TI eficaz.
» La matriz RACI incluida en CobiT 4.1 y en el Val IT muestra ejemplos de roles y responsabilidades relacionados a los procesos y actividades de las TI.
» La publicación "*The IT governance implementation guide: Using CobiT® and Val IT™*" explica las responsabilidades de las personas involucradas en la organización y en la implementación del gobierno de las TI.

El dominio: Monitorear y Evaluar, ME de CobiT 4.1 muestra como la organización puede acompañar y evaluar el gobierno de las TI y el desempeño de las TI por medio del proceso "ME4. Monitorear".

### Principio 2: Estrategia

» La planeación estratégica de las TI de la organización es un proceso complejo y crítico que exige alineamiento entre las unidades de negocios y el área de las TI.

La planeación estratégica es fundamental para priorizar los proyectos y recursos que aumenta el desempeño de la organización.

Los planes tácticos y operacionales agregan valor cuando están alineados a los objetivos estratégicos de la organización, teniendo en cuenta los riesgos asociados a la toma decisiones. Deben ser flexibles y adaptables para atender oportunamente los requisitos de negocios y de las TI.

Además de esto, la falta o no de recursos de las TI puede dificultar o facilitar las estrategias empresariales. Por eso, la planeación estratégica debe incluir una planificación de capacidades trasparente y adecuada de las TI. Esto debe incluir una evaluación de capacidad actual de la infraestructura y de los recursos humanos de las TI para apoyar las necesidades futuras de negocio, teniendo en cuenta el desarrollo tecnológico que permita una ventaja competitiva o la optimización de los costos.

Los recursos de las TI incluyen relaciones con proveedores de productos y servicios externos y prestadores de servicios, algunos de los cuales probablemente desempeñan un papel fundamental en el apoyo al negocio.

El ITGI apoya este principio con las siguientes publicaciones:

» La publicación "*Board Briefing on IT Governance and Unlocking Value: an Executive Primer on the Critical Role of IT Governance*" muestra como el comité de estrategias de las TI crea una planeación estratégica de las TI alineada con la planificación estratégica de la organización, y como el área de negocios y el área de las TI deben trabajar juntas para producir el mejor resultado para la organización.

» El modelo Val IT ofrecer una guía específica para la gestión de las inversiones de las TI y muestra como los objetivos estratégicos de la organización son soportados por los procesos de negocios.

El dominio de CobiT 4.1 Planear y Organizar, PO, muestra los procesos necesarios para planear y organizar los recursos de las TI, incluyendo planeación estratégica, organizacional, de arquitectura tecnológica, de inversiones, además de la gestión de riesgos, de calidad y de proyecto.

» El alineamiento entre los objetivos de negocios y objetivos de las TI también es mostrado, a través de ejemplos genéricos de soporte a los objetivos estratégicos.

### Principio 3: Adquisición

» Las soluciones de las TI existen para soportar los procesos de negocio.
» Es preciso tener cuidado para no considerar las soluciones de las TI de forma aislada o como un simple "proyecto de tecnología" o servicio.

Por otro lado, una elección inadecuada de la arquitectura tecnológica, la incapacidad de mantener una infraestructura adecuada o la ausencia de recursos humanos calificados son factores que pueden resultar en el fracaso del proyecto, incapacidad para sustentar las operaciones o reducción en el valor para el negocio.

La tecnología adquirida también debe soportar y operar con los procesos de negocio e infraestructura de las TI existentes. La implementación de una nueva adquisición de las TI no es apenas una cuestión de tecnología, y si una combinación de cambio organizacional, revisión de procesos de negocio y entrenamiento.

Los proyectos de las TI deben ser realizados como parte de un amplio programa de cambio organizacional, que incluye otros proyectos que satisfacen todas las actividades necesarias para alcanzar el resultado esperado por la organización.

El ITGI apoya este principio con las siguientes publicaciones:

- El dominio IM de Val IT brinda orientaciones sobre la gestión de inversiones de las TI en las organizaciones.
- El dominio de gestión de portafolio, PM, aborda la aplicación del programa de inversiones en el portafolio para garantizar el alcance de los beneficios y la optimización de los costos.

El dominio PO de CobiT 4.1 brinda orientaciones para la planificación de la adquisición, incluyendo planificación de programas, de proyectos, de inversiones y de calidad, además de la gestión de riesgos.

El dominio Adquirir e Implementar, AI, orienta, por medio de los procesos, la adquisición e implementación de soluciones de las TI, abarcando la definición de requisitos, la identificación de soluciones viables, la elaboración de documentación y el entrenamiento de usuarios para la operación de nuevos sistemas.

Además de esto, se ofrecen orientaciones para ayudar a garantizar las pruebas y controles adecuados de las soluciones, y también el modo en que los cambios son aplicados a los negocios y al ambiente operacional de las TI.

### Principio 4: Desempeño

La medición eficaz del desempeño es un asunto técnico complejo y, por esto, es importante para alcanzar la trasparencia, expresando objetivos, métricas e informes de desempeño en un lenguaje claro para las partes interesadas, para que las acciones apropiadas puedan ser tomadas. Depende de dos aspectos fundamentales: la definición clara de metas de desempeño y el establecimiento de métricas eficaces para acompañar la concretización de los objetivos. El proceso de evaluación de desempeño también es necesario para ayudar a garantizar que el desempeño sea monitoreado de forma consistente y confiable.

El gobierno eficaz es alcanzado cuando:

- Las metas son definidas de arriba para abajo y alineadas con el nivel superior de los objetivos de negocio.
- Las métricas son establecidas de abajo para arriba y alineadas en forma que permitan la realización de las metas en todos los niveles de la organización que serán monitoreados por cada nivel de gestión.

Dos factores críticos del éxito del gobierno:

- La aprobación de metas por las partes interesadas.
- La aceptación de la responsabilidad para la realización de metas por directores y gerentes.

El ITGI apoya este principio con las siguientes publicaciones:

- El modelo CobiT 4.1 y Val IT brindan ejemplos genéricos de metas y métricas de procesos para TI y presentan como ellos se relacionan con los objetivos de negocio, permitiendo a las organizaciones adaptarlos para su uso específico.

CobiT 4.1 brinda orientaciones sobre el alineamiento de los objetivos de las TI con los objetivos de negocio y describe como monitorear el desempeño de estos objetivos usando las metas y métricas.

- En el proceso "ME1. Monitorear y evaluar el desempeño de las TI", CobiT brinda orientaciones sobre las responsabilidades de gestión ejecutiva para esta actividad.
- En el proceso "ME4. Proveer gobierno de las TI" CobiT brinda orientaciones sobre el monitoreo del gobierno de TI.
- El modelo Val IT brinda orientaciones y ejemplos específicos para el acompañamiento del desempeño de una inversión en TI a través de su ciclo de vida económico.
- El "*IT Assurance Guide: Using CobiT*" brinda información sobre la garantía del desempeño de las TI.

Dos procesos de CobiT 4.1 brindan orientaciones específicas:

- "PO1 - Definir un plan estratégico de las TI" se concentra en establecer metas.
- "DS1 - Definir y gestionar niveles de servicio" incide sobre la definición de servicios adecuados y objetivos de servicio, y su documentación en SLA.

### Principio 5. Conformidad

- En el actual mercado global, facilitado por el internet y tecnologías avanzadas, las organizaciones necesitan cumplir una creciente serie de requisitos legales y reglamentarios.

Por causa de escándalos corporativos y fracasos financieros en los últimos años, existe una mayor concientización en las organizaciones para

el cumplimiento de las leyes y reglamentaciones. Las partes interesadas exigen mayor garantía del cumplimiento de las organizaciones de las disposiciones legislativas y reglamentarias y en conformidad con prácticas de buen gobierno corporativo en su ambiente operacional. Además de eso, existe la necesidad de asegurar el cumplimiento de requisitos legales relacionados a TI en áreas como la privacidad, confidencialidad, propiedad intelectual y de seguridad.

Los dirigentes de las organizaciones necesitan garantizar que el cumplimiento de las exigencias externas sea tratado como parte de la planificación estratégica. Ellos también necesitan definir el posicionamiento de la alta dirección y establecer políticas y procedimientos para la gestión de personal, garantizando que las metas de las organizaciones sean realizadas y los riesgos minimizados.

La alta administración debe mantener el equilibrio entre el desempeño y la conformidad, asegurando metas de desempeño qué no comprometan el cumplimiento y, inversamente, que la conformidad sea adecuada y no restrinja excesivamente el negocio.

El ITGI apoya este principio con las siguientes publicaciones:

- La publicación "*The IT Assurance Guide: Using CobiT*" explica cómo los auditores independientes pueden proveer garantía de conformidad y adherencia a las políticas internas derivadas de directrices internas o externas legales, reglamentarias o requisitos contractuales, confirmando que las medidas necesarias para corregir eventuales vacíos hayan sido tomadas oportunamente por el propietario del proceso.
- La conformidad involucra decisiones de inversión; en Val IT, específicamente por medio del *Value Governance*, VG, 1 y 3, PM 1 y 4 *Investment Management*, IM, 4.

Los objetivos de control de CobiT 4.1 brindan una base para la creación de un ambiente de evaluación de la adecuación de los controles de TI en la organización. Los modelos de madurez de gestión permiten evaluar y medir la capacidad de los procesos de las TI.

- El proceso "PO1 - Definir un plan estratégico de las TI" ayuda a garantizar el alineamiento entre los planes de las TI y los objetivos de negocio, incluyendo los requisitos para el gobierno.
- El proceso "ME2 - Monitorear y evaluar los controles internos" apoya la TI a evaluar si los controles son adecuados para atender los requisitos de conformidad.
- El proceso "ME3 - Asegurar la conformidad con requisitos externos" ayuda a identificar los requisitos de conformidad externa.

### Principio 6: comportamiento humano

» La implementación de cambios autorizados por TI, incluyendo el gobierno de las TI, generalmente exige un cambio cultural y de comportamiento en las organizaciones, así como de clientes y organizaciones asociadas.

La exigencia de cambio en la cultura y en el comportamiento puede generar miedo e inseguridad en las personas. Así, la implementación debe ser gestionada con cuidado, para que las personas se mantengan comprometidas. La administración de la organización debe comunicar claramente los objetivos, apoyando positivamente las alteraciones propuestas.

Formación y valoración de competencias de personal son aspectos claves de cambio, especialmente teniendo en cuenta la rápida evolución de la tecnología. Las personas son afectadas por el cambio en todos los niveles de la organización. El cambio afecta también a los clientes y socios de negocio y permite que cada vez más las operaciones entre las organizaciones se han automatizadas.

Al soportar los procesos de negocio para atraer nuevos beneficios y oportunidades, la TI también debe estar atenta al aumento de los riesgos. Situaciones relacionadas a la privacidad y al fraude están creciendo, entre otros riesgos que necesitan ser gestionados para que las personas tengan confianza en los sistemas informatizados que usan.

Los sistemas de información también pueden afectar las prácticas de trabajo, por medio de la automatización de procesos manuales. El instituto para el gobierno de las TI apoya este principio con las siguientes publicaciones:

» Val IT, Capítulos 6: "*Functional Accountabilities and Responsibilities*" enfatiza la necesidad de entender los cambios requeridos relacionados a las inversiones en gobierno de las TI y los respectivos cambios.
» El proceso "PO4. Definir los procesos, la organización y las relaciones de las TI" es desarrollado y mantenido para atender las necesidades y exigencias del personal en todos los niveles.
» El proceso "PO6. Comunicar metas y directrices gerenciales" para garantizar que las metas y objetivos son claramente comunicados, y que la cultura de trabajo promueve la actitud correcta con relación al riesgo y su control.
» El proceso "PO7. Gestionar los recursos humanos de las TI" brinda información sobre el alineamiento entre el desempeño indi-

vidual y los objetivos de la organización, formas de mantener un especialista en TI y definición de roles y responsabilidades.

- El proceso "AI2. Adquirir y mantener software aplicativo" ayuda garantizar el proyecto de aplicaciones que satisfagan a los usuarios y sus requisitos de negocios.
- El proceso "AI4. Habilitar operación y uso" ayuda a garantizar que los usuarios están aptos para usar los sistemas de forma efectiva.
- El proceso "DS7. Educar y entrenar usuarios" brinda información de cómo identificar a las necesidades de entrenamiento de los usuarios, garantizando una utilización eficaz de los sistemas de las TI.
- El proceso "ME2. Monitorear y evaluar los controles internos" ayuda a monitorear los controles internos y el desempeño de las personas por medio de informes de acompañamiento gerencial.

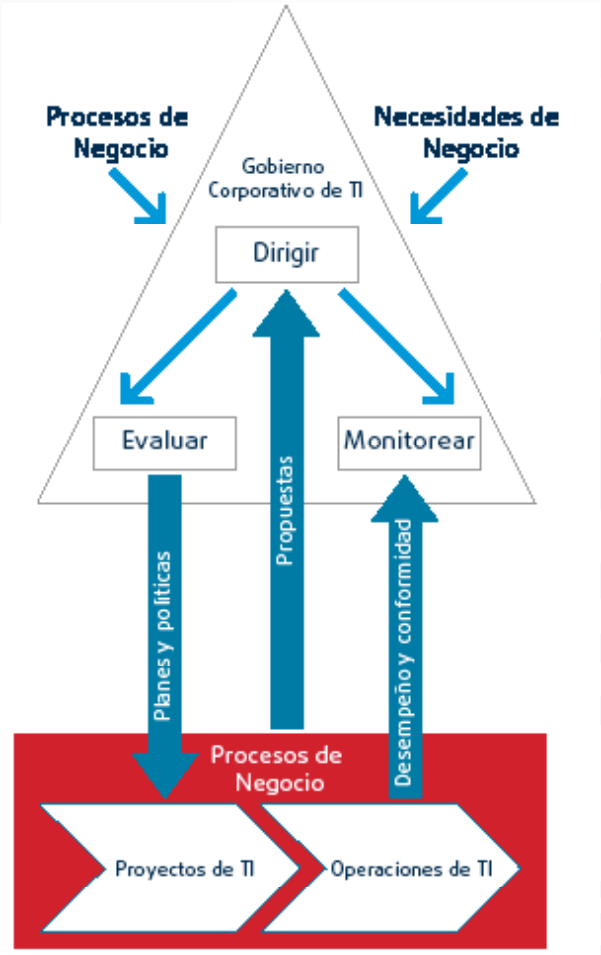
### 6.2.2 Modelo

La ISO/IEC 38500 recomienda tres tareas principales para el gobierno de las TI:

- Evaluar el uso actual y futuro de las TI.
- Dirigir y orientar la preparación y la implementación de planes y políticas para asegurar que el uso de las TI atienda los objetivos de negocio.
- Monitorear en el cumplimiento de las políticas y el desempeño en relación a los planes.

La ISO/IEC 38500 recomienda que los administradores de las TI realicen el gobierno a través de tres tareas principales, como muestra la siguiente figura:

Figura 16. Relación entre el gobierno de las TI y los procesos de negocio




La implementación de un enfoque de gobierno de las TI eficaz es facilitada cuando:

- Está alineada con los estándares y prácticas aceptadas de gobierno corporativo de las TI.
- Está alineada con el enfoque de la organización para alcanzar el gobierno.
- Abarca todos los aspectos relacionados con las actividades del área de las TI.

» Está basada en principios y objetivos que pueden ser entendidos y aplicados por todos los interesados.

El área de las TI recibe requerimientos de las áreas de negocios, que poseen necesidades específicas que impulsan la organización. El gobierno corporativo de las TI debe proveer mecanismos para recibir los requerimientos del negocio y realizar el alineamiento con los procesos establecidos, con el fin de garantizar que los proyectos y las operaciones de las TI soporten las necesidades de la organización. De esta forma, las tres principales tareas del gobierno corporativo de las TI descritas en la norma son fundamentales para establecer el alineamiento necesario entre TI y los negocios.

## 6.3 Guía para el gobierno corporativo de las TI

La dirección de la organización debe realizar el gobierno de las TI de acuerdo con los principios y las siguientes tareas.

**Principio 1: Responsabilidad**

- » Evaluar
  - Evaluar las opciones de delegación de responsabilidades en el uso de las TI que apoyan los objetivos del negocio.
  - Evaluar la competencia de aquellos a los cuales fue delegada la responsabilidad para la toma de decisión en relación con TI.
- » Dirigir
  - Cumplir los planes establecidos para TI de acuerdo con las responsabilidades del área.
  - Recibir informaciones para atender las responsabilidades y compromisos.
- » Monitorear
  - Monitorear el gobierno de las TI.
  - Monitorear la delegación de responsabilidades.
  - Monitorear el desempeño de aquellos a los cuales fue delegada la responsabilidad por el gobierno de las TI.

### Principio 2: Estrategia

- Evaluar
  - Evaluar el desarrollo de sistemas y los procesos de negocios asociados, garantizando el soporte de las TI a los negocios.
  - Evaluar las actividades de las TI para asegurar que estén alineadas con los objetivos de la organización con relación a los cambios circunstanciales, que lleven a considerar el uso de mejores prácticas y satisfagan otros requisitos de las partes interesadas.
  - Evaluar la utilización de las TI en relación a los riesgos.
- Dirigir
  - Liderar la preparación y el uso de planes y políticas que aseguren que la organización sea beneficiada por el desarrollo de las TI.
  - Estimular la presentación de propuestas para usos innovadores de las TI que permitan que la organización pueda responder a nuevas oportunidades y desafíos, emprender nuevos negocios o mejorar procesos existentes.
- Monitorear
  - Monitorear el progreso de las propuestas de las TI aprobadas para garantizar que alcancen sus objetivos dentro de los plazos exigidos, utilizando los recursos disponibles.
  - Monitorear el uso de las TI para asegurar que los beneficios pretendidos están siendo alcanzados.

### Principio 3: Adquisición

- Evaluar
  - Evaluar las opciones de provisión a  TI con el fin de alcanzar los objetivos de las propuestas aprobadas, buscando el equilibrio entre los riesgos y el retorno sobre las inversiones propuestas.
- Dirigir
  - Dar la debida orientación para que los activos de las TI (sistemas e infraestructura) sean adquiridos de forma apropiada, incluyendo la preparación de documentación adecuada que asegure la provisión  de las capacidades necesarias.
  - Asegurarse de que los acuerdos de provisión (internos y externos) darán soporte a las necesidades de la organización.
- Monitorear
  - Monitorear las inversiones de las TI para asegurar la provisión de las capacidades requeridas.
  - Monitorear hasta qué punto la dirección y los proveedores

mantienen una comprensión mutua de las intenciones de la organización para hacer cualquier adquisición de las TI.

### Principio 4: Desempeño

- » Evaluar
  - Evaluar proposiciones para asegurar que la TI apoyará los procesos de negocios con la capacidad requerida
  - Evaluar los riesgos a la continuidad de operación resultante de la actividad de las TI.
  - Evaluar los riesgos a la integridad de la información y a la protección de los activos de TI.
  - Evaluar la garantía de que el uso de las TI sea adecuado.
  - Evaluar el desempeño del gobierno de las TI
- » Dirigir
  - Asegurar que los recursos sean asignados para garantizar que TI atienda las necesidades de la organización.
  - Orientar a los responsables de las TI sobre las necesidades de mantener los datos actualizados y seguros.
- » Monitorear
  - Monitorear el soporte de las TI al negocio.
  - Monitorear los recursos y las inversiones alineadas con los objetivos de negocio.
  - Monitorear la exactitud de datos e información.

### Principio 5: Conformidad

- » Evaluar
  - Evaluar el cumplimiento de las obligaciones de las TI (leyes y reglamentos).
  - Evaluar la conformidad de gobierno de las TI.
- » Dirigir
  - Garantizar que el uso de las TI este de acuerdo (en conformidad) con las exigencias legales (leyes y reglamentos)
  - Cumplir las políticas establecidas en el uso de las TI.
  - Exigir a los profesionales de las TI comportamiento profesional, con ética y responsabilidad.
- » Monitorear
  - Monitorear el cumplimiento de conformidad de las TI, por medio de informes y auditorías.
  - Monitorear las actividades de las TI de acuerdo con los reglamentos ambientales y de seguridad, principalmente en el descarte de activos de las TI (hardware y software).

### Principio 6: Comportamiento humano

- Evaluar
  - Evaluar las actividades de las TI con relación al comportamiento humano.
- Dirigir
  - Garantizar que las actividades de las TI sean compatibles con las diferencias de comportamiento.
  - Permitir que los riesgos y oportunidades puedan ser identificados y comunicados por cualquier miembro de la organización
- Monitorear
  - Monitorear el comportamiento de las personas y realizar ajustes comportamentales.
  - Monitorear el cumplimento de todos los procedimientos y procesos de trabajo.

Los siguientes documentos publicados por el ITGI soportan las tres principales tareas recomendadas en la norma IOS/IEC 38500.

### Evaluar

- Las publicaciones "*The Board Briefing on IT Governance*" y "*Unlocking Value: an Executive Primer on the Critical Role of IT Governance*" describen lo que la alta dirección de la organización debe hacer en relación con el gobierno de las TI, cuál debe ser su alcance, las preguntas que necesitan ser respondidas y la forma de comparar la propia organización con las mejores prácticas.
- Los modelos CobiT 4.1 y Val IT brindan una base para evaluar la adecuación de los controles y prácticas de gestión de las TI, así como evaluar y medir la capacidad de los procesos de las TI.
- La publicación "*Identify Needs and Envision Solution phases of the IT Governance Implementation Guide: Using CobiT and Val IT*" muestra cómo evaluar el soporte de las TI a los negocios y cómo realizar un análisis de brechas por medio de buenas prácticas.
- La publicación "*CobiT quickstart*" brinda una guía para pequeñas, medianas y grandes organizaciones que desean evaluar las prácticas de gobierno de las TI.
- La publicación "*Enterprise VALUE: Governance of IT Investment, Getting Started With Value Management*" ayuda a evaluar las necesidades de negocio y gestionar mejor las inversiones relacionadas con TI.

» La publicación "*Enterprise VALUE: Governance of IT Investment, The Business Case*" ayuda a crear un caso de negocio para proveer al gobierno de las TI.
» La publicación "*IT Assurance Guide: Using CobiT*" habilita a los profesionales de las TI para la adopción de la ISO/IEC 38500.

### Dirigir

» Las publicaciones "*The Board Briefing on IT Governance*" y "U*nlocking Value: an Executive Primer on the Critical Role of IT Governance*" describen como la alta dirección de la organización puede conducir el gobierno de las TI.
» Las publicaciones CobiT 4.1 y Val IT brindan una guía de implementación en forma de objetivos de control y prácticas de gestión que deben ser considerados para proveer un gobierno de las TI adecuado.
» La publicación "*IT Governance Implementation Guide. Using CobiT and Val IT*" muestra como la organización debe priorizar y planear la implantación de gobierno de TI.
» La publicación "*CobiT quickstart*" presentar las recomendaciones y controles para pequeñas, medianas y grandes organizaciones que desean iniciar la implementación de gobierno de las TI.
» Para las organizaciones en donde la seguridad es altamente requerida, la publicación "*CobiT Security Baseline*" brinda una guía rápida para direccionar la implementación de los principales controles de seguridad de las TI alineados con la norma de seguridad ISO/IEC 27002.

### Monitorear

» Las publicaciones "*The Board Briefing on IT Governance*" y "*Unlocking Value: an Executive Primer on the Critical role of IT Governance*" describen como la alta dirección de la organización debe realizar el monitoreo eficaz del gobierno de las TI.
» Los procesos del dominio "Evaluar y Monitorear, ME" de CobiT 4.1 son una guía para las organizaciones en el monitoreo del gobierno de las TI.
» Los modelos CobiT 4.1 y Val IT poseen ejemplos de metas y métricas para soportar el monitoreo de los procesos de gobierno de las TI alineados con los objetivos y metas de los negocios.
» La publicación "*IT Governance Implementation Guide. Using CobiT and Val IT*" muestra como el gobierno de las TI se debe ajustar a las operaciones de negocios y como monitorear y medir el

éxito de la implementación del gobierno de las TI.

» La publicación "*IT Assurance Guide: Using CobiT*" habilita a los profesionales a alcanzar una opinión independiente en la gestión del desempeño y conformidad, brindando un método y ejemplos de pruebas para conducir auditorías.

## 6.4 El modelo Val IT

Val IT es una guía de procesos y prácticas para ayudar a los ejecutivos en la comprensión de sus roles y responsabilidades relacionados a las inversiones en TI.

El modelo Val IT ayuda a las organizaciones en la comprensión de las inversiones de las TI buscando responder las siguientes preguntas para cuatro asuntos específicos:

» Estrategia

- ¿Las inversiones en estrategia de las TI están alineadas con la visión de la organización?
- ¿Las inversiones son consistentes con los principales objetivos de negocios?
- ¿Las inversiones contribuyen a los objetivos estratégicos de la organización?
- ¿Las inversiones contribuyen en la entrega de valor de los servicios de las TI, con los costos deseados y dentro de un margen aceptable de riesgo?

» Arquitectura de las TI

- ¿Las inversiones están alineadas con la arquitectura de las TI de la organización?
- ¿Las inversiones son consistentes con los principios de arquitectura de las TI de la organización?
- ¿Las inversiones contribuyen en la utilización consciente de la arquitectura de las TI?
- ¿Las inversiones en arquitecturas de las TI están alineadas con otras iniciativas de la organización?
- Valor de las TI
- ¿La organización tiene una comprensión clara de los beneficios esperados por las inversiones en TI?
- ¿La organización tiene una comprensión clara de la respon-

sabilidad para alcanzar los beneficios de las inversiones en TI?
- ¿La organización tiene métricas para medir el valor que la TI entrega al negocio?

» Entrega

- ¿La organización tiene una comprensión de las entregas del servicio de las TI para soportar los negocios?
- La organización tienen competencia, disponibilidad y recursos para entregar:
- ¿La capacidad requerida por el negocio?
- ¿Los cambios organizacionales requeridos para soportar el negocio?

El objetivo del modelo Val IT, creado por ITGI, es apoyar las organizaciones en la gestión de las inversiones en TI, de manera que el valor generado por TI para soportar los negocios sea plenamente conocido.

El concepto de valor no es algo simple de definir, pues es dinámico y complejo. El concepto de valor también diverge para diferentes tipos de organizaciones. Para organizaciones privadas, el valor tiende a ser entendido y principalmente en términos financieros, lo que puede estar asociado al aumento de lucro de la organización que es soportado por las inversiones realizadas.

Para una organización pública, la definición de valor es más compleja y frecuentemente de naturaleza no financiera. Debe ser la mejora en el desempeño de la organización en relación a las métricas del negocio o al aumento líquido de la renta disponible para brindar los servicios que surjan de  la inversión.

Las organizaciones pueden optar por utilizar definiciones y significados diferentes para el concepto de valor. El Val IT define los siguientes términos para la comprensión del Valor de las TI:

» **Valor:** el resultado final esperado por los usuarios de negocios que utilizan un servicio habilitado por las inversiones en TI, pudiendo ser financieros, no financieros o una combinación de los dos.
» **Portafolio:** un grupo de programas, proyectos, servicios o bienes seleccionados, gestionados y monitoreados para optimizar el retorno sobre las inversiones para el negocio. Es importante indicar que el énfasis inicial de Val IT está principalmente en un portafolio de programas. CobiT 4.1 está interesado en portafo-

lios de proyectos, servicios o activos.

» **Proyecto:** un conjunto estructurado de actividades relacionadas con la entrega de un producto o servicio para la organización (lo que es necesario, pero no suficiente para alcanzar el resultado exigido) con base en un cronograma y presupuesto acordados previamente.
» **Implementar:** incluye ciclo de vida económico del programa de inversiones.

### 6.4.1 Principios de Val IT

**Principios fundamentales de Val IT:**

» Las inversiones en TI serán gestionadas por un portafolio de inversiones.
» Las inversiones en TI deben incluir todo el conjunto actividades necesarias para alcanzar el valor del negocio.
» Las inversiones en TI serán gestionadas a través de un ciclo de vida económico.

**Según el Val IT, las prácticas de valor de las TI deben:**

» Reconocer diferentes categorías de inversiones que serán evaluadas y gestionadas de forma diferente.
» Definir y monitorear indicadores de inversiones en TI y responder rápidamente a cualquier alteración o desvío.
» Involucrar a todos los interesados y asignar responsabilidades adecuadas para la presentación de cuentas.
» Monitorear, evaluar y proveer el mejoramiento continuo.

**Siendo que CobiT 4.1 se enfoca en la ejecución:**

» ¿La organización está actuando de forma correcta?
» ¿La organización está haciendo las cosas de forma correcta?


**Figura 17.**
Relación entre Val IT y CobiT. 4.1

Para obtener el retorno de las inversiones de las TI, el Val IT debe ser aplicado en las organizaciones por los siguientes dominios:

» Gobierno de Valor, VG.

- El objetivo de este dominio es optimizar el valor en la organización por las inversiones en TI de la siguiente forma:
  - Establecer el gobierno, monitoreo y una estructura de control.
  - Brindar direccionamiento estratégico sobre las inversiones.
  - Definir un portafolio de inversiones.

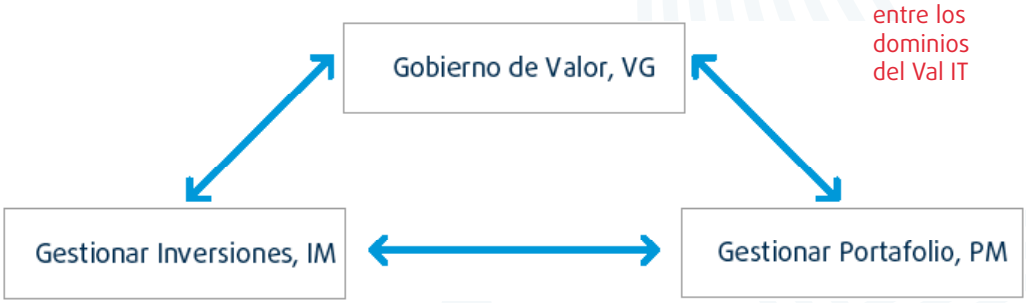
» Gestionar Portafolio, PM.

- El objetivo de este dominio es garantizar un portafolio de las inversiones de las TI alineado con los objetivos estratégicos del organización, de la siguiente forma:
  - Establecer y gestionar perfiles de recursos.
  - Definir los límites de las inversiones en TI.
  - Evaluar, priorizar, seleccionar, posponer o rechazar una nueva inversión de las TI.
  - Gestionar completamente el portafolio de inversiones.
  - Monitorear y presentar los resultados del desempeño del portafolio de inversiones en TI.

» Gestionar Inversiones, IM.

- El objetivo de este dominio es garantizar que la organización gestione las inversiones de las TI dentro de los criterios de costos establecidos y con el conocimiento de los niveles de riesgo asociados a las inversiones de las TI, de la siguiente manera:
  - Identificar requisitos de negocios.
  - Entender claramente el programa de inversiones en TI.
  - Definir el programa inversiones en TI y detallar claramente los planes de negocios, con los beneficios asociados.
  - Gestionar el programa de inversiones en TI por medio de un ciclo de vida económico.
  - Monitorear y presentar los resultados de desempeño del programa de inversiones en TI.

**Figura 18.** Relación entre los dominios del Val IT




Los dominios de VAL IT 2.0 están constituidos por procesos como se muestra en la siguiente tabla:

Tabla 76. Dominios y procesos

| Dominio: Gobierno de Valor, VG | |
|---|---|
| VG1. | Establezca un liderazgo informado y comprometido |
| VG2. | Definir e implementar procesos |
| VG3. | Definir características del portafolio |
| VG4. | Alinear e integrar la gestión de valor con la planificación financiera de la organización. |
| VG5. | Establecer el monitoreo efectivo del gobierno. |
| VG6. | Continuamente mejore prácticas de gestión de valor. |

Continuación tabla 76. Dominios y procesos

| | |
|---|---|
| **Dominio: Gestionar Portafolio, PM** | |
| PM1. | Establecer direccionamiento estratégico y mezcla de inversiones objetivo. |
| PM2. | Determinar disponibilidad y fuentes de fondos. |
| PM3. | Gestionar la disponibilidad de los recursos humanos. |
| PM4. | Evaluar y seleccionar programas para invertir. |
| PM5. | Monitorear y reportar el desempeño del portafolio de inversiones. |
| PM6. | Optimizar el desempeño del portafolio de inversiones. |
| **Dominio: Gestionar Inversiones, IM** | |
| IM1. | Desarrollar y evaluar el caso de negocio del programa inicial. |
| IM2. | Entender el programa candidato y las opciones de implementación. |
| IM3. | Desarrollar un plan de programa. |
| IM4. | Desarrollar un ciclo de vida completo de costos y beneficios. |
| IM5. | Desarrollar el caso de negocio detallado del programa. |
| IM6. | Lanzar y gestionar el programa. |
| IM7. | Actualizar el portafolio operacional de las TI. |
| IM8. | Actualizar el caso de negocio |
| IM9. | Monitorear e informar sobre el programa. |
| IM10. | Retirar el programa |

## 6.5 Visión general del modelo COSO

El proceso regulatorio relacionado a los controles internos tiene un marco importante relacionado con la Ley aprobada por el congreso norteamericano en diciembre en 1987, llamada *Foreign corrupt practices act*, FCPA, dedicada a sociedades anónimas por acciones. Las organizaciones bajo la FCPA están obligadas a crear, implementar y mantener sistemas de control que ofrezcan garantías de que las transacciones serán registradas en conformidad con los principios contables.

Los auditores independientes advierten que la administración debe establecer una estructura de control interno compuesta por tres elementos:

- Ambiente de control;
- Sistema contable;

» Procedimientos de control.

Un estudio hecho por la *Treadway Commission* estableció una recomendación, en el sentido del desarrollo de una definición común de control interno con directrices procesales. Entonces fue creado el *Comitte of Sponsoring Organizations*, COSO (comité de las organizaciones patrocinadoras). Se trata de una organización sin ánimo de lucro, dedicada a la mejora de los informes financieros, principalmente por la aplicación de la ética y de la efectividad en el cumplimiento de los controles internos. Es patrocinado por cinco de las principales asociaciones de clase de profesionales relacionados al área financiera en los Estados Unidos.

El modelo presentado por COSO en 1992 es actualizado en 1994 (*Internal Control – Integrated framework*), actualmente conocido como COSO 1, definió el control interno y elaboró de criterios para la evaluación de los sistemas. COSO 1 hace responsable del proceso de control interno al consejo directivo, a la administración y a los funcionarios de la entidad.

Definición del control interno según COSO:

» Un proceso desarrollado para garantizar, con razonable certeza, que sean alcanzados los objetivos de la organización, en las siguiente categorías:

- Eficacia y eficiencia en las operaciones.
- Confiabilidad en los registros contables y financieros.
- Conformidad con leyes y reglamentos.

COSO 1 sugiere también que la evaluación del proceso de control interno deba ser permanente a lo largo del tiempo (trimestral, anual etc.)

El modelo define que un sistema de control interno debe tener cinco componentes relacionados:

» Ambiente de control, con énfasis en la estructura organizacional y en las relaciones con el ambiente externo.
» Evaluación del riesgo.
» Actividad de control (políticas y procedimientos).
» Información y comunicación.
» Monitoreo.

Posterior a COSO, el FCPA emitió el SAS 78 (*Statement of Auditing Standard* - Declaración Estándar de Auditoría), que adhiere a COSO 1, y que se convirtió en un estándar para las organizaciones de auditoría. CobiT 4.1 surgió a partir del modelo COSO 1.

COSO 1, SAS 78 y CobiT 4.1 hacen énfasis en que la administración es responsable por establecer, mantener y monitorear el sistema de control interno de una organización.

COSO tuvo una revisión técnica, llamada *Enterprise Risk Management Framework*, ERM, conocida como COSO 2. Este documento está estructurado en ocho componentes principales:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos
- Evaluación del riesgo
- Respuesta al riesgo
- Evaluación de control
- Información y comunicación
- Monitoreo

El control interno está formado por cinco elementos interrelacionados:

- Ambiente de control
- Evaluación del riesgo
- Control de actividades
- Información y comunicación
- Monitoreo

### 6.5.1 Ambiente de control

COSO crea las bases para un control interno eficaz en la estructura de gobierno de la organización. Las cuestiones que surgen en los ambientes de control se aplican para toda la organización. Sin embargo, frecuentemente existen características que pueden requerir un énfasis adicional en el alineamiento entre negocios, roles y responsabilidades, políticas y procedimientos, competencias y técnicas. La siguiente lista describe algunas consideraciones relacionadas al ambiente de control de las TI:

- Es considerada muchas veces, erróneamente, como un área separada de negocio y, así, un ambiente de control separado.
- Es complejo, no sólo lo relacionado con sus componentes técnicos, sino también en la integración de estos componentes con el sistema global de control interno de la organización.
- TI puede presentar riesgos que requieren nuevas actividades de control, o mejoras en las actividades existentes, para obtener

éxito en la mitigación del riesgo.
» Requiere habilidades especializadas que pueden ser insuficientes.
» Puede exigir recursos de terceros, donde los procesos significativos o componentes de las TI son externalizados.
» Los controles propios de TI pueden no ser claros, principalmente para los controles de aplicaciones.

### 6.5.2 Evaluación del riesgo

Involucra la identificación y el análisis de riesgos relevantes para alcanzar los objetivos predeterminados, que constituyen la base para determinar las actividades de control. Es probable que los riesgos de control interno puedan ser más difundidos en la organización de las TI que en otras áreas de la organización. La evaluación de riesgos puede ocurrir para toda la entidad (global de la organización) o restringida a actividades específicas (para un determinado proceso o unidad de negocio).

En relación con la entidad, pueden ser esperadas:

- Una subcomisión de planeación de las TI de la organización y un comité de dirección Sarbanes-Oxley, con las siguientes responsabilidades:
- Supervisión del desarrollo del plan de control interno de la estrategia de las TI, su ejecución eficaz y la integración con el cumplimiento del plan global Sarbanes –Oxley;
- Gestión de evaluación de riesgos y de la gestión y operación de las TI, seguridad de datos, desarrollo y cambio de sistemas.

Restringido a actividades, pueden ser esperadas:

» Evaluaciones formales de riesgo en toda metodología de desarrollo de sistemas;
» Evaluación de riesgo embebido en la operación de infraestructura y procesos de cambio;
» Evaluación de riesgo embebido en el proceso de cambio de sistemas.

### 6.5.3 Control de actividades

Son las políticas, procedimientos y prácticas definidas para que los objetivos de negocio sean alcanzados y las estrategias de mitigación de riesgos sean realizadas. El control de actividades es desarrollado específicamente para cada objetivo de control para mitigar los riesgos identificados. Sin sistemas de información confiables y eficaces para controlar las actividades de las TI, las organizaciones públicas no serían capaces de generar informes financieros precisos. COSO reconoce estas relaciones e identifica dos grandes agrupaciones de información de actividades del sistema de control: controles generales y controles de aplicaciones.

» Controles generales son diseñados con el fin de que la información financiera generada a partir de sistemas de aplicación pueda ser confiable, incluyendo las siguientes tipos:

  - Datos de controles del centro de operación, como controles de configuración y programación de trabajo, acciones del operador, *backup* de datos y procedimientos de recuperación.
  - Controles de software del sistema y sobre la efectiva adquisición, implementación y mantenimiento de sistemas de software, gestión de base de datos, software de telecomunicaciones, de seguridad y utilitarios.

» Los controles de aplicativos son controles de desarrollo y mantenimiento de sistemas y aplicativos y de metodologías de desarrollo, incluyendo:

  - Controles de seguridad, controles de acceso que impidan la utilización inadecuada y no autorizada del sistema en todas las capas de las funcionalidades, operación de base de datos del sistema y de la propia aplicación.
  - Concepción e implementación del sistema, con descripción de las fases específicas, exigencias de documentación y gestión de cambios.

### 6.5.4 Información y comunicación

La información es necesaria en todos los niveles de una organización para ejecutar el negocio y alcanzar los objetivos de control de la entidad. Sin embargo, la identificación, la gestión y la comunicación de

información relevante representan un desafío creciente para el área de las TI. La determinación de la información necesaria para alcanzar los objetivos de control, y la comunicación de las mismas, en formato específico y dentro del plazo que permita que las personas realicen sus tareas, apoyan los otros cuatro componentes del cuadro de COSO.

Los procesos de las TI de la organización deben proveer la información financiera. Sin embargo, su alcance es generalmente mucho más amplio. El departamento de las TI también puede ayudar en la implementación de mecanismos para identificar y comunicar eventos significativos, como sistemas de correo electrónico o sistemas de apoyo a decisión. COSO también indica que la calidad de la información incluye la definición de los siguientes aspectos:

- ¿La información está correcta?
- ¿La información es oportuna, disponible cuando es necesaria y reportada en el periodo correcto de tiempo?
- ¿La información está actualizada?
- ¿La información es precisa, brindando datos correctos?
- ¿Las personas autorizadas tienen acceso a la información cuando es necesario?

Con relación a la entidad, pueden ser esperados:

- Desarrollo y comunicación de políticas corporativas;
- Desarrollo y comunicación de las exigencias de información, incluyendo plazos, informes mensual, trimestral y anual de gestión;
- Consolidación y comunicación de la información financiera.

Pueden ser esperadas las siguientes actividades:

- Desarrollo y comunicación del normas y procedimientos;
- Identificación y comunicación de información confiable para apoyar el alcance de los objetivos de negocio;
- Identificación y comunicación de violaciones de seguridad.

### 6.5.5 Monitoreo

El monitoreo, que abarcan la fiscalización del control interno de la administración por medio de procesos de evaluación, es cada vez más importante para las organizaciones. Existen dos tipos de actividades de monitoreo: acompañamiento continuo y evaluaciones separadas. Cada vez más el desempeño y la eficacia de las TI son constantemente controladas por medio de medidas de desempeño que indican si un control

subyacente está operando de forma eficaz. Considere los siguientes ejemplos:

» Monitoreo eficaz de seguridad en la configuración de una infraestructura de las TI reduce el riesgo de acceso no autorizado.
» Aumentar la seguridad puede reducir el riesgo de procesamiento de transacciones no autorizadas, que pueden generar informes imprecisos, si los aplicativos y componentes de infraestructura de las TI están comprometidos.

Con relación a las entidades, pueden ser esperados:

» Monitoreo continuo centralizado de operaciones de infraestructura de las TI;
» Monitoreo centralizado de seguridad;
» Auditoría interna de las TI: mientras la auditoría puede ocurrir en el nivel de actividad, la comunicación de los resultados de la auditoría ocurren en el nivel de la entidad.

Pueden ser esperadas las siguientes actividades:

» Identificación de problemas de gestión;
» Monitoreo de locales de operación de la infraestructura de las TI;
» Supervisión del local y del personal de las TI

La siguiente tabla representa el mapeo entre los procesos de las TI de CobiT 4.1 y COSO.

Tabla 77. Procesos de CobiT 4.1 y del COSO. H = alta, M = media, L = baja, X = asociación CobiT – COSO

| Procesos del CobiT | Importancia | COSO | | | | |
|---|---|---|---|---|---|---|
| | | Ambiente de control | Evaluación de riesgos | Control de actividades | Información y comunicación | Monitoreo |
| Planificar y Organizar, PO | | | | | | |
| PO1. Definir un plan estratégico de las TI | H | | X | | X | X |
| PO2. Definir la arquitectura de la información. | L | | | X | X | |

Continuación tabla 77. Procesos de CobiT 4.1 y del COSO. H = alta, M = media, L = baja, X = asociación CobiT – COSO

| Procesos del CobiT | COSO | | | | | |
|---|---|---|---|---|---|---|
| | Importancia | Ambiente de control | Evaluación de riesgos | Control de actividades | Información y comunicación | Monitoreo |
| PO3. Determinar las directrices de tecnología. | M | | X | X | X | |
| PO4. Definir los procesos, las organizaciones y las relaciones de las TI. | L | X | | | X | X |
| PO5. Gestionar la inversión de las TI. | M | | X | X | | |
| PO6. Comunicar metas y directrices gerenciales. | M | X | | | X | |
| PO7. Gestionar los recursos humanos de las TI. | L | X | | | X | |
| PO8. Gestionar la calidad. | M | X | X | X | | X |
| PO9. Evaluar y gestionar los riesgos de las TI. | H | | X | | | |
| PO10. Gestionar proyectos. | H | X | X | X | | X |
| Adquirir e Implementar | | | | | | |
| AI1. Identificar soluciones automatizadas. | M | | | X | | |
| AI2. Adquirir y mantener el software aplicativo. | M | | | X | | |
| AI3. Adquirir y mantener la infraestructura tecnológica. | L | | | X | | |
| AI4. Habilitar la operación y uso. | L | | | x | x | |
| AI5. Adquirir recursos de las TI | M | | | X | | |
| AI6. Gestionar cambios. | H | | X | X | | X |
| AI7. Instalar y homologar - soluciones y cambios. | M | | | X | X | X |
| Entregar y Soportar, DS | | | | | | |
| DS1. Definir y gestionar niveles de servicio. | M | X | | X | X | X |
| DS2. Gestionar servicios de terceros. | L | X | X | X | | X |
| DS3. Gestionar el desempeño y la capacidad. | L | | | X | | X |

Continuación tabla 77. Procesos de CobiT 4.1 y del COSO. H = alta, M = media, L = baja, X = asociación CobiT – COSO

| Procesos del CobiT | Importancia | COSO | | | | |
|---|---|---|---|---|---|---|
| | | Ambiente de control | Evaluación de riesgos | Control de actividades | Información y comunicación | Monitoreo |
| DS4. Asegurar la continuidad de los servicios. | M | X | | X | X | |
| DS5. Garantizar la seguridad de los sistemas. | H | | | X | X | X |
| DS6. Identificar y asignar costos | L | | | X | | |
| DS7. Sensibilizar y entrenar a los usuarios. | L | X | | | X | X |
| DS8. Gestionar el centro de servicios y los incidentes. | L | | | X | | |
| DS9. Gestionar la configuración. | M | | | X | | |
| DS10. Gestionar los problemas. | M | | | X | | |
| DS11. Gestionar los datos. | H | | | X | | |
| DS12. Gestionar el ambiente físico. | L | | | X | | |
| DS13. Gestionar las operaciones. | L | | | X | | |
| Monitorear y Evaluar. | | | | | | |
| ME1. Monitorear y evaluar el desempeño de las TI. | H | | | | X | X |
| ME2. Monitorear y evaluar los controles internos. | M | | | | | X |
| ME3. Asegurar la conformidad con requisitos externos. | H | | | X | X | X |
| ME4. Proveer el gobierno de las TI. | H | X | X | | X | X |

## Soluciones de gobierno de las TI de acuerdo con la legislación y normas de la administración pública colombiana

» Decreto 2145 del 4 de noviembre de 1999 por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y Territorial y se dictan otras disposiciones.

» Artículo 10. definición del Sistema Nacional de Control Interno. Es el conjunto de instancias de articulación y participación, competencias y sistemas de control interno, adoptados en ejercicio de la función administrativa por los organismos y entidades del Estado en todos sus órdenes, que de manera armónica, dinámica, efectiva, flexible y suficiente, fortalecen el cumplimiento cabal y oportuno de las funciones del Estado.

» Artículo 20. ámbito de aplicación. "Artículo modificado por el artículo 1 del Decreto 2539 de 2000. El nuevo texto es el siguiente:" El presente decreto se aplica a todos los organismos y entidades del Estado, en sus diferentes órdenes y niveles, así como a los particulares que administren recursos del Estado.

» Artículo 30. dirección y coordinación. De conformidad con el artículo 29 de la Ley 489 de 1998, el Sistema Nacional de Control Interno será dirigido por el Presidente de la República como máxima autoridad administrativa, apoyado y coordinado por el Consejo Asesor del Gobierno Nacional en materia de Control Interno de las entidades del orden nacional y territorial, el cual será presidido por el Director del Departamento Administrativo de la Función Pública.

» Artículo 21. Sistemas de información institucional. El Sistema Nacional de Control Interno como instancia de articulación, tendrá como base para su funcionamiento, entre otros, al Sistema Nacional de Evaluación de Resultados Sinergia, el Sistema Nacional de Contabilidad Pública, el Sistema de Desarrollo Administrativo y el Sistema General de Información Administrativa, los cuales deben fundamentarse en criterios de confiabilidad e integridad.

Decreto 3816 de 2003 del 31 de diciembre de 2003 por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública", la cual tendrá los siguientes objetivos:

1. Definir las estrategias y los programas para la producción de la información necesaria, para lograr una óptima generación de bienes y servicios públicos por parte del Estado. Lo anterior, sin perjuicio de la autonomía del DANE, en la producción de la información oficial básica.
2. Generar los escenarios adecuados que permitan a los ciudadanos tener acceso a la información necesaria para garantizar la transparencia de la administración pública y para que puedan ejercer un efectivo control social. Lo anterior, sin perjuicio de la

autonomía del DANE, en la producción de la información oficial básica.
3. Optimizar mediante el uso de medios tecnológicos, la calidad, la eficiencia y la agilidad en las relaciones de la administración pública con el ciudadano, con sus proveedores, y de las entidades de la administración pública entre sí.
4. Establecer mecanismos tendientes a eliminar la duplicidad de solicitud de información o la solicitud de información innecesaria a los ciudadanos.
5. Optimizar la inversión en tecnologías de información y de comunicaciones de la administración pública.
6. Facilitar el seguimiento y evaluación de la gestión pública, mediante la producción, el manejo y el intercambio de información y uso de tecnologías de información y comunicaciones de la administración pública.
7. Asegurar la coherencia, la coordinación y la ejecución de las políticas definidas para la estrategia de Gobierno en Línea a través del Programa Agenda de Conectividad.

Decreto 1599 del 20 de mayo del 2005 por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano MECI 1000:2005, el cual determina las generalidades y la estructura necesaria para establecer, documentar, implementar y mantener un Sistema de Control Interno en las entidades y agentes obligados conforme al artículo 5º de la Ley 87 de 1993. Las entidades obligadas a implementar el Sistema de Control Interno deberán adoptar el Modelo Estándar de Control Interno para el Estado Colombiano, teniendo como plazo máximo abril del 2008.

Decreto 1151 de 14 de abril de 2008 (Derogado por el art. 12, Decreto Nacional 2693 de 2012 )"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

Objetivo de la Estrategia de Gobierno en Línea. El objetivo es contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las organizaciones, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación.

Ley 1341 del 30 de julio de 2009 por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones, TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Artículo 1°. Objeto. La presente Ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

Decreto 2693 de 21 de diciembre de 2012, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Artículo 1°. Objeto. Definir los lineamientos, plazos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad.

Artículo 3°. Principios y fundamentos de la Estrategia de Gobierno en línea. La Estrategia de Gobierno en línea se desarrollará conforme a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998 y 3° de la Ley 1437 de 2011.

Así mismo, serán fundamentos de la estrategia los siguientes:

**Construcción colectiva:** La toma de decisiones y la implementación de soluciones específicas para problemas públicos, se lleva a cabo mediante el estímulo y aprovechamiento del interés y conocimiento de la sociedad, al igual que un esfuerzo conjunto dentro de las propias entidades públicas y sus servidores.

**Innovación:** El Estado desarrolla nuevas formas de usar las Tecnologías de la Información y las Comunicaciones para producir cambios que generen nuevo y mayor valor en la forma de operar, así como en la prestación de trámites y servicios.

**Neutralidad tecnológica:** El Estado garantiza la libre adopción de tecno-

logías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, emplear contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

**Confianza y seguridad:** El Estado garantiza la integridad, coherencia y confiabilidad en la información y los servicios que se realicen a través de medios electrónicos.

Artículo 4°. Líder de la Estrategia de Gobierno en línea. La Estrategia de Gobierno en línea será liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual orientará a las entidades a que se refiere el artículo 2° del presente decreto para su ejecución, en coordinación con el Departamento Administrativo de la Función Pública, el Departamento Nacional de Planeación y los demás organismos o entidades que tengan a su cargo la formulación de políticas públicas relacionadas con la Estrategia de Gobierno en línea.

Decreto 0032 DE 2013 Por el cual se crea la Comisión Nacional Digital y de Información Estatal.

Artículo 1°, Comisión Nacional Digital y de Información Estatal.

Créase una comisión intersectorial que se denominará "Comisión Nacional Digital y de Información Estatal", cuyo objeto será la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano, emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de tecnologías de la información y las comunicaciones, de conformidad con la definición que de éstas hace la Ley.

El Ministerio de Tecnología de la Información y Telecomunicaciones actualmente gestiona el proyecto denominado Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información del Estado Colombiano, que tiene como propósito fortalecer la infraestructura y los procesos de Tecnologías de Información de las entidades públicas, así como organizar orientar la manera de gestionar la Tecnología de Información en todos los sectores, con el propósito de ofrecer mejores servicios a las personas y a las instituciones, maximizar

los beneficios hacia el ciudadano y aumentar la eficiencia y transparencia de las entidades del Estado.

El Ministerio de Tecnología de la Información y Telecomunicaciones a través del Marco de referencia para la gestión de TI en el Estado colombiano ha venido desarrollando los lineamientos para que las entidades puedan realizar las adquisiciones de recursos de TI a través de mecanismos colectivos entre los que se destacan los acuerdos marco de precios y adquisiciones en modalidad de servicio y/o por demanda.

## Lo aprendido

- Cómo utilizar la norma ISO/IEC 38500 para dirigir la implementación del gobierno de las TI.
- Cómo utilizar COSO en conjunto con CobiT 4.1 para evaluar los controles internos.
- Las principales iniciativas contenidas en el modelo Val IT para gestionar las inversiones de las TI.
- Las normas, reglamentos y documentos de la República de Colombia.

Capítulo

07

# Fundamentos de CobiT 5.0

**Objetivos**

Profundizar en el marco de CobiT como estructura fundamental, reconocida hoy por hoy, para gobierno y gestión de las TI. Analizar los componentes del marco de trabajo de CobiT y su adaptación a una organización

**Conceptos**

Gobierno y gestión de las TI; dominios y procesos de CobiT 5.0.

# Introducción

El área de las TI dentro de las organizaciones viene asumiendo un rol cada vez más importante y es por ello que debe estar preparada para asumir este reto que le significa estar más cerca de las decisiones de negocio, aportando con la innovación tecnológica y su aplicación al negocio, lo que puede marcar la diferencia en la ventaja competitiva que busca la organización para sobrevivir o para sobresalir.

En ese orden de ideas se hace necesario que el área de las TI cuente con la estructura adecuada para la toma de decisiones y para el accionar de los procesos tanto de gobierno como de gestión de las tecnologías de información y las comunicaciones.

ISACA ha desarrollado la quinta edición de CobiT atendiendo esa necesidad del área de las TI de contar con un marco de referencia que le permita gobernar y gestionar la Tecnología de la Información y las Comunicaciones, TIC, como una evolución que incorpora alrededor de CobiT 4.1 procesos de Val IT y de RISK IT.

La información que se presenta en este capítulo está basada en varios documentos generados por ISACA (antiguamente esta sigla significaba *Information Systems Auditing and Control Association* y desde hace cierto tiempo hacia acá se usa el acrónimo para reflejar el amplio rango de profesionales de las TI a quienes sirve esta asociación).

En la Figura 19 puede apreciarse cómo ha venido evolucionando el marco de referencia de ISACA denominado CobiT. Allí se ve cómo en un comienzo el marco estaba orientado hacia la auditoría de sistemas de información (CobiT 1) y hacia el control (CobiT 2) en consonancia con el significado original de ISACA (*Information Systems Auditing and Control Association*).


**Figura 19.** Evolución de CobiT

Fuente: tomado y adaptado del sitio de ISACA (www.isaca.org) - CobiT 5 *Introduction*

En la versión de CobiT 3 del año 2000 ya se empezó a contextualizar en el ambiente de gestión de las TI y entre los años 2005 y 2007 ISACA publicó tanto las versiones 4 y 4.1 de CobiT como los productos VAL IT para gestión de las inversiones de las TI como RISK IT para gestión de los riesgos de las TI.

CobiT 5, lanzado en abril del 2012, integra los principales marcos y guías de ISACA, con un enfoque principal en CobiT 4.1, Val IT 2.0 y RISK IT 2.0, pero considerando también el Modelo de Negocio para la Seguridad de la Información, BMIS, el Marco de Aseguramiento de las TI, ITAF, la publicación titulada *Board Briefing on IT Governance* y el documento *Taking Governance Forward* , TGF, de modo que cubra la actividad de la organización por completo y proporcione una base para integrar otros marcos, normas y prácticas como un referente único.

CobiT 5 es el único marco de negocio para el gobierno y la gestión de las TI de la organización. CobiT 5 ayuda a maximizar el valor de la información mediante la incorporación de las últimas ideas en la gobernanza empresarial y técnicas de gestión, y proporciona principios globalmente aceptados, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza en las tareas de Tecnologías de la Información.

CobiT 5 provee de un marco de trabajo integral que ayuda a las organizaciones a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las organizaciones a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

CobiT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la organización, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de las TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. CobiT 5 es genérico y útil para organizaciones de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

## 7.1 La familia de productos de CobiT 5

La familia de productos de CobiT 5 incluye los siguientes productos, tal como puede verse en la Figura 20:

- CobiT 5 (el marco de trabajo)
- Guías de facilitadores de CobiT 5, en las que se discuten en detalle los facilitadores para el gobierno y gestión, estas incluyen:
  - CobiT 5: Información catalizadora
  - Información posibilitadora (en desarrollo)
  - Otras guías de facilitadores (visitar www.isaca.org/cobit)

- Guías profesionales de CobiT 5, incluyendo:
  - Implementación de CobiT 5
  - CobiT 5 para seguridad de la información (en desarrollo)
  - CobiT 5 para aseguramiento (en desarrollo)
  - CobiT 5 para riesgos (en desarrollo)
  - Otras guías profesionales (visitar www.isaca.org/cobit)

- Un entorno colaborativo *online*, que estará disponible para dar soporte al uso de CobiT 5

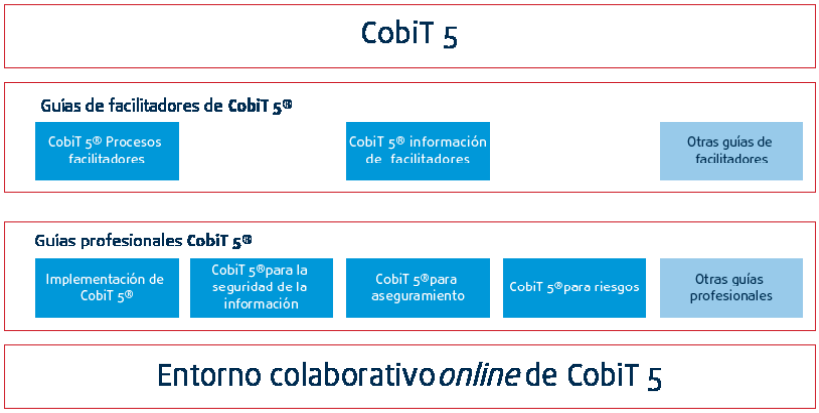



**Figura 20.** Familia de productos de CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish* (figura 1 página 11)

## 7.2 Los cinco principios de CobiT 5

CobiT 5 provee de un marco de trabajo integral que ayuda a las organizaciones a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las organizaciones a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

CobiT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la organización, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de las TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. CobiT 5 es genérico y útil para organizaciones de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. CobiT 5 se basa en cinco principios claves (mostrados en la Figura 21) para el gobierno y la gestión de las TI empresariales:

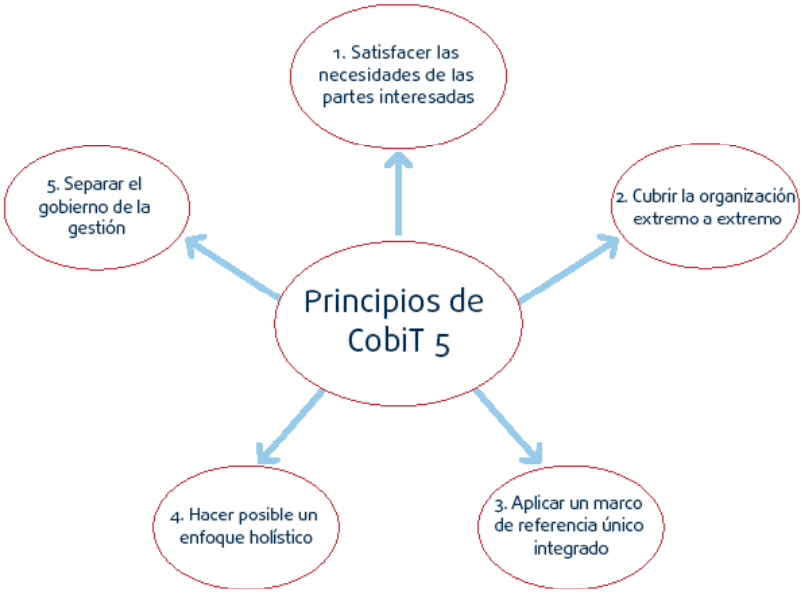



**Figura 21.**
Principios de CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish* (figura 2 página 13)

### Principio 1. Satisfacer las necesidades de las partes interesadas

Las organizaciones existen para crear valor para sus partes interesadas, manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. CobiT 5 provee todos los procesos necesarios y otros facilitadores para permitir la creación de valor del negocio mediante el uso de las TI. Dado que toda organización tiene objetivos diferentes, una organización puede personalizar CobiT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con las TI y mapeándolas con procesos y prácticas específicos.

### Principio 2: Cubrir la organización extremo a extremo

CobiT 5 integra el gobierno y la gestión de las TI en el gobierno corporativo:

» Cubre todas las funciones y procesos dentro de la organización; CobiT 5 no se enfoca sólo en la "función de las TI", sino que trata

la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la organización.
» Considera que los facilitadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la organización y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la organización y TI relacionadas.

### Principio 3: Aplicar un marco de referencia único e integrado

Hay muchos estándares y buenas prácticas relativos a las TI, ofreciendo cada uno ayuda para un subgrupo de actividades de las TI. CobiT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la organización.

### Principio 4: Hacer posible un enfoque holístico

Un gobierno y gestión de las TI de la organización efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. CobiT 5 define un conjunto de facilitadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la organización. Los facilitadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la organización. El marco de trabajo CobiT 5 define siete categorías de facilitadores:

» Principios, políticas y marcos de trabajo
» Procesos
» Estructuras organizativas
» Cultura, ética y comportamiento
» Información
» Servicios, infraestructuras y aplicaciones
» Personas, habilidades y competencias

### Principio 5: Separar el gobierno de la gestión

El marco de trabajo CobiT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de CobiT 5 en esta distinción clave entre gobierno y gestión es:

**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 muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

**Gestión**
La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En muchas organizaciones, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo, CEO.

Juntos, estos cinco principios habilitan a la organización a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

## Ejercicio de refuerzo - principios de CobiT 5

¿Cuáles son los principios de CobiT 5?

## 7.3 Principio 1: satisfacer las necesidades de las partes interesadas

Las organizaciones existen para crear valor para sus accionistas. En consecuencia, cualquier organización, comercial o no, tendrá la creación de valor como un objetivo de gobierno. Creación de valor significa conseguir beneficios a un costo óptimo de los recursos mientras se optimiza el riesgo. (Ver Figura 22 .) Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las organizaciones comerciales o de servicio público para entidades gubernamentales.

Las organizaciones tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes y a veces contradictorias para cada uno de ellos. Las actividades de gobierno se refieren a negociar y decidir entre los diferentes intereses en el valor de las partes interesadas. En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deben hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren?

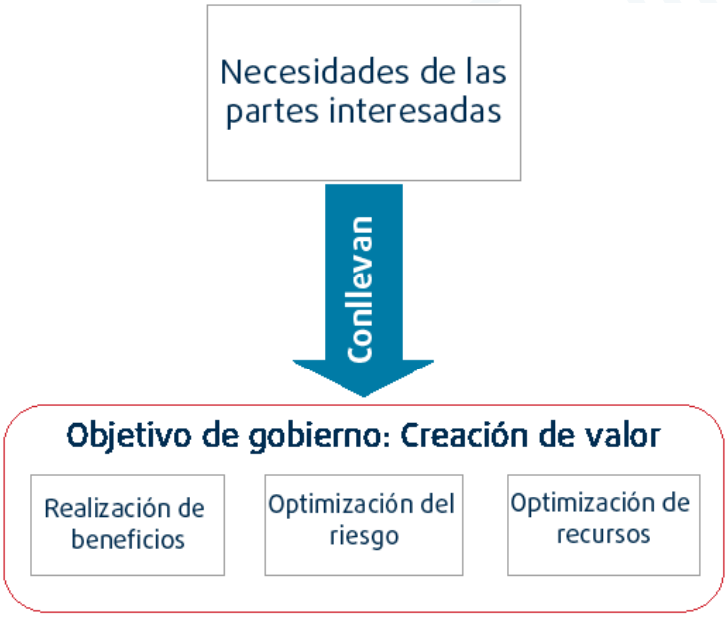



**Figura 22.** Necesidades de las partes interesadas según CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish* (figura 3 página 17)

### 7.3.1 Cascada de metas de CobiT 5

Cada organización opera en un contexto diferente; este contexto está determinado por factores externos (el mercado, la industria, geopolítica, etc.) y factores internos (la cultura, organización, umbral de riesgo, etc.) y requiere un sistema de gobierno y gestión personalizado.

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de CobiT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la organización en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la organización y las soluciones y servicios de TI. La cascada de metas de CobiT 5 se muestra en la Figura 23.

**Paso 1. Los motivos de las partes interesadas influyen en las necesidades de las partes interesadas.**

Las necesidades de las partes interesadas están influenciadas por diferentes motivos, por ejemplo, cambios de estrategia, un negocio y entorno regulatorio cambiantes y las nuevas tecnologías.

**Paso 2. Las necesidades de las partes interesadas desencadenan metas empresariales.**

Las necesidades de las partes interesadas pueden estar relacionadas con un conjunto de metas empresariales genéricas.

Estas metas corporativas han sido desarrolladas utilizando las dimensiones del Cuadro de Mando Integral, CMI, (en inglés: Balanced Scorecard, BSC, creado por Robert Kaplan y David P. Norton y publicado en; T*he Balanced Scorecard: Translating Strategy Into Action, Harvard University Press*, EE.UU., 1996) y representan una lista de objetivos comúnmente usados que una organización puede definir por sí misma. Aunque esta lista no es exhaustiva, la mayoría de metas corporativas específicas de la organización pueden relacionarse fácilmente con uno o más de los objetivos genéricos de la organización.

CobiT 5 define 17 objetivos genéricos, como se muestra en la Tabla 78 que incluye la siguiente información:

- La dimensión del BSC en la que encaja la meta corporativa
- Las metas corporativas
- La relación con los tres objetivos principales de gobierno: realización de beneficios, optimización de riesgos y optimización de recursos ('P' indica una relación primaria y 'S' una relación secundaria, es decir una relación menos fuerte).

### Paso 3. Cascada de metas de la organización a metas relacionadas con las TI

El logro de metas empresariales requiere un número de resultados relacionados con las TI2, que esté representado por las metas relacionadas con las TI. Se entiende como relacionados con las TI a la información, tecnologías y l metas relacionadas con las TI, que se estructuran en dimensiones del CMI. CobiT 5 define 17 metas relacionadas con las TI.

### Paso 4. Cascada de metas relacionadas con las TI hacia metas catalizadoras

Alcanzar metas relacionadas con las TI requiere la aplicación satisfactoria y el uso de varios facilitadores. El concepto de facilitador se explica detalladamente en el capítulo 5 del libro de ISACA CobiT 5. Los facilitadores incluyen procesos, estructuras organizativas e información, y para cada catalizador puede definirse un conjunto de metas relevantes en apoyo de las metas relacionadas con las TI.

## Ejercicio de refuerzo - cascada de metas de CobiT 5

¿Revise dentro de su organización la planeación estratégica de las TI y determine si sigue el flujo de la cascada de metas de CobiT 5?


**Figura 23.**
La cascada de metas de CobiT 5

Fuente: tomado de Cobit5 *framework Spanish* (figura 4 página 18)

Tabla 78. Metas Corporativas de CobiT 5

| Dimensión del BSC | Meta corporativa | Relación con los objetivos de gobierno | | |
|---|---|---|---|---|
| | | Realización de Beneficios | Optimización de Riesgos | Optimización de Recursos |
| Financiera | 1. Valor de las inversiones de negocio para las partes interesadas | P | | S |
| | 2. Portafolio de productos y servicios competitivos | P | P | S |
| | 3. Riesgos de negocio gestionados (salvaguarda de activos) | | P | S |
| | 4. Cumplimiento de leyes y regulaciones externas | | P | |
| | 5. Transparencia financiera | P | S | S |
| Cliente | 6. Cultura de servicio orientada al cliente | P | | S |
| | 7. Continuidad y disponibilidad del servicio de negocio | | P | |
| | 8. Respuestas ágiles a un entorno de negocio cambiante | P | | S |
| | 9. Toma estratégica de decisiones basada en información | P | P | P |
| | 10. Optimización de costos de entrega del servicio | P | | P |
| Interna | 11. Optimización de la funcionalidad de los procesos de negocio | P | | P |
| | 12. Optimización de los costos de los procesos de negocio | P | | P |
| | 13. Programas gestionados de cambio en el negocio | P | P | S |
| | 14. Productividad operacional y de los empleados | P | | P |
| | 15. Cumplimiento con las políticas internas | | P | |
| Aprendizaje y Crecimiento | 16. Personas preparadas y motivadas | S | P | P |
| | 17. Cultura de innovación de producto y negocio | P | | |

Fuente: tomado de CobiT 5 *framework Spanish* (figura 5 página 19)

Tabla 79. Metas relacionadas con las TI

| Dimensión del BSC TI | Metas relacionadas con TI | |
|---|---|---|
| Financiera | 01 | Alineamiento de TI y estrategia de negocio |
| | 02 | Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas |
| | 03 | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI |
| | 04 | Riesgos de negocio gestionados relacionados con TI |
| | 05 | Realización de beneficios del portafolio de inversiones y servicios relacionados con TI |
| | 06 | Transparencia de los costos, beneficios y riesgos de TI |
| Cliente | 07 | Entrega de servicios de TI de acuerdo con los requisitos del negocio |
| | 08 | Uso adecuado de aplicaciones, información y soluciones tecnológicas |
| Interna | 09 | Agilidad de TI |
| | 10 | Seguridad de la información, infraestructura de procesamiento y aplicaciones |
| | 11 | Optimización de activos, recursos y capacidades de TI |
| | 12 | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio |
| | 13 | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. |
| | 14 | Disponibilidad de información útil y fiable para la toma de decisiones |
| | 15 | Cumplimiento de las políticas internas por parte de TI |
| Aprendizaje y Crecimiento | 16 | Personal del negocio y de TI competente y motivado |
| | 17 | Conocimiento, experiencia e iniciativas para la innovación de negocio |

Fuente: tomado de CobiT 5 *framework Spanish* (figura 6 página 19)

### 7.3.2 Beneficios de la cascada de metas de CobiT 5

La cascada de metas es importante porque permite la definición de prioridades de implementación, mejora y aseguramiento del gobierno de las TI de la organización, que se basa en metas corporativas (estratégicas) de la organización y el riesgo relacionado. En la práctica, la cascada de metas:

- Define objetivos y metas relevantes y tangibles a varios niveles de responsabilidad
- Filtra la base de conocimiento de CobiT 5, sobre la base de las metas corporativas, para extraer las guías relevantes a incluir en proyectos específicos de implementación, mejora o aseguramiento.
- Identifica claramente y comunica cómo (algunas veces de forma muy operativa) los facilitadores son importantes para alcanzar metas de la organización.

## 7.4 Principio 2: cubrir la organización extremo a extremo

CobiT 5 contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo a extremo y para toda la organización, tal como puede verse en la Figura 24. Esto significa que CobiT 5:

- Integra el gobierno de la organización de TI en el gobierno corporativo. Es decir, el sistema de gobierno para la organización TI propuesto por CobiT 5 se integra sin problemas en cualquier sistema de gobierno. CobiT 5 se alinea con las últimas visiones sobre gobierno.
- Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada.

Dado este alcance corporativo amplio, CobiT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

CobiT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la organización TI (ver el principio 4), basada en varios facilitadores. Los facilitadores son para toda la organización y extremo-a-extremo, es decir, incluyendo todo y a todos, internos y externos, que

sean relevantes para el gobierno y la gestión de la información de la organización y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

La información es una de las categorías de facilitadores de CobiT. El modelo mediante el que CobiT 5 define los facilitadores 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.

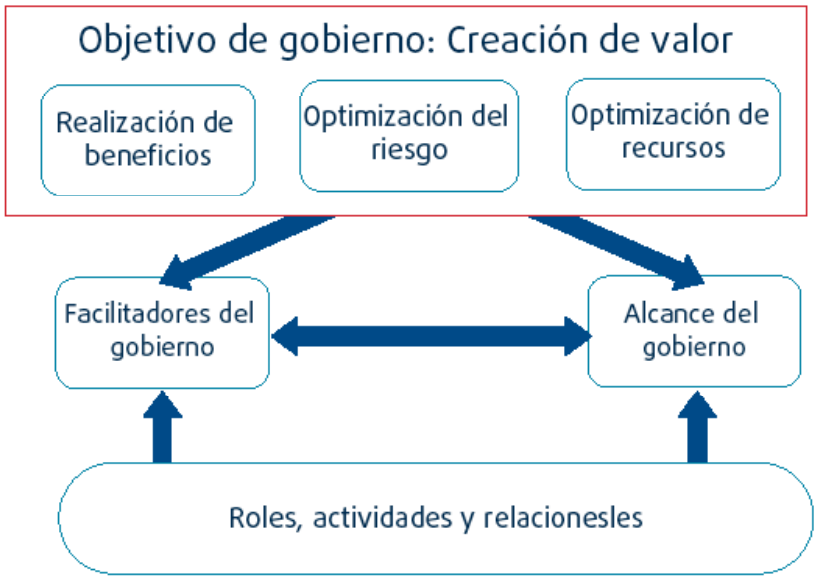



**Figura 24.** El gobierno y la gestión de las TI en CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish* (figura 8 página 23)

### 7.4.1 Facilitadores de gobierno

Los facilitadores 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. Los facilitadores también incluyen los recursos corporativos, por ejemplo, capacidades de servicios (infraestructura TI, aplicaciones, etc.), personas e información.

Una falta de recursos o facilitadores puede afectar a la capacidad de la organización de crear valor.

### Alcance de gobierno

El gobierno puede ser aplicado a toda la organización, a una entidad, a un activo tangible o intangible, etc. Es decir, es posible definir diferentes vistas de la organización a la que se aplica el gobierno, y es esencial definir bien este alcance del sistema de gobierno. El alcance de CobiT 5 es la organización, pero en esencia, CobiT 5 puede tratar con cualquiera de las diferentes vistas.

### Roles, actividades y relaciones

Un último elemento son los roles, actividades y relaciones de gobierno. Definen quién está involucrado en el gobierno, cómo se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno. En CobiT 5, se hace una clara diferenciación entre las actividades de gobierno y de gestión en los dominios de gobierno y gestión, así como en la interconexión entre ellos y los actores implicados. La Figura 25 detalla la parte inferior de la Figura 24, enumerando las interacciones entre los diferentes roles.

**Figura 25.** Interacciones entre roles a través de las actividades en CobiT 5


Fuente: tomado de Cobit5 *framework Spanish* (figura 9 página 24)

## 7.5 Principio 3: aplicar un marco de referencia único integrado

CobiT 5 es un marco de referencia único e integrado porque:

- Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la organización usar CobiT 5 como el marco integrador general de gestión y gobierno.
- Es completo en cuanto a la cobertura de la organización, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general úni-

co sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico.

» Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.

» Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como CobiT, Val IT, RISK IT, BMIS, la publicación Información sobre gobierno de las TI para la Dirección (*Board Briefing on IT Governance*) e ITAF para proporcionar guía y asistencia a las organizaciones. CobiT 5 integra todo este conocimiento. Véase la Figura 26 en la cual se muestra todo el compendio de publicaciones de ISACA y su armonización para lograr un marco de referencia único integrado.

## Ejercicio de refuerzo - CobiT 5 como marco de referencia único integrado

» ¿Conoce alguna organización en la cual se aplique CobiT y algún otro marco de referencia para gobierno o gestión de las TI?

» Explique brevemente su aplicación.

» Si no conoce organización alguna que lo aplique, investigue en organizaciones especialmente de gran tamaño y que sean de avanzada y verifique la aplicación de marcos de referencia para gobierno o gestión de las TI.

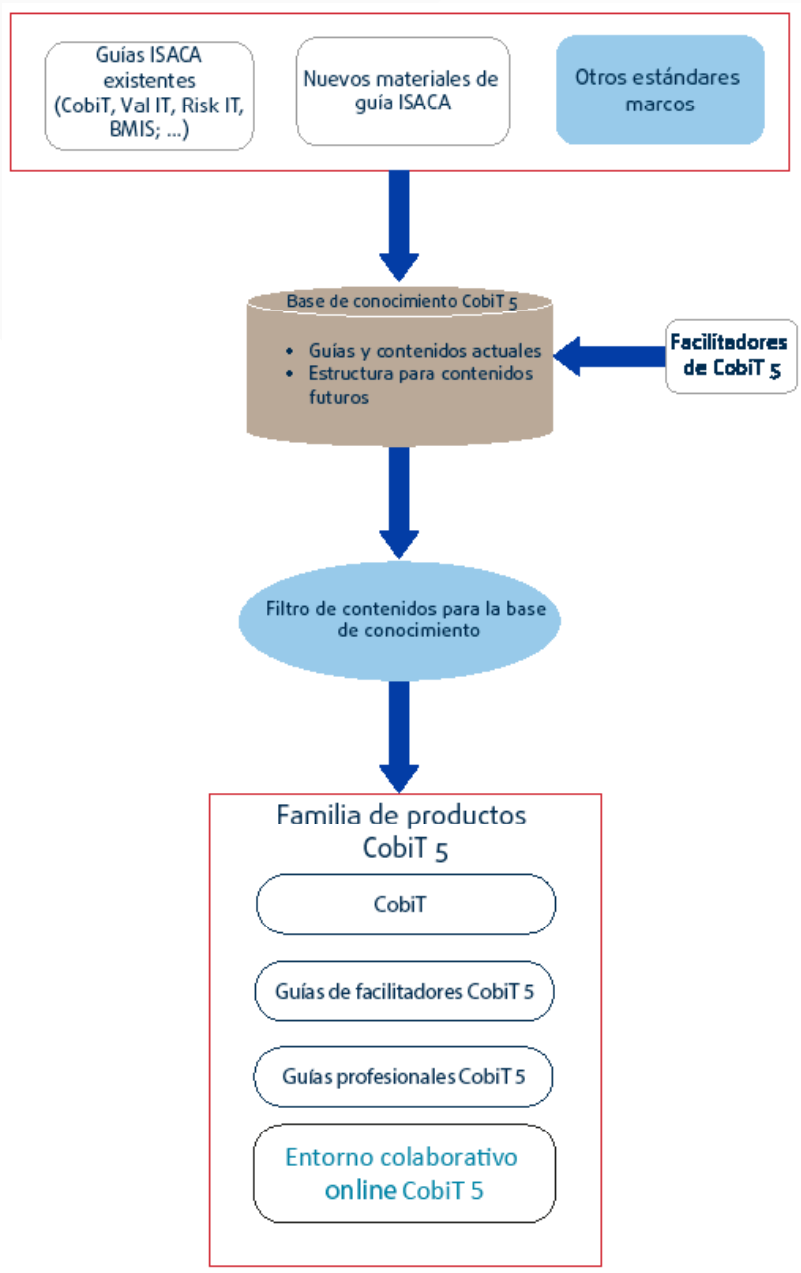



**Figura 26.** CobiT 5 marco de referencia único integrado

Fuente: tomado de Cobit5 *framework Spanish* (figura 10 página 25)

## 7.6 Principio 4: hacer posible un enfoque holístico

### 7.6.1 Facilitadores CobiT 5

Los facilitadores son factores que, individual y colectivamente, influyen sobre si algo funcionará, en este caso, el gobierno y la gestión de la organización TI. Los facilitadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes facilitadores deberían conseguir.

El marco de referencia CobiT 5 describe siete categorías de facilitadores (Figura 27):

- Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los 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.
- Las estructuras organizativas son las entidades de toma de decisiones clave en una organización.
- La cultura, ética y comportamiento de los individuos y de la organización son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La información impregna toda la organización e incluye toda la información producida y utilizada por la organización. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la organización en sí misma.
- Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la organización, servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

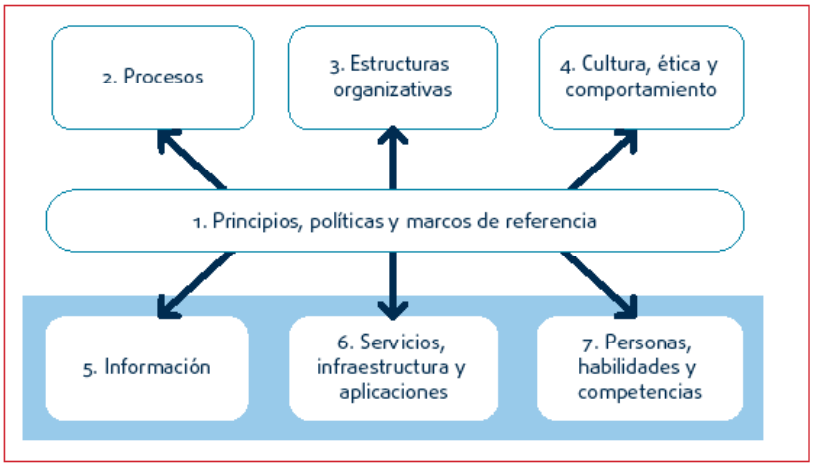



**Figura 27.** Las 7 categorías de facilitadores empresariales de CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish* (figura 12 página 27)

Algunos de los facilitadores definidos previamente son también recursos corporativos que también necesitan ser gestionados y gobernados. Esto aplica a:

- La información, que necesita ser gestionada como un recurso. Alguna información, tal como informes de gestión y de inteligencia de negocio son importantes facilitadores para el gobierno y la gestión de la organización.
- Servicios, infraestructura y aplicaciones.
- Personas, habilidades y competencias.

### 7.6.2 Gobierno y gestión sistémicos mediante facilitadores interconectados

La Figura 27 también transmite la mentalidad que debería ser adoptada para el gobierno corporativo, incluyendo el gobierno de las TI, que es alcanzar las principales metas corporativas. Cualquier organización debe siempre considerar un conjunto interconectado de facilitadores. Es decir, cada facilitador:

- Necesita del resultado de otros facilitadores para ser completamente efectivo, por ejemplo, los procesos necesitan información, las estructuras organizativas necesitan habilidades y comportamiento.

» Proporciona una salida para beneficio de otros facilitadores, por ejemplo, los procesos proporcionan información, habilidades y el comportamiento hace los procesos eficientes.

Por tanto, cuando se trata con el gobierno y la gestión de la organización TI, se pueden tomar buenas decisiones solo cuando se toma en consideración esta naturaleza sistémica del gobierno y de la gestión. Esto significa que para tratar con cualquier necesidad de un grupo de interés, todos los facilitadores interrelacionados tienen que ser analizados para saber si son relevantes y contemplados, si fuera necesario.

### Ejercicio de refuerzo - los facilitadores empresariales de CobiT 5

¿Cuáles son las categorías de facilitadores empresariales de CobiT 5?

## 7.7 Principio 5: separar el gobierno de la gestión

### Gobierno y gestión

El marco de CobiT 5 realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos.

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

#### 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 organizaciones, el gobierno es responsabilidad del consejo de administración bajo la dirección de su presidente.

## Gestión

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En la mayoría de las organizaciones, la gestión es responsabilidad de la dirección ejecutiva bajo la dirección del CEO.

## Interacciones entre gobierno y gestión

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 facilitadores, se muestran a alto nivel en la Tabla 80

Tabla 80. Interacciones gobierno y gestión en CobiT 5

| Catalizador | Interacción gobierno-gestión |
|---|---|
| Procesos | En el modelo ilustrativo de procesos de CobiT 5 (CobiT 5: procesos facilitadores), 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 organización. |
| 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 organización, 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. |

Continuación tabla 80. Interacciones gobierno y gestión en CobiT 5

| Catalizador | Interacción gobierno-gestión |
|---|---|
| Principios, políticas y marcos | Los principios, políticas y marcos son los vehículos mediante los cuales las decisiones de gobierno son sancionadas en la organización, 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 facilitador 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. |

Fuente: tomado de CobiT 5 *framework Spanish* (figura 14 página 31)

## 7.8 Modelo de referencia de procesos de CobiT 5

CobiT 5 no es una fórmula como tal pero sí defiende que las organizaciones implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas, tal y como se muestra en la Figura 28

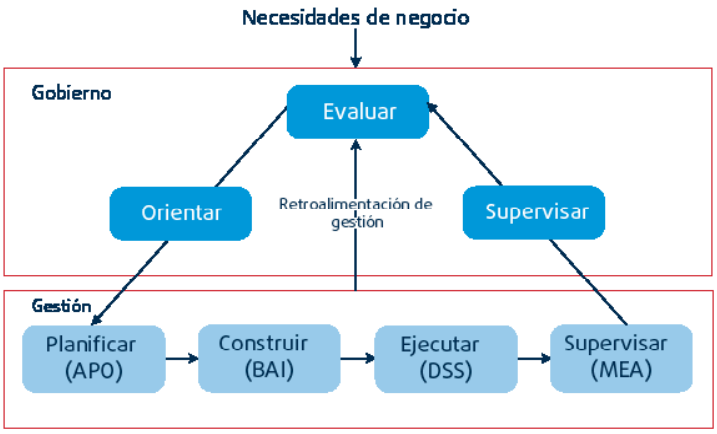



**Figura 28.** Áreas claves de gobierno y gestión en CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish* (figura 15 página 32)

Una organización puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Organizaciones más pequeñas pueden tener pocos procesos; organizaciones 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 organización relacionados con las actividades de las TI, proporciona un modelo de referencia común entendible para las operaciones de las TI y los responsables de negocio. El modelo de procesos propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada organización 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 organización involucradas en las actividades de las 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 las TI, proporcionar garantía de las TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de CobiT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- **Gobierno:** contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).
- **Gestión:** contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (*Plan, Build, Run and Monitor,* PBRM), y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de CobiT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:
  - Alinear, Planificar y Organizar (*Align, Plan and Organise*, APO)
  - Construir, Adquirir e Implementar (*Build, Acquire and Implement*, BAI)
  - Entregar, dar Servicio y Soporte (*Deliver, Service and Support,* DSS)
  - Monitorear, Evaluar y Valorar (*Monitor, Evaluate and Assess,* MEA)

## Ejercicio de refuerzo - El modelo de procesos de CobiT 5

¿Cuáles son los dominios de procesos de CobiT 5?

## 7.9 El modelo de capacidad de los procesos de CobiT 5

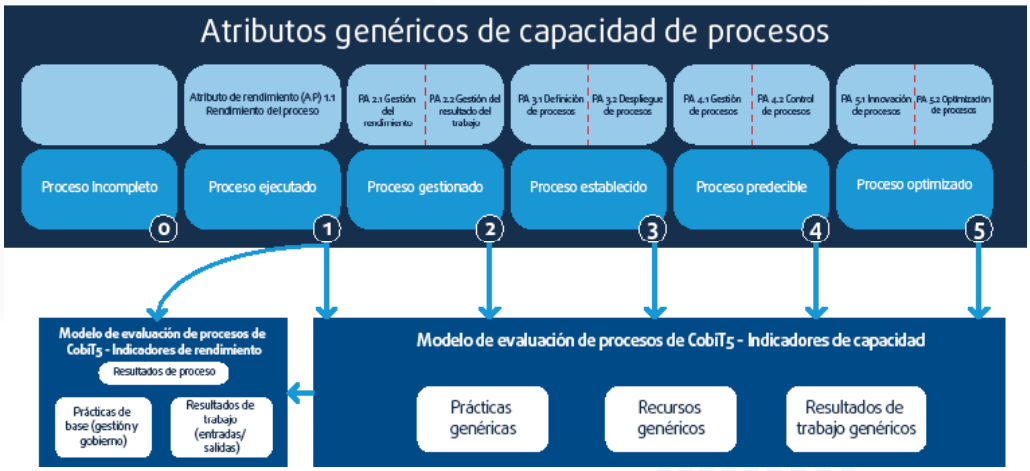
Los usuarios de CobiT 4.1, RISK IT y Val IT están familiarizados con los modelos de madurez de procesos incluidos en esos marcos. Estos modelos se utilizan para medir la madurez actual o en el estado en que se encuentran ('*as-is*') los procesos relacionados con las TI de una organización, para definir un estado de madurez requerido ('*to-be*'), y para determinar la brecha entre ellos y la forma de mejorar el proceso para alcanzar el nivel de madurez deseado.

El conjunto de productos de CobiT 5 incluye un modelo de capacidad de procesos, basado en la norma internacionalmente reconocida ISO/IEC 15504 de Ingeniería de Software -Evaluación de Procesos. Este modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, es decir, que proporcionará un medio para medir el desempeño de cualquiera de los procesos de gobierno (basado en EDM) o de gestión (basado en PBRM), y permitirá identificar áreas de mejora.

Sin embargo, el nuevo modelo es diferente del modelo de madurez de CobiT 4.1 en su diseño y uso.

Los detalles del enfoque de evaluación de la capacidad basada en CobiT 5 están incluidos en la publicación de ISACA (*CobiT® Process Assessment Model, PAM: Using CobiT® 4.1*)

El enfoque de CobiT 5 de capacidad de los procesos se puede ver en la siguiente figura.




Fuente: tomado de CobiT 5 *framework Spanish* (figura 19 página 42)

**Figura 29.** Resumen del modelo capacidad de procesos de CobiT 5

Existen seis niveles de capacidad que se pueden alcanzar por un proceso, incluida la designación de "proceso incompleto", si las prácticas definidas en el proceso no alcanzan la finalidad prevista:

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

## 7.10 Resumen de los cambios entre CobiT ® 4.1 y CobiT® 5

Tabla 81. Diferencias entre CobiT ® 4.1 y CobiT ® 5

| CobiT ® 4.1 | CobiT ® 5 |
|---|---|
| Tiene cuatro dominios:<br>1. Planear y Organizar, PO,<br>2. Adquirir e Implementar, AI,<br>3. Entregar y Dar Soporte, DS<br>4. Monitorear y Evaluar, ME | Tiene cinco dominios: el primero de ellos dedicado al gobierno de las TI y los cuatro restantes a la gestión de las TI:<br>1. Evaluar, Orientar y Supervisar, EDM,<br>2. Alinear, Planear y Organizar, APO,<br>3. Construir, Adquirir e Implementar, BAI,<br>4. Entregar, Dar Soporte y Dar Servicio, DSS y<br>5. Monitorear, Evaluar y Valorar, MEA. |
| Los procesos de CobiT ® 4.1 que se combinan en CobiT ® 5<br>» DS7 (Educar y Entrenar a los usuarios) se fusionó con PO7(Administrar Recursos Humanos de las TI) y se convirtió en APO-07 Gestionar los Recursos Humanos<br>» PO6 (Comunicar las Aspiraciones y la Dirección de la Gerencia) se fusionó con PO1 (Definir el Plan Estratégico de las TI) y se convirtió en APO-02 Gestionar la Estrategia.<br>» PO2 (Definir la Arquitectura de la Información) se fusionó con PO3 (Determinar la Dirección Tecnológica) y se convirtió en APO-03 Gestionar la Arquitectura Empresarial.<br>» AI2 (Adquirir y Mantener el Software Aplicativo) se fusiona con AI3 (Adquirir y Mantener la Infraestructura Tecnológica) y se convirtió en BAI-03 Gestionar la Identificación y Construcción de Soluciones.<br>» DS12 (Administrar el ambiente físico) se fusiona con DS5 (Garantizar la Seguridad de los sistemas) y se convirtió en DSS-05 Gestionar los Servicios de Seguridad. | |
| Los procesos de CobiT ® 4.1 que son reasignados en CobiT ® 5<br>» ME4 (proporcionar gobierno de las TI) a EDM1 , 2, 3 , 4, 5 ( procesos de gobierno de las TI Empresarial). | |
| Los procesos de CobiT ® 4.1 que están reubicados en CobiT ® 5<br>» PO1(definir el plan estratégico de las TI) a APO-02 (gestionar la estrategia)<br>» PO4 (definir procesos, organización y relaciones de las TI a APO-01 (gestionar el marco de gestión de las TI) | |
| | Procesos nuevos de CobiT ® 5<br>» EDM1 Establecer y mantener el Marco de gobierno<br>» APO-01 Gestionar el marco de gestión de las TI<br>» APO-04 Gestionar la innovación (en parte PO3 )<br>» APO-08 Gestionar las relaciones<br>» BAI-08 Gestionar el Conocimiento<br>» DSS2 Gestionar los activos (en parte DS9 )<br>» DSS6 Gestionar los controles de los procesos de negocio |

## 7.11 Procesos en CobiT 5

En CobiT 5 existen 37 procesos de los cuales cinco corresponden al gobierno de las TI y los otros 32 corresponden a la gestión de las TI, como se indica en la siguiente figura

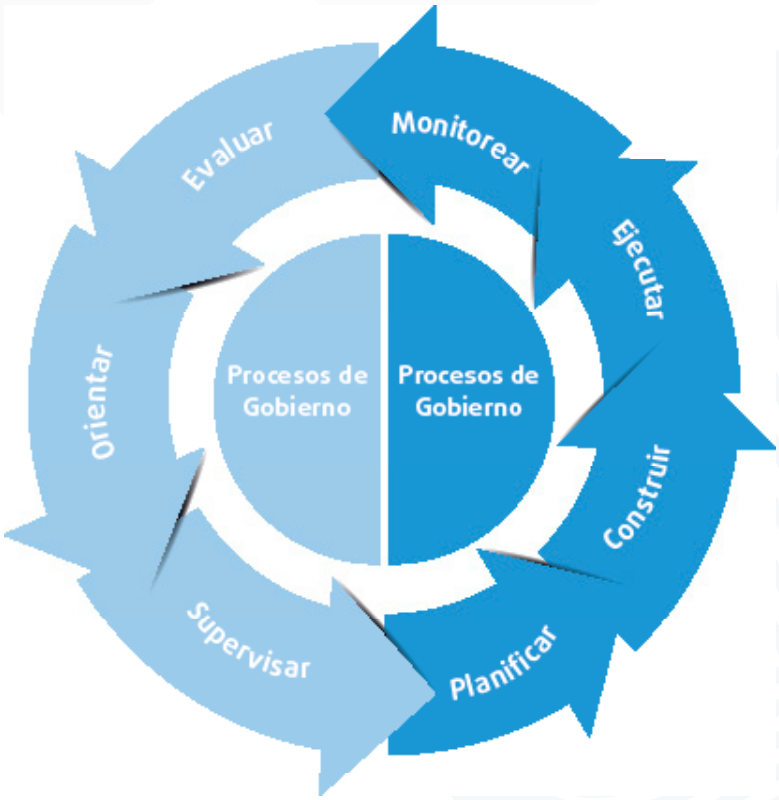



**Figura 30.** Procesos en CobiT 5

Fuente: tomado de CobiT 5 *framework Spanish*

## Procesos de gobierno de las TI

### 7.11.1 Dominio: Evaluar, Orientar y Supervisar, EDM:

Este dominio en particular hace referencia a los procesos de las TI que deben ser responsabilidad de la capa de gobierno de las TI.

Hay cinco procesos en este dominio, a saber:

- EDM01. Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
- EDM02. Asegurar la entrega de beneficios.
- EDM03. Asegurar la optimización del riesgo.
- EDM04. Asegurar la optimización de recursos.
- EDM05. Asegurar la transparencia hacia las partes interesadas.

### Proceso EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

Analiza y articula los requerimientos para el gobierno de las TI de la organización y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la organización.

Su propósito es facilitar un enfoque consistente, integrado y alineado con el alcance del gobierno de la organización. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la organización, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del consejo de administración.

Tabla 82. Prácticas del proceso EDM01

| Prácticas proceso EDM01 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM01.01: Evaluar el sistema de gobierno | Identificar y comprometerse continuamente con las partes interesadas de la organización, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de las TI de la organización | a. Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno.<br>b. Determinar la relevancia de las TI y su papel con respecto al negocio.<br>c. Considerar las regulaciones externas, obligaciones legales y contractuales y determinar cómo deben ser aplicadas en del gobierno de las TI de la organización.<br>d. Alinear el uso y el procesamiento ético de la información y su impacto en la sociedad, en el entorno natural y en los intereses de las partes interesadas internas y externas con los objetivos, visión y dirección de la organización.<br>e. Determinar las implicaciones del entorno de control conjunto de la organización con respecto a TI.<br>f. Articular los principios que guiarán el diseño de la toma de decisiones sobre el gobierno de las TI.<br>g. Comprender la cultura empresarial de la toma de decisiones y determinar un modelo óptimo en la toma de decisiones para TI.<br>h. Determinar los niveles apropiados para la delegación de autoridad, incluyendo reglas de umbrales, para las decisiones de las TI. |
| EDM01.02 Orientar el sistema de gobierno. | Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de las TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas. | a. Comunicar los principios del gobierno de las TI y acordar con el gestor ejecutivo la manera de establecer un liderazgo informado y comprometido.<br>b. Establecer o delegar el establecimiento de las estructuras, procesos y prácticas del gobierno en línea con los principios de diseño acordados.<br>c. Asignar responsabilidad, autoridad y la responsabilidad de que se apliquen los principios de diseños de gobierno, los modelos de toma de decisión y de delegación acordados.<br>d. Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos con la responsabilidad de la supervisión y toma de decisiones.<br>e. Orientar al personal para que siga las directrices relevantes para un comportamiento ético y profesional y garantizar que las consecuencias del no cumplimiento se conocen y se respetan.<br>f. Orientar el establecimiento de un sistema de recompensa para promover el cambio cultural deseable. |

Continuación tabla 82. Prácticas del proceso EDM01

| Prácticas proceso EDM01 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM01.03 Supervisar el sistema de gobierno | Supervisar la ejecución y la efectividad del gobierno de las TI de la organización. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de las TI. | a. Evaluar la efectividad y rendimiento de las partes interesadas en las que se ha delegado responsabilidad y autoridad para el gobierno de las TI de la organización.<br>b. Evaluar periódicamente si los mecanismos para el gobierno de las TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.<br>c. Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.<br>d. Mantener la supervisión sobre el punto hasta el que TI satisface las obligaciones (regulatorias, legislación, leyes comunes, contractuales), políticas internas, estándares y directrices profesionales.<br>e. Proporcionar supervisión de la efectividad de, y el cumplimiento, con el sistema de control de la organización.<br>f. Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de las TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices. |

**Proceso EDM02 Asegurar la entrega de beneficios**

Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de las TI resultado de la inversión hecha por TI a unos costos aceptables.

Su propósito es asegurar un valor óptimo de las iniciativas de las TI, servicios y activos disponibles; una entrega de costos eficiente de los servicios y soluciones y una visión confiable y precisa de los costos y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.

Tabla 83. Prácticas del proceso EDM02

| Prácticas proceso EDM02 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM02.01 Evaluar la optimización de valor | Evaluar continuamente las inversiones, servicios y activos del portafolio de las TI para determinar la probabilidad de alcanzar los objetivos de la organización y aportar valor a un costo razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor | a. Comprender los requerimientos de las partes interesadas; temas estratégicos de las TI, tales como la dependencia de las TI; y comprender la tecnología y sus capacidades considerando la importancia actual y potencial de las TI para la estrategia de la organización.<br>b. Comprender los elementos clave de gobierno necesarios para la entrega fiable, segura y económica de un valor óptimo por el uso de los servicios, activos y recursos de las TI existentes y potenciales.<br>c. Comprender y discutir regularmente las oportunidades que podrían surgir de los cambios habilitados en la organización por las tecnologías actuales, nuevas o emergentes y optimizar el valor creado por estas oportunidades.<br>d. Comprender lo que se entiende por valor en la organización y considerar cómo de bien se ha comunicado, comprendido y aplicado a través de los procesos de la organización.<br>e. Evaluar la efectividad de la integración y alineamiento de las estrategias de las TI en la organización y con los objetivos de la organización para aportar valor.<br>f. Comprender y considerar cómo de efectivos son los roles, responsabilidades, asignaciones y organismos de toma de decisiones actuales asegurando la creación de valor de las inversiones, servicios y activos de las TI.<br>g. Considerar cómo de bien alineada está la gestión de las inversiones, servicios y activos de las TI con la gestión de valor y las prácticas de gestión financiera.<br>h. Evaluar la alineación del portafolio de inversiones, servicios y activos con los objetivos estratégicos de la organización; con el valor de la organización financiero y no financiero; con el riesgo, tanto de servicio como al del beneficio; con los procesos de negocio; la efectividad en términos de usabilidad, disponibilidad y responsabilidad; y eficiencia en términos de coste, redundancia y salud técnica |

Continuación tabla 83. Prácticas del proceso EDM02

| Prácticas proceso EDM02 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM02.02 Orientar la optimización del valor. | Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico. | a. Definir y comunicar la cartera y los tipos de inversión, categorías, criterios y ponderaciones relativas a los criterios que permitan puntuaciones de valores relativos.<br>b. Definir los requerimientos para los cambios de fase (s*tage-gate*) y otras revisiones por la importancia de la inversión para la organización y el riesgo asociado, cronograma del programa, planes de financiación y la entrega de capacidades clave y beneficios y la contribución continuada al valor.<br>c. Orientar a la dirección para considerar usos potenciales de las TI innovadoras que posibiliten que la organización responda a nuevas oportunidades y desafíos, lleve a cabo nuevos negocios, incremente la competitividad o mejore sus procesos.<br>d. Orientar los cambios necesarios en la asignación de imputaciones y responsabilidades en la ejecución del portafolio de inversiones y la entrega de valor a partir de los servicios y procesos de negocio.<br>e. Definir y comunicar a nivel de organización los objetivos de entrega de valor y las medidas de resultados para permitir un control eficaz.<br>f. Orientar los cambios necesarios en la cartera de inversiones y servicios para realinearlos con los objetivos de la organización actuales y esperados y/o sus limitaciones.<br>g. Recomendar la consideración de innovaciones potenciales, cambios organizativos o mejoras operativas que desde las iniciativas TI pudieran impulsar un incremento de valor para la organización. |

Continuación tabla 83. Prácticas del proceso EDM02

| Prácticas proceso EDM02 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM02.03 Supervisar la optimización de valor. | Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Identificar los problemas significativos y considerar las acciones correctivas. | a. Definir un conjunto equilibrado de objetivos de desempeño, métricas, metas y puntos de referencia. Las métricas deberían cubrir la actividad y la medida de resultados, incluyendo los indicadores de retardo y de avance de los resultados, así como un equilibrio adecuado de las medidas financieras y no financieras. Revisarlos y acordarlos con las funciones de las TI y de negocio, y otras partes interesadas relevantes.<br>b. Recoger los datos pertinentes, oportunos, completos, fiables y precisos para informar sobre los avances en la entrega de valor respecto a los objetivos. Obtener una sucinta, de alto nivel, completa vista de la cartera, programa y desempeño TI (capacidades técnicas y operativas) que soporten la toma de decisiones y aseguren que los resultados esperados se están logrando.<br>c. Conseguir informes habituales y relevantes de la cartera, programa y desempeño de las TI (tecnológico y funcional). Revisar el progreso de la organización hacia los objetivos identificados y el grado en el que los objetivos previstos son alcanzados, los entregables obtenidos, los objetivos de rendimiento alcanzados y el riesgo mitigado.<br>d. Tras la revisión de los informes, tomar las medidas de gestión apropiadas según sea necesario para asegurar que el valor sea optimizado.<br>e. Tras la revisión de los informes, asegúrese de que las medidas correctivas apropiadas son iniciadas y controladas |

## Proceso EDM03 Asegurar la optimización del riesgo

Asegurar que el apetito y la tolerancia al riesgo de la organización son entendidos, articulados y comunicados y que el riesgo para el valor de la organización relacionado con el uso de las TI es identificado y gestionado.

Su propósito es asegurar que los riesgos relacionados con TI de la organización no exceden ni el apetito ni la tolerancia de riesgo, que el impacto de los riesgos de las TI en el valor de la organización se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.

Tabla 84. Prácticas del proceso EDM03

| Prácticas proceso EDM03 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM03.01 Evaluar la gestión de riesgos | Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la organización. Considerar si el apetito de riesgo de la organización es apropiado y el riesgo sobre el valor de la organización relacionado con el uso de las TI es identificado y gestionado. | a. Determinar el nivel de riesgos relacionados con las TI que la organización está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).<br>b. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la organización.<br>c. Determinar el grado de alineación de la estrategia de riesgos de las TI con la estrategia de riesgos empresariales.<br>d. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la organización pendientes y asegurar que las decisiones de la organización se toman conscientes de los riesgos.<br>e. Determinar si el uso de las TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.<br>f. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la organización para las pérdidas relacionadas con TI y la tolerancia de los líderes a los mismos. |
| EDM03.02 Orientar la gestión de riesgos | Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del consejo. | a. Promover una cultura consciente de los riesgos TI e impulsar a la organización a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.<br>b. Orientar la integración de las operaciones y la estrategia de riesgos de las TI con las decisiones y operaciones empresariales estratégicas.<br>c. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la organización), así como los planes de acción de riesgo.<br>d. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).<br>e. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.<br>f. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición. |

Continuación tabla 84. Prácticas del proceso EDM03

| Prácticas proceso EDM03 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM03.03 Supervisar la gestión de riesgos | Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución. | a. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.<br>b. Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.<br>c. Facilitar la revisión por las principales partes interesadas del progreso de la organización hacia los objetivos identificados.<br>d. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección. |

**Proceso EDM04 Asegurar la optimización de recursos**

Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la organización a un costo óptimo.

Su propósito es asegurar que las necesidades de recursos de la organización son cubiertas de un modo óptimo, que el costo TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.

Tabla 85. Prácticas del proceso EDM04

| Prácticas proceso EDM04 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM04.01 Evaluar la gestión de recursos. | Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la organización. | a. Examinar y evaluar la estrategia actual y futura, las opciones de aprovisionamiento de recursos TI y desarrollar capacidades para cubrir las necesidades actuales y futuras (incluyendo alternativas de aprovisionamiento).<br>b. Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI puedan satisfacer las necesidades de la organización, con la habilidad y capacidad requerida de acuerdo a las prioridades acordadas y las limitaciones presupuestarias.<br>c. Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la organización para la entrega de valor y la mitigación de riesgos con los recursos asignados.<br>d. Comprender los requisitos para alinear la gestión de recursos con la planificación de recursos empresariales financieros y humanos.<br>e. Definir los principios para la gestión y el control de la arquitectura de la organización. |
| EDM04.02 Orientar la gestión de recursos | Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de las TI a lo largo de su completo ciclo de vida económica | a. Comunicar e impulsar la adopción de estrategias de gestión de recursos, principios y el plan de recursos y las estrategias de arquitectura de organización acordadas.<br>b. Asignar responsabilidades para la ejecución de la gestión de recursos.<br>c. Definir los objetivos, medidas y métricas clave para la gestión de los recursos.<br>d. Establecer los principios relacionados con la protección de recursos.<br>e. Alinear la gestión de recursos con la planificación de RRHH y financiera de la organización. |
| EDM04.03 Supervisar la gestión de recursos | Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas. | a. Supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la organización mediante objetivos y métricas acordados.<br>b. Supervisar las estrategias de aprovisionamiento TI y de arquitectura de la organización y los recursos y capacidades TI para garantizar que las necesidades actuales y futuras de la organización puedan ser satisfechas.<br>c. Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes. |

### Proceso EDM05 Asegurar la transparencia hacia las partes interesadas

Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la organización son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.

Su propósito es asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.

Tabla 86. Prácticas del proceso EDM05

| Prácticas proceso EDM05 | | |
|---|---|---|
| **Práctica** | **Definición** | **Principales actividades** |
| EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. | Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación. | a. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes respecto al uso de las TI dentro de la organización (regulación, legislación, leyes generales, requisitos contractuales), incluyendo alcance y frecuencia.<br>b. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes para otros interesados respecto al uso de las TI dentro de la organización, incluyendo alcance y condiciones.<br>c. Mantener los principios de comunicación con interesados externos e internos, incluyendo formatos y canales de comunicación y los principios de aceptación y aprobación de los informes por parte de las partes interesadas. |
| EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes. | Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas. | a. Orientar el establecimiento de la estrategia de comunicación para interesados externos e internos.<br>b. Orientar la implementación de mecanismos para garantizar que la información cumple todos los criterios de los requisitos corporativos obligatorios en cuanto a elaboración de informes de las TI.<br>c. Establecer mecanismos de validación y aprobación de la elaboración obligatoria de informes.<br>d. Establecer mecanismos de escalado en la elaboración de informes. |
| EDM05.03 Supervisar la comunicación con las partes interesadas | Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados. | a. Evaluar periódicamente la eficacia de los mecanismos para asegurar la precisión y la fiabilidad de la elaboración obligatoria de informes.<br>b. Evaluar periódicamente la eficacia de los mecanismos y las salidas de la comunicación con interesados externos e internos.<br>c. Determinar si se están cumpliendo los requisitos de los diferentes interesados. |

## Ejercicio de refuerzo - el dominio de gobierno de CobiT 5

¿Cuáles son los procesos del dominio de gobierno de CobiT 5?

# Dominios de gestión de las TI

En CobiT 5 existen cuatro dominios de gestión de las TI, también mencionados como PBRM

– Alinear, planificar y organizar (*Align, Plan and Organize, APO*)
– Construir, adquirir e implementar (*Build, Acquire and Implement*, BAI)
– Entregar, dar servicio y soporte (*Deliver, Service and Support,* DSS)
– Monitorear, evaluar y valorar (*Monitor, Evaluate and Assess*, MEA)

## 7.11.2 Dominio: Alinear, Planificar y Organizar, APO

Hay 13 procesos en este dominio, a saber:

- APO01 Gestionar el marco de gestión de las TI.
- APO02 Gestionar la estrategia.
- APO03 Gestionar la arquitectura empresarial.
- APO04 Gestionar la innovación.
- APO05 Gestionar el portafolio.
- APO06 Gestionar el presupuesto y los costos.
- APO07Gestionar los recursos humanos.
- APO08 Gestionar las relaciones.
- APO09 Gestionar los acuerdos de servicio.
- APO10 Gestionar los proveedores.
- APO11Gestionar la calidad.
- APO12 Gestionar el riesgo.
- APO13 Gestionar la seguridad.

**Proceso APO01. Gestionar el marco de gestión de las TI**

Aclarar y mantener el gobierno de la misión y la visión corporativa de las TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de las TI en la organización, para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.

Su propósito es proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.

Y sus prácticas son:

- APO01.01 Definir la estructura organizativa.
- APO01.02 Establecer roles y responsabilidades.
- APO01.03 Mantener los elementos facilitadores del sistema de gestión.
- APO01.04 Comunicar los objetivos y la dirección de gestión.
- APO01.05 Optimizar la ubicación de la función de las TI.
- APO01.06 Definir la propiedad de la información (datos) y del sistema.
- APO01.07 Gestionar la mejora continua de los procesos.
- APO01.08 Mantener el cumplimiento con las políticas y procedimientos.

### Proceso APO02. Gestionar la estrategia

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

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

Y sus prácticas son:

- APO02.01 Comprender la dirección de la organización.
- APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.
- APO02.03 Definir el objetivo de las capacidades de las TI.
- APO02.04 Realizar un análisis de diferencias.
- APO02.05 Definir el plan estratégico y la hoja de ruta.
- APO02.06 Comunicar la estrategia y la dirección de las TI.

### Proceso APO03. Gestionar la arquitectura empresarial

Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la organización y de las TI, mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costos potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.

Su propósito es representar a los diferentes módulos que componen la organización y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos.

Y sus prácticas son:

- APO03.01 Desarrollar la visión de la arquitectura de la organización.
- APO03.02 Definir la arquitectura de referencia.
- APO03.03 Seleccionar las oportunidades y las soluciones.
- APO03.04 Definir la implementación de la arquitectura.
- APO03.05 Proveer los servicios de arquitectura empresarial.

### Proceso APO04. Gestionar la innovación

Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de las TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de la organización.

Su propósito es lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.

Y sus prácticas son:

- APO04.01 Crear un entorno favorable para la innovación.
- APO04.02 Mantener un entendimiento del entorno de la organización.
- APO04.03 Supervisar y explorar el entorno tecnológico.
- APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.
- APO04.05 Recomendar iniciativas apropiadas adicionales.
- APO04.06 Supervisar la implementación y el uso de la innovación.

### Proceso APO05. Gestionar el portafolio

Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación.

Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.

Su propósito es optimizar el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas.

Y sus prácticas son:

- APO05.01 Establecer la mezcla del objetivo de inversión.
- APO05.02 Determinar la disponibilidad y las fuentes de fondos.
- APO05.03 Evaluar y seleccionar los programas a financiar.
- APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.
- APO05.05 Mantener los portafolios.
- APO05.06 Gestionar la consecución de beneficios.

### Proceso APO06. Gestionar el presupuesto y los costos

Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de las TI, abarcando presupuesto, costo y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costos a la organización. Consultar a las partes interesadas para identificar y controlar los costos totales y los beneficios en el contexto de los planes estratégicos y tácticos de las TI, e iniciar acciones correctivas cuando sea necesario.

Su propósito es fomentar la colaboración entre TI y las partes interesadas de la organización para facilitar el uso eficaz y eficiente de los recursos relacionados con las TI y brindar transparencia y responsabilidad sobre el costo y valor de negocio de soluciones y servicios. Permitir a la organización tomar decisiones informadas con respecto a la utilización de soluciones y servicios de las TI.

Y sus prácticas son:

- APO06.01 Gestionar las finanzas y la contabilidad.
- APO06.02 Priorizar la asignación de recursos.
- APO06.03 Crear y mantener presupuestos
- APO06.04 Modelar y asignar costos.
- APO06.05 Gestionar costos.

### Proceso APO07. Gestionar los recursos humanos

Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.

Su propósito es optimizar las capacidades de recursos humanos para cumplir los objetivos de la organización.

Y sus prácticas son:

- APO07.01 Mantener la dotación de personal suficiente y adecuada.
- APO07.02 Identificar personal clave de las TI.
- APO07.03 Mantener las habilidades y competencias del personal.

- » APO07.04 Evaluar el desempeño laboral de los empleados.
- » APO07.05 Planificar y realizar un seguimiento del uso de recur sos humanos de las TI y del negocio.
- » APO07.06 Gestionar el personal contratado.

### Proceso APo08. Gestionar las relaciones

Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos, apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.

Su propósito es crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.

Y sus prácticas son:

- » APO08.01 Entender las expectativas del negocio
- » APO08.02 Identificar oportunidades, riesgos y limitaciones de las TI para mejorar el negocio.
- » APO08.03 Gestionar las relaciones con el negocio.
- » APO08.04 Coordinar y comunicar.
- » APO08.05 Proveer datos de entrada para la mejora continua de los servicios.

### Proceso APo09. Gestionar los acuerdos de servicio

Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la organización, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.

Su propósito es asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la organización.

Y sus prácticas son:

- » APO09.01 Identificar servicios TI.
- » APO09.02 Catalogar servicios basados en TI.
- » APO09.03 Definir y preparar acuerdos de servicio.
- » APO09.04 Supervisar e informar de los niveles de servicio.
- » APO09.05 Revisar acuerdos de servicio y contratos.

### Proceso APO10. Gestionar los proveedores

Administrar todos los servicios de las TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.

Su propósito es minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.

Y sus prácticas son:

- APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.
- APO10.02 Seleccionar proveedores.
- APO10.03 Gestionar contratos y relaciones con proveedores.
- APO10.04 Gestionar el riesgo en el suministro.
- APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor.

### Proceso APO11. Gestionar la calidad

Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.

Su propósito es asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.

Y sus prácticas son:

- APO11.01 Establecer un sistema de gestión de la calidad (SGC).
- APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
- APO11.03 Enfocar la gestión de la calidad en los clientes.
- APO11.04 Supervisar y hacer controles y revisiones de calidad.
- APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.
- APO11.06 Mantener una mejora continua

### Proceso APO12. Gestionar el riesgo

Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la organización.

Su propósito es integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costos y beneficios de gestionar riesgos empresariales relacionados con TI.

Y sus prácticas son:

- APO12.01 Recopilar datos.
- APO12.02 Analizar el riesgo.
- APO12.03 Mantener un perfil de riesgo.
- APO12.04 Expresar el riesgo.
- APO12.05 Definir un portafolio de acciones para la gestión de riesgos.
- APO12.06 Responder al riesgo.

### Proceso APO13 Gestionar la seguridad

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

Su propósito es mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la organización.

Y sus prácticas son:

- APO13.01 Establecer y mantener un SGSI.
- APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
- APO13.03 Supervisar y revisar el SGSI.

## Ejercicio de refuerzo - el dominio de gestión de CobiT 5: Alinear, Planear y Organizar

Compare los procesos de este dominio con los del dominio Planear y Organizar de CobiT 4.1 y diga las diferencias generales

### 7.11.3 Dominio: Construir, Adquirir e Implementar, BAI

Existen 10 procesos en este dominio, a saber:

- BAI01 Gestionar programas y proyectos.
- BAI02 Gestionar la definición de requisitos.
- BAI03 Gestionar la identificación y construcción de soluciones.
- BAI04 Gestionar la disponibilidad y la capacidad.
- BAI05 Gestionar la introducción del cambio organizativo.
- BAI06 Gestionar los cambios.
- BAI07 Gestionar la aceptación del cambio y la transición.
- BAI08 Gestionar el conocimiento.
- BAI09 Gestionar los activos.
- BAI10 Gestionar la configuración.

#### Proceso BAI01. Gestión de programas y proyectos

Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.

Su propósito es alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costos inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.

Y sus prácticas son:

- BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos.
- BAI01.02 Iniciar un programa.
- BAI01.03 Gestionar el compromiso de las partes interesadas.
- BAI01.04 Desarrollar y mantener el plan de programa.
- BAI01.05 Lanzar y ejecutar el programa.
- BAI01.06 Supervisar, controlar e informar de los resultados del programa.
- BAI01.07 Lanzar e iniciar proyectos dentro de un programa.
- BAI01.08 Planificar proyectos.
- BAI01.09 Gestionar la calidad de los programas y proyectos.
- BAI01.10 Gestionar el riesgo de los programas y proyectos.

- » BAI01.11 Supervisar y controlar proyectos.
- » BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.
- » BAI01.13 Cerrar un proyecto o iteración.
- » BAI01.14 Cerrar un programa.

### Proceso BAI02. Gestionar la definición de requisitos

Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costos y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.

Su propósito es crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.

Y sus prácticas son:

- » BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.
- » BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.
- » BAI02.03 Gestionar los riesgos de los requerimientos.
- » BAI02.04 Obtener la aprobación de los requerimientos y soluciones.

### Proceso BAI03. Gestionar la identificación y construcción de soluciones

Establecer y mantener soluciones identificadas en línea con los requerimientos de la organización que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

Su propósito es establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales.

Y sus prácticas son:

- BAI03.01 Diseñar soluciones de alto nivel.
- BAI03.02 Diseñar los componentes detallados de la solución
- BAI03.03 Desarrollar los componentes de la solución
- BAI03.04 Obtener los componentes de la Solución
- BAI03.05 Construir soluciones.
- BAI03.06 Realizar controles de calidad.
- BAI03.07 Preparar pruebas de la solución
- BAI03.08 Ejecutar pruebas de la solución
- BAI03.09 Gestionar cambios a los requerimientos.
- BAI03.10 Mantener soluciones.
- BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.

### Proceso BAI04. Gestionar la disponibilidad y la capacidad

Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costos. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.

Su propósito es mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad.

Y sus prácticas son:

- BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.
- BAI04.02 Evaluar el impacto en el negocio.
- BAI04.03 Planificar requisitos de servicio nuevos o modificados.
- BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.
- BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.

### Proceso BAI05. Gestionar la facilitación del cambio organizativo

Maximizar la probabilidad de la implementación exitosa en toda la organización del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de las TI.

Su propósito es preparar y comprometer a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.

Y sus prácticas son:

- BAI05.01 Establecer el deseo de cambiar.
- BAI05.02 Formar un equipo de implementación efectivo.
- BAI05.03 Comunicar la visión deseada.
- BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.
- BAI05.05 Facilitar la operación y el uso.
- BAI05.06 Integrar nuevos enfoques.
- BAI05.07 Mantener los cambios.

### Proceso BAI06. Gestionar los cambios

Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

Su propósito es posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.

Y sus prácticas son:

- BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.
- BAI06.02 Gestionar cambios de emergencia. Hacer seguimiento e informar de cambios de estado.
- BAI06.03 Hacer seguimiento e informar de cambios de estado.
- BAI06.04 Cerrar y documentar los cambios.

### Proceso BAI07. Gestionar la aceptación del cambio y la transición

Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.

Su propósito es implementar soluciones de forma segura y en línea con las expectativas y resultados acordados.

Y sus prácticas son:

- BAI07.01 Establecer un plan de implementación.
- BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.
- BAI07.03 Planificar pruebas de aceptación.
- BAI07.04 Establecer un entorno de pruebas.
- BAI07.05 Ejecutar pruebas de aceptación.
- BAI07.06 Pasar a producción y gestionar los lanzamientos.
- BAI07.07 Proporcionar soporte en producción desde el primer momento.
- BAI07.08 Ejecutar una revisión post-implantación.

### Proceso BAI08. Gestionar el conocimiento

Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.

Su propósito es proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad.

Y sus prácticas son:

- BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos.
- BAI08.02 Identificar y clasificar las fuentes de información.
- BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.
- BAI08.04 Utilizar y compartir el conocimiento.
- BAI08.05 Evaluar y retirar la información.

### Proceso BAI09. Gestionar los activos

Gestionar los activos de las TI a través de su ciclo de vida para asegurar que su uso aporta valor a un costo óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.

Su propósito es contabilización de todos los activos de las TI y optimización del valor proporcionado por estos activos.

Y sus prácticas son:

- BAI09.01 Identificar y registrar activos actuales.
- BAI09.02 Gestionar activos críticos
- BAI09.03 Gestionar el ciclo de vida de los activos.
- BAI09.04 Optimizar el coste de los activos.
- BAI09.05 Administrar licencias.

### Proceso BAI10. Gestionar la configuración

Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

Su propósito es proporcionar suficiente información sobre los activos del servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.

Y sus prácticas son:

- BAI10.01 Establecer y mantener un modelo de configuración.
- BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.
- BAI10.03 Mantener y controlar los ítem de configuración.
- BAI10.04 Generar informes de estado y configuración.
- BAI10.05 Verificar y revisar la integridad del repositorio de configuración.

## Ejercicio de refuerzo - El dominio de gestión de CobiT 5: Construir, Adquirir e Implementar

Compare los procesos de este dominio con los del dominio: Adquirir e Implementar de CobiT 4.1 y cite algunas diferencias generales

### 7.11.4 Dominio: Entrega, Servicio y Soporte, DSS

Hay seis procesos en este dominio, a saber:

- DSS01 Gestionar operaciones.
- DSS02 Gestionar peticiones e incidentes de servicio.
- DSS03 Gestionar problemas.
- DSS04 Gestionar la continuidad.
- DSS05 Gestionar servicios de seguridad.
- DSS06 Gestionar controles de procesos de negocio.

#### Proceso DSS01. Gestionar operaciones

Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de las TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

Su propósito es entregar los resultados del servicio operativo de las TI, según lo planificado.

Y sus prácticas son:

- DSS01.01 Ejecutar procedimientos operativos
- DSS01.02 Gestionar servicios externalizados de las TI
- DSS01.03 Supervisar la infraestructura de las TI
- DSS01.04 Gestionar el entorno
- DSS01.05 Gestionar las instalaciones

#### Proceso DSS02. Gestionar peticiones e incidentes de servicio

Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

Su propósito es lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.

Y sus prácticas son:

- DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.
- DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.
- DSS02.03 Verificar, aprobar y resolver peticiones de servicio.
- DSS02.04 Investigar, diagnosticar y localizar incidentes.
- DSS02.05 Resolver y recuperarse de incidentes.
- DSS02.06 Cerrar peticiones de servicio e incidentes.
- DSS02.07 Seguir el estado y emitir informes.

### Proceso DSS03. Gestionar problemas

Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

Su propósito es incrementar la disponibilidad, mejorar los niveles de servicio, reducir costos, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.

Y sus prácticas son:

- DSS03.01 Identificar y clasificar problemas.
- DSS03.02 Investigar y diagnosticar problemas.
- DSS03.03 Levantar errores conocidos.
- DSS03.04 Resolver y cerrar problemas.
- DSS03.05 Realizar una gestión de problemas proactiva.

### Proceso DSS04. Gestionar la continuidad

Establecer y mantener un plan para permitir al negocio y a la TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la organización.

Su propósito es continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la organización ante el evento de una interrupción significativa.

Y sus prácticas son:

- DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.
- DSS04.02 Mantener una estrategia de continuidad.
- DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
- DSS04.04 Ejercitar, probar y revisar el plan de continuidad.
- DSS04.05 Revisar, mantener y mejorar el plan de continuidad.
- DSS04.06 Proporcionar formación en el plan de continuidad.
- DSS04.07 Gestionar acuerdos de respaldo.
- DSS04.08 Ejecutar revisiones posterior a la reanudación.

### Proceso DSS05. Gestionar servicios de seguridad

Proteger la información de la organización para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

Su propósito es minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.

Y sus prácticas son:

- DSS05.01 Proteger contra software malicioso (*malware*).
- DSS05.02 Gestionar la seguridad de la red y las conexiones.
- DSS05.03 Gestionar la seguridad de los puestos de usuario final.
- DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
- DSS05.05 Gestionar el acceso físico a los activos de las TI.
- DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
- DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

### Proceso DSS06. Gestionar controles de procesos de negocio

Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la or-

ganización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.

Propósito del proceso mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la organización o externalizados.

Y sus prácticas son:

- DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.
- DSS06.02 Controlar el procesamiento de la información.
- DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
- DSS06.04 Gestionar errores y excepciones.
- DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.
- DSS06.06 Asegurar los activos de información.

### Ejercicio de refuerzo - El dominio de gestión de CobiT 5: Entrega, Servicio y Soporte

Compare los procesos de este dominio con los del dominio: Entrega y Soporte de CobiT 4.1 y cite algunas diferencias generales

## 7.11.5 Dominio: Monitorear, Evaluar y Valorar, MEA

Hay tres procesos en este dominio, a saber:

- MEA01 Monitorear, evaluar y valorar el rendimiento y la conformidad.
- MEA02 Monitorear, evaluar y valorar el sistema de control interno.
- MEA03 Monitorear, evaluar y valorar la conformidad con los requerimientos externos.

### Proceso MEA01. Monitorear, evaluar y valorar el rendimiento y la conformidad

Recolectar, validar y evaluar métricas y objetivos de negocio, de las TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

Su propósito es proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.

Y sus prácticas son:

- MEA01.01 Establecer un enfoque de la supervisión.
- MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.
- MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.
- MEA01.04 Analizar e informar sobre el rendimiento.
- MEA01.05 Asegurar la implantación de medidas correctivas.

### Proceso MEA02. Monitorear, evaluar y valorar el sistema de control interno

Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

Su propósito es ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.

Y sus prácticas son:

- MEA02.01 Supervisar el control interno.
- MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.
- MEA02.03 Realizar autoevaluaciones de control.
- MEA02.04 Identificar y comunicar las deficiencias de control.
- MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.

- MEA02.06 Planificar iniciativas de aseguramiento.
- MEA02.07 Estudiar las iniciativas de aseguramiento.
- MEA02.08 Ejecutar las iniciativas de aseguramiento.

**Proceso MEA03. Monitorear, evaluar y valorar la conformidad con los requerimientos externos.**

Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de las TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de las TI en el cumplimiento de la organización general.

Su propósito es asegurar que la organización cumple con todos los requisitos externos que le sean aplicables.

Y sus prácticas son:

- MEA03.01 Identificar requisitos externos de cumplimiento.
- MEA03.02 Optimizar la respuesta a requisitos externos.
- MEA03.03 Confirmar el cumplimiento de requisitos externos.
- MEA03.04 Obtener garantía de cumplimiento de requisitos externos.

A continuación se presenta un resumen de procesos y prácticas descritos anteriormente.

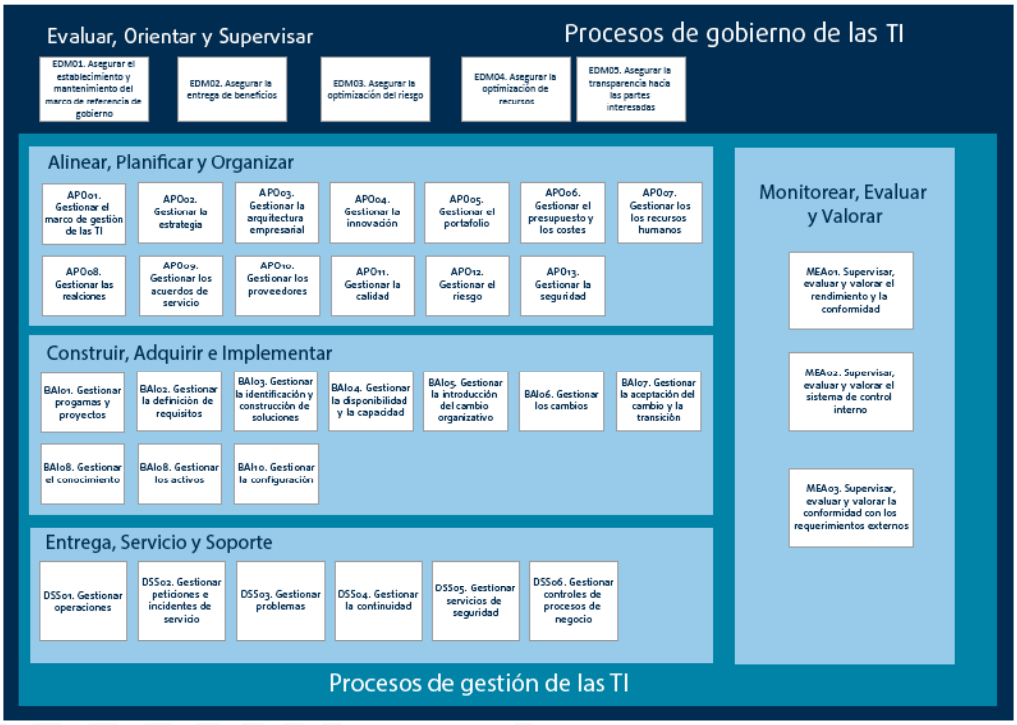



**Figura 31.**
Procesos
y prácticas
del CobiT 5

Capítulo

08

# Cuaderno de actividades

## 8.1 Guía de actividades 1

### Actividad 1 – alineamiento estratégico en las organizaciones públicas

Una organización pública (nacional, departamental, o municipal) definió los siguientes procesos de negocio:

- Aumento del recaudo;
- Aplicar recursos.

El gobierno de las TI definió los siguientes procesos:

- Adquirir y mantener la infraestructura tecnológica;
- Adquirir y mantener los sistemas y aplicaciones;
- Asegurar la continuidad de los servicios;
- Asegurar la seguridad del sistema;
- Gestionar las operaciones;
- Gestionar los datos.

La armonía entre los procesos de negocio y los procesos de las TI garantiza el alineamiento entre el gobierno corporativo y el gobierno de las TI.


**Figura 32.** Alineamiento entre procesos de negocio y procesos de las TI.

## Procesos de las TI

Con la información descrita, complete los espacios en blanco:

» Para el proceso de negocio "aumentar el recaudo" fueron propuestos los siguientes objetivos:
  - Negociar impuestos atrasados;

» Para el proceso de negocio " aplicar recursos" fueron propuestos los siguientes objetivos:
  - Definir prioridades;

» Para el proceso de las TI de "adquisición y conservación de la infraestructura tecnológica" fueron propuestos los siguientes objetivos:
  - Crear agilidad para la TI;

» Para el proceso de las TI de "adquisición y conservación de los sistemas y aplicaciones" fueron propuestos los siguientes objetivos:
  - Definir cómo las funciones de negocio y requerimientos de control son convertidos en soluciones automatizadas efectivas y eficientes;

» Para el proceso de las TI de "asegurar la continuidad de los servicios" fueron propuestos los siguientes objetivos:
  - Asegurar que los servicios e infraestructuras de las TI pueden resistir y recuperarse de fallas causadas por errores, ataques de liberados o desastres;

» Para el proceso de las TI de "asegurar la seguridad de los sistemas" los siguientes objetivos fueron propuestos:
  - Responsabilizar y proteger todos los activos de las TI;

» Para el proceso de las TI " Gestionar las operaciones" fueron propuestos los siguientes objetivos:
  - Asegurar la satisfacción de los usuarios finales con la oferta y niveles de servicios;

### Actividad 2. Gestión de recursos

Describa las acciones que su organización realiza para mantener la gestión de recursos alineada con el negocio.

- Información:
  - Definición de un plan de continuidad de servicios de las TI;

- Aplicativos:
  - Desarrollo de sistemas de acuerdo con la aprobación de los requisitos del negocio;

- Infraestructura:
  - Elaboración de un plan de dirección de arquitectura tecnológica;

- Personas:
  - Desarrollo de un plan de capacitación;

### Actividad 3. Gestión de riesgos

Su organización necesita entender los daños que los riesgos de seguridad pueden causar a los negocios. Las preguntas a continuación ayudan a su organización a identificar los riesgos y sus daños. Suponiendo que usted es el responsable de determinar los riesgos de su organización, responda las siguientes preguntas:

- ¿Cuáles son las partes más importantes de los negocios de su organización (productos, servicios, actividades, entre otros)?
- ¿Cómo es soportado el negocio por el uso de tecnología y qué tan esencial es este soporte?
- ¿Cuánto dependen las decisiones esenciales de la actualización, precisión, disponibilidad e integridad de la información?
- ¿Cuál es la información confidencial que necesita ser protegida?
- ¿Cuáles son las implicaciones de los incidentes de seguridad, relacionados a la información, para los negocios y para su organización?

## 8.2 Guía de actividades 2

### Actividad 1. Alineamiento entre objetivos de la organización y objetivos de las TI

Una agencia pública ambiental posee en su planta de personal 250 profesionales, y está instalada en una sola localidad que hospeda sus operaciones. La agencia presta los servicios de control y monitoreo del medio ambiente de una determinada localidad y brinda información para otros órganos públicos y privados, y obtiene información externa para sus estudios. Todo el equipo de las TI de esta agencia está compuesto por 12 funcionarios que trabajan tiempo completo, realizando las actividades de gestión, soporte y desarrollo de aplicaciones para soportar las actividades de la organización. Actualmente, el área de las TI y el área de negocios no tienen alineamiento, o sea, las acciones de las TI y del negocio son tomadas de forma independiente.

1. Considerando esta información, defina:

Tres objetivos de negocio que esta agencia posee.
a.
b.
c.

Tres objetivos de las TI alineados a los objetivos de negocio.
a.
b.
c.

Tres objetivos de procesos de las TI asociados a los objetivos de las TI.
a.
b.
c.

Tres objetivos de actividades relacionadas a los tres procesos de las TI.

a.
b.
c.

2. Después de las definiciones, establezca el alineamiento entre los objetivos, de acuerdo con el siguiente modelo:

Tabla 87. Ejercicio alineamiento entre objetivos de la organización y objetivos de las TI

| Objetivos de negocio | Objetivos de las TI | Objetivos de procesos | Objetivos de actividades |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

### Actividad 2. Gestión de riesgos en TI

La siguiente tabla presenta una lista de riesgos a los que está sometida una organización cuando no implementa la gestión de riesgos en el gobierno de las TI. Para cada riesgo de la tabla, defina un objetivo de control para minimizar o eliminar este riesgo. Utilice el *framework* CobiT 4.1 para resolver esta actividad.

Tabla 88. Ejercicio gestión de riesgos en TI

| Riesgo | Objetivo de control |
|---|---|
| Los planes de las TI no están presentes en los planes de corto o largo plazo de la organización. Los planes de la organización no soportan a TI. | |
| Los planes de las TI no son actualizados regularmente. | |
| Los cambios en los negocios o en la TI pueden involuntariamente generar impactos en los planes de las TI. | |
| La arquitectura de las TI no soporta el crecimiento de la organización o de los objetivos de negocios. | |
| Los niveles de seguridad del área de las TI no están de acuerdo con políticas reguladoras o empresariales referentes a la protección de la información. Los planes de seguridad de la información no están siendo actualizados regularmente. | |
| El desarrollo de sistemas no sigue los procesos de procedimientos reguladores o empresariales y colocan en riesgo la integridad de los datos. | |
| Los proveedores tienen acceso a datos protegidos y confidenciales, y la privacidad de la información puede estar comprometida. | |

## Actividad 3. Evaluando el nivel de madurez de los procesos

Una organización del área de prestación de servicios automotrices realizó una evaluación para obtener el nivel de madurez en que se encuentran los procesos y las mejoras que deben ser realizadas. La siguiente tabla muestra el resultado de cada uno de los procesos evaluados. Para cada nivel de madurez alcanzado, y suponiendo que usted fuese el evaluador, describa el motivo que definió el nivel de madurez.

Tabla 89. Ejercicio evaluando el nivel de madurez de los procesos

| Proceso | Madurez | Aspectos considerados para la definición de madurez |
|---|---|---|
| Balanceo de ruedas | 2 – Repetible | |
| Cambio de amortiguadores | 3 – Proceso definido | |
| Cambio de frenos | 4 – gestionado y medido | |
| Atención | 1 – Inicial/Ad Hoc | |
| Facturación | 5 – Optimizado | |

## 8.3 Guía de Actividades 3

### Actividad 1. Recomendaciones para la planificación estratégica de las TI

El siguiente texto es el resultado de la evaluación del proceso de planificación estratégica de una organización.

El proceso de planificación estratégica de las TI (PO1 - Definir un plan estratégico de las TI) se inició con una gran lluvia de ideas con área de negocio (clientes), que tenía un canal abierto, libre y sin ninguna imposición de las TI que sólo conducía a las actividades. De este modo, se identificó un conjunto de proyectos con participación del área TI, que fueron priorizados dando lugar a iniciativas estratégicas. Este trabajo se realizó en paralelo con la planificación estratégica de la organización, con el objetivo de ganar tiempo, pero resultó generando un riesgo de reprocesamiento.

La participación del área de negocio fue vital, fomentando ganancias de conocimiento comunicación y comprometimiento; pero, la paralelización de actividades de planificación de las TI frente a la planificación estratégica no permitió una consecuencia natural de las acciones estratégicas.

A pesar de haber realizado un mapeo de las iniciativas de las TI en las iniciativas de la organización, generando de esta manera las iniciativas de las TI consideradas estratégicas, esto incrustó riesgos de asignación de recursos en proyectos no prioritarios y un reprocesamiento en la planificación de las TI. Por otra parte, el número de iniciativas se consideró elevado cuando se trata de estrategia, lo que hace difícil la ejecución de todos los proyectos. Así, a pesar de todo el involucramiento de la organización no quedó evidenciado un proceso de planificación definido sino apenas una secuencia de acciones.

Con la información sobre la evaluación, ¿Cuál sería la recomendación para que la organización realice una planificación estratégica de las TI para lograr el gobierno de las TI?

## Actividad 2. Definiendo procesos de CobiT para la implementación en la organización

En una organización pública no existe un plan de infraestructura tecnológica. El proceso Utilizado para el direccionamiento tecnológico está basado en el análisis de impacto en la infraestructura instalada, mediante las necesidades de la organización, que llega al área de las TI bajo la forma de demanda, sin criterios preestablecidos. Ese análisis de impacto contempla la identificación de nuevas adquisiciones de infraestructura y además una estimación financiera.

El hecho de no existir un Plan Estratégico de las TI, PETI, implica que no existe un alineamiento entre TI y el área de negocio, por lo tanto se puede decir que este proceso es inicial, sin las definiciones de una estructura, roles, responsabilidades y herramientas de apoyo. Cuando los proyectos de las TI son iniciados un desglose de bajo criterio de la infraestructura necesaria es realizado.

De acuerdo con las afirmaciones anteriores, ¿Cuáles procesos de CobiT 4.1 deberían ser implementados y que debería hacer la organización para minimizar los problemas, tanto para TI como para el negocio? Justifique la elección de los procesos.

**Actividad 3. Definiendo los criterios para alcanzar el nivel de madurez esperado**

En una organización, fueron obtenidos los siguientes niveles de madurez después de una evaluación de los procesos de CobiT 4.1:

Tabla 90. Niveles de madurez después de una evaluación de los procesos de CobiT 4.1

| Proceso | Madurez | Aspectos considerados para la definición de madurez |
|---|---|---|
| AI3 – Adquirir y mantener la infraestructura de tecnología | 1 – Inicial/Ad Hoc | La adquisición y el mantenimiento de la infraestructura de las TI no están basados en una estrategia, sino son llevadas en consideración las aplicaciones de negocio que deben ser soportadas. Existe la comprensión de la importancia de la infraestructura de las TI con base en prácticas formales. Algunos mantenimientos son programados, pero no existe una ventana de mantenimiento definida. Existen ambientes de pruebas separados |
| AI6 – Gestionar Cambios | 2 – Repetitivo | La organización es consciente de la importancia de un proceso de gestión de cambios pero la mayoría de los cambios no sigue este proceso, aumentando los riesgos relacionados con la ocurrencia de problemas. La documentación de la configuración es inconsistente, por la falta de una base de datos de configuración. Además son ejecutados una planificación y un análisis de impacto limitado. |
| AI7 –Instalar y homologar soluciones y cambios | 2 – Repetitivo | Una metodología relacionada con la instalación, migración, conversión y homologación está establecida. Mientras tanto, la gestión de esa metodología no trae resultados de conformidad con el proceso. Aunque exista formalmente un ciclo de vida de desarrollo, instalación y homologación no se integran con la gestión de configuraciones. La calidad de las soluciones que entran en producción es variable y generalmente esas soluciones no tienen una revisión pos implantación. |

Después de esta información defina para cada proceso:

- ¿Qué debe ser considerado para que los procesos alcancen el nivel 3 de madurez?
- ¿Cuáles acciones deben ser desarrolladas para alcanzar el nivel 3 de madurez?
- ¿Cuáles resultados serán alcanzados con la ejecución de las acciones y consecuentemente del nivel de madurez deseado?

### Actividad 4 (Completar). Alineamiento con los procesos de CobiT 4.1

La siguiente tabla presenta un conjunto de acciones que una organización debería ejecutar para alcanzar el gobierno de las TI. Relacione que procesos de CobiT 4.1 están asociados con las acciones propuestas.

Tabla 91. Ejercicio Alineamiento con los procesos de CobiT 4.1

| Acciones | Alineamiento con los procesos de CobiT 4.1 |
|---|---|
| Alinear el área de tecnología y sus actividades a los objetivos estratégicos de la organización, por medio de la definición de procesos estructurados para la Planificación Estrategia de Tecnología, así como su formalización. | |
| Formalizar las principales normas y procesos de tecnologías, además de definir la estructura organizacional necesaria para la ejecución de la estrategia, del presupuesto y del enfoque de calidad. Con el fin de crear un plan de comunicación coherente con la estrategia. | |
| Definir un conjunto de procesos, estándares y guías para formalizar, estructurar, garantizar la calidad en el desarrollo de soluciones de tecnología, tanto para soluciones desarrolladas internamente como para adquiridas. | |
| Definir una arquitectura de información corporativa creando y manteniendo un modelo de información de negocio y garantizando la adopción de esta arquitectura en desarrollo de sistemas. | |

## 8.4 Guía de Actividades 4

**Actividad 1. Auditoría de continuidad de los negocios**

En una organización fue realizada una auditoría para evaluar la continuidad de los negocios. Los auditores levantaron los siguientes puntos:

- La organización definió un plan de continuidad de negocios para el proceso de negocio de nuevos clientes. Esta iniciativa está siendo realizada con el énfasis en entrenamiento/piloto de una posible solución de la organización y atención a los intereses de las TI.
- El plan elaborado para este proceso es bastante consistente con las estrategias de negocio de la organización. Pero los planes de continuidad no fueron probados, hecho que crea un riesgo muy grande en el caso de que este plan se necesite.
- Aún con la iniciativa, no existe un marco para la continuidad del negocio, esto es, personas responsables, procesos y metodología de apoyo.
- No fueron identificadas evidencias sobre iniciativas organizacionales para la continuidad del negocio.
- Desde el punto de vista técnico, existe redundancia de máquinas para algunos servicios.
- Existen iniciativas aisladas para la elaboración de un plan de recuperación de desastres.
- Desde el punto de vista del negocio, no existen información sobre procedimientos alternativos de las demás áreas de la organización.
- No fueron encontradas evidencias sobre la existencia de un trabajo de identificación de recursos críticos, consecuentemente no fueron observadas acciones para definir alternativas para la operación de esos recursos en caso de catástrofe.

Suponiendo que usted sea el auditor, ¿cuáles serían sus recomendaciones para esta organización sobre la continuidad de los negocios?

### Actividad 2. Evaluación del área de las TI

En una evaluación del área de las TI de una organización, fueron identificados los siguientes aspectos relevantes:

- Se puede dividir el área de las TI de la organización en dos cuando hablamos de ANS. En el caso de prestación de servicios internos, no existe ningún tipo de acuerdo de servicios, todo es hecho de manera informal para el usuario de negocio, mientras el equipo de atención está consciente de los plazos establecidos (informalmente) y actúan conforme a esa información. En el caso de los clientes externos existe un centro de atención que posee ANS definida para la atención.
- En la relación entre la organización y sus proveedores, existen ANSs en todos los contratos, y son acompañados mediante informes de desempeño recibidos todos los meses, hasta el quinto día hábil de cada mes. Trimestralmente es realizada una evaluación de cada proveedor, en donde es posible tomar algunas acciones, como en el caso del proveedor que no atiende algún requisito contractual, lo que resulta en la aplicación de multas.
- No existe ningún documento (políticas o procedimientos) que defina los niveles de servicio. Todo es tratado caso a caso. Las áreas de negocio cierran contratos de ANS con los clientes sin analizar la capacidad de atención de la organización, quedando está desprotegida, y generando mucho riesgo al negocio.
- La organización no tiene un contrato estándar de ANS, pues cada contrato tiene particularidades específicas. Existió la tentativa de elaborar un estándar, pero no fue posible terminarlo.
- Los contratos firmados por la organización con clientes no exigen el envío de informes. El sistema que la organización está instalando realizará todo el acompañamiento de ANS, con emisión de informes y acompañamiento *on-line* de las peticiones abiertas.
- Existen gestores de contratos, que son responsables por todo, inclusive por el ANS. Los gestores de contratos y los gerentes tienen acceso a los informes desempeño.
- La información sobre el ANS son divulgadas a los funcionarios del área de las TI, que rinden cuentas por los resultados.
- Anualmente el desempeño es evaluado y las metas son revisadas.
- La necesidad de cambios a los contratos es analizada caso a caso, inclusive con un análisis de impacto sobre los negocios de la organización, aunque de manera informal.

De acuerdo con esta información, responda:

- ¿Cuáles procesos de CobiT 4.1 fueron usados para realizar esta evaluación?
- ¿Cuáles aspectos fueron observados para incluir en esta evaluación?

### Actividad 3. Evaluación de seguridad de sistemas

En una organización, en la evaluación del proceso DS5 – Garantizar la seguridad de los sistemas fueron obtenidos los siguientes aspectos relevantes:

- No existe un comité organizacional responsable por patrocinar y promover la seguridad de la información.
- Las actividades para el inventario de software son realizadas, pero este proceso no es formalizado ni documentado.
- No existe un procedimiento para cambios y actualizaciones de software, pero estas actividades son ejecutadas rutinariamente.
- No existe un proceso para revisión de concesión de accesos.
- A pesar de existir la práctica de uso de los recursos de las TI, no existe un proceso o procedimiento aplicado al monitoreo de los funcionarios de la organización en relación con esta práctica.
- Son utilizadas tecnologías de criptografía, sin embargo sin prácticas organizacionales definidas.
- Son utilizadas tecnologías de gestión y de seguridad de redes (*firewall*, IDS) aunque sin procesos o procedimientos formales, que ocurren de modo no estandarizado.
- No existe la relación de clientes y proveedores que acceden a los recursos del sistema externamente. Son relacionados apenas los funcionarios externos que actúan dentro de las instalaciones de la organización.
- El control de acceso a sistemas y plataformas es descentralizado, no bloquea al usuario por tentativa de acceso no autorizado, pero si registra todas las tentativas infructuosas de acceso.
- No existe una práctica formal sobre el uso de y el mantenimiento de contraseñas por los usuarios.

Con base en esta información responda:

- En su opinión, ¿cuál es el nivel de madurez en que se encuentra este proceso? ¿Por qué considera este nivel de madurez?

- ¿Qué acciones deberían ser tomadas para elevar a 4 el nivel de madurez de este proceso?

## Actividad 4 (complementaria). Evaluación del desempeño de las TI

Lea el siguiente texto:

Muchos procesos de las TI están siendo conducidos informalmente, sin un modelo ni definición clara de las actividades y responsabilidades. En vista de esto, no fue observada una estructura capaz de brindar información para la elaboración de indicadores de desempeño de esos procesos. Sin embargo, existen acciones puntuales de algunas áreas, que están mejor estructuradas, en el sentido de hacer seguimiento a los indicadores. El área de infraestructura tiene excelentes controles, recolectando inclusive indicadores en tiempo real con énfasis en disponibilidad. El área de investigación de nuevas tecnologías también tiene mecanismos para hacer seguimiento a la satisfacción de sus clientes, así como el área de planeación y control, que analiza información de costos. Sin embargo, las demás áreas enfocan sus controles en proyectos, controlando principalmente el avance en términos de fechas y horas de personas asignadas, pero aun así de forma desestructurada y sin estándar.

Este es un análisis de evaluación del proceso "ME1 – Monitorear y evaluar el desempeño" de las TI de una organización.

Responda:

- En su opinión, ¿cuál es el nivel de madurez en que se encuentra este proceso? ¿Por qué considera este nivel de madurez?

- ¿Qué acciones deberían ser tomadas para elevar a 4 el nivel de madurez de este proceso?

## 8.5 Guía de Actividades 5

### Actividad 1 – Evaluación del nivel de madurez de procesos

Su organización pretende implementar el gobierno de las TI para soportar adecuadamente los procesos de negocio. El área de las TI de la organización decide definir un plan estratégico de tecnología de la información para subsidiar la implementación del gobierno de las TI. Para dar inicio a la planificación estratégica es necesario conocer el nivel de madurez de cada proceso de las TI. En reunión con el director de las TI, usted fue escogido para realizar la evaluación del nivel de madurez de los procesos del área y definir la prioridad para la implementación o actualización de cada proceso.

Con la herramienta presentada en esta sesión, ejecute la evaluación del nivel de madurez de los procesos de las TI de su organización, iniciando con diligenciar la guía REI (Tabla 92) y continuando con las demás guías. Elabore un informe para ser enviado al director de las TI que contemple las siguientes dimensiones:

Tabla 92. Guía REI: Relevancia, Estrategia, Impacto

| | Relevancia del proceso (A) | Contribución estratégica (B) | Impacto (C) | Resultados | | | |
|---|---|---|---|---|---|---|---|
| | | | | Total | A | B | C |
| **PO: Planificar y Organizar** | | | | | | | |
| PO: Planear y Organizar | Irrelevante | Ninguna contribución | Sin impacto | | 1 | 1 | 1 |
| PO1 – Definir un plan estratégico de TI | | | | | | | |
| PO2 – Definir la arquitectura de la información | | | | | | | |
| PO3 – Determinar las directrices de tecnología. | | | | | | | |
| PO4 – Definir los Procesos, la organización y las relaciones de TI. | | | | | | | |
| PO5 – Gestionar la inversión en TI. | | | | | | | |
| PO6 – Comunicar metas y directrices gerenciales. | | | | | | | |
| PO7 – Gestionar los recursos humanos de TI | | | | | | | |
| PO8 – Gestionar la calidad. | | | | | | | |
| PO9 – Evaluar y gestionar los riesgos de TI. | | | | | | | |

Continuación tabla 92. Guía REI: Relevancia, Estrategia, Impacto

| | Relevancia del proceso (A) | Contribución estratégica (B) | Impacto (C) | Resultados | | | |
|---|---|---|---|---|---|---|---|
| | | | | Total | A | B | C |
| PO10 – Gestionar proyectos. | | | | | | | |
| **AI - Adquirir e Implementar** | | | | | | | |
| AI1. Identificar soluciones automatizadas. | | | | | | | |
| AI2. Adquirir y mantener el software aplicativo. | | | | | | | |
| AI3. Adquirir y mantener la infraestructura tecnológica. | | | | | | | |
| AI4. Habilitar la operación y uso. | | | | | | | |
| AI5. Adquirir recursos de las TI | | | | | | | |
| AI6. Gestionar cambios. | | | | | | | |
| AI7. Instalar y homologar - soluciones y cambios. | | | | | | | |
| **Entregar y Soportar, DS** | | | | | | | |
| DS1. Definir y gestionar niveles de servicio. | | | | | | | |
| DS2. Gestionar servicios de terceros. | | | | | | | |
| DS3. Gestionar el desempeño y la capacidad. | | | | | | | |
| DS4. Asegurar la continuidad de los servicios. | | | | | | | |
| DS5. Garantizar la seguridad de los sistemas. | | | | | | | |
| DS6. Identificar y asignar costos | | | | | | | |
| DS7. Sensibilizar y entrenar a los usuarios. | | | | | | | |
| DS8. Gestionar el centro de servicios y los incidentes. | | | | | | | |
| DS9. Gestionar la configuración. | | | | | | | |
| DS10. Gestionar los problemas. | | | | | | | |
| DS11. Gestionar los datos. | | | | | | | |
| DS12. Gestionar el ambiente físico. | | | | | | | |
| DS13. Gestionar las operaciones. | | | | | | | |
| **Monitorear y Evaluar, ME** | | | | | | | |
| ME1. Monitorear y evaluar el desempeño de las TI. | | | | | | | |
| ME2. Monitorear y evaluar los controles internos. | | | | | | | |

Continuación tabla 92. Guía REI: Relevancia, Estrategia, Impacto

| | Relevancia del proceso (A) | Contribución estratégica (B) | Impacto (C) | Resultados | | | |
|---|---|---|---|---|---|---|---|
| | | | | Total | A | B | C |
| ME3. Asegurar la conformidad con requisitos externos. | | | | | | | |
| ME4. Proveer el gobierno de las TI. | | | | | | | |

| índices | | | | | |
|---|---|---|---|---|---|
| Relevancia del proceso | Índices | Contribución estratégica | Índices | Impacto | Índices |
| Irrelevante | 1 | Ninguna contribución | 1 | Sin impacto | 1 |
| Poca relevancia | 2 | Poco contribución | 2 | Algunos impactos | 2 |
| Relevante | 3 | Contribuye a la estrategia | 3 | Impacto | 3 |
| Muy relevante | 4 | contribución relevante | 4 | mucho impacto | 4 |
| Extremadamente relevante | 5 | Esencial para la estrategia | 5 | Impacto extremo | 5 |

1. Análisis crítico en el nivel de madurez evaluado de cada dominio de CobiT 4.1 a partir de los datos consolidados en la guía "Resumen" (Tabla 93)

Tabla 93. Guía resumen

| PO: Planificar y Organizar | |
|---|---|
| **Objetivos de control** | |
| Total Objetivos de control CobiT | 70* |
| **Modelo de madurez** | |
| Madurez del dominio | ** |
| **REI: Relevancia, Estrategia, Impacto** | |
| Promedio de puntuación | *** |

| AI - Adquirir e Implementar |
|---|
| **Objetivos de control** |
| Total Objetivos de control CobiT |
| **Modelo de madurez** |
| Madurez del dominio |
| **REI: Relevancia, Estrategia, Impacto** |
| Promedio de puntuación |

Continuación tabla 93. Guía resumen

| Entregar y Soportar, DS | | Monitorear y Evaluar, ME |
|---|---|---|
| **Objetivos de control** | | **Objetivos de control** |
| Total Objetivos de control CobiT | | Total Objetivos de control CobiT |
| **Modelo de madurez** | | **Modelo de madurez** |
| Madurez del dominio | | Madurez del dominio |
| **REI: Relevancia, Estrategia, Impacto** | | **REI: Relevancia, Estrategia, Impacto** |
| Promedio de puntuación | | Promedio de puntuación |

* 70: corresponde al total de objetivos de control que se calculan en la tabla 74.
** Corresponde al promedio de la madurez evaluada por cada dominio en la tabla 74
*** Corresponde al promedio de la REI evaluado en la tabla 92 - Guía REI

2. Con base en la guía "Análisis de prioridades", defina los procesos que serán priorizados en la implantación del gobierno de las TI.

Tabla 94. Guía. Análisis de prioridades

| Análisis de prioridades | | | |
|---|---|---|---|
| **ID** | **Proceso** | **REI** | **GAP** |
| **PO: Planificar y Organizar** | | | |
| PO1 | Definir un plan estratégico de TI | * | ** |
| PO2 | Definir la arquitectura de la información | | |
| PO3 | Determinar las directrices de tecnología. | | |
| PO4 | Definir los Procesos, la organización y las relaciones de TI. | | |
| PO5 | Gestionar la inversión en TI. | | |
| PO6 | Comunicar metas y directrices gerenciales. | | |
| PO7 | Gestionar los recursos humanos de TI | | |
| PO8 | Gestionar la calidad. | | |
| PO9 | Evaluar y gestionar los riesgos de TI. | | |
| PO10 | Gestionar proyectos. | | |
| **AI - Adquirir e Implementar** | | | |
| AI1 | Identificar soluciones automatizadas. | | |

Continuación tabla 94. Guía. Análisis de prioridades

| | | | |
|---|---|---|---|
| AI2 | Adquirir y mantener el software aplicativo. | | |
| AI3 | Adquirir y mantener la infraestructura tecnológica. | | |
| AI4 | Habilitar la operación y uso. | | |
| AI5 | Adquirir recursos de las TI | | |
| AI6 | Gestionar cambios. | | |
| AI7 | Instalar y homologar - soluciones y cambios. | | |
| **Entregar y Soportar, DS** | | | |
| DS1 | Definir y gestionar niveles de servicio. | | |
| DS2 | Gestionar servicios de terceros. | | |
| DS3 | Gestionar el desempeño y la capacidad. | | |
| DS4 | Asegurar la continuidad de los servicios. | | |
| DS5 | Garantizar la seguridad de los sistemas. | | |
| DS6 | Identificar y asignar costos | | |
| DS7 | Sensibilizar y entrenar a los usuarios. | | |
| DS8 | Gestionar el centro de servicios y los incidentes. | | |
| DS9 | Gestionar la configuración. | | |
| DS10 | Gestionar los problemas. | | |
| DS11 | Gestionar los datos. | | |
| DS12 | Gestionar el ambiente físico. | | |
| DS13 | Gestionar las operaciones. | | |
| **Monitorear y Evaluar, ME** | | | |
| ME1 | Monitorear y evaluar el desempeño de las TI. | | |
| ME2 | Monitorear y evaluar los controles internos. | | |
| ME3 | Asegurar la conformidad con requisitos externos. | | |
| ME4 | Proveer el gobierno de las TI. | | |

* Corresponde al resultado TOTAL obtenido en la tabla 92
** Corresponde a la resta entre la meta deseada para el proceso menos la madurez evaluada, obtenidos en la tabla 75

3. Qué estrategia de implementación del gobierno de las TI debe ser adoptada.

## 8.6 Guía de Actividades 6

### Actividad 1. Alineamiento entre COSO y CobiT 4.1

Relacione el proceso de CobiT 4.1 "PO1 – Definir un plan estratégico de las TI" con los elementos de COSO, haciendo un enfoque sobre estos componentes. Utilice la "Tabla 77. Procesos de CobiT 4.1 y del COSO. H = alta, M = media, L = baja, X = asociación CobiT – COSO", para apoyar la actividad.

### Actividad 2. Aplicación de la norma ISO 38500

Con la información sobre la norma ISO 38500, establezca un plan para aplicarla en su organización.

### Actividad 3. Aplicación del modelo Val IT

Con la información sobre el modelo Val IT, establezca un plan para definir un portafolio de inversiones en TI en su organización.

## 8.7 Guía de actividades 7

### Actividad 1. Comparativo entre CobiT 5 y CobiT 4.1

En una tabla relacione cada uno de los procesos de CobiT 5 y al frente ubique los procesos de CobiT 4.1 que considere son desarrollados en el proceso de CobiT 5 en cuestión.

Tabla 95. Ejercicio comparación entre CobiT 5 y CobiT 4.1

| CobiT 5 | CobiT 4.1 |
|---|---|
| | |
| | |
| | |

## Actividad 2. Aplicación del modelo de capacidad de CobiT 5

Tomando como ejemplo la tabla siguiente aplique el modelo de capacidad para cada uno de los 37 procesos de CobiT 5 a la organización a la cual usted pertenece, de manera similar al llevado a cabo en la Actividad 1 de la Guía de Actividades 5. Obtenga sus propias conclusiones.

Tabla 96. Ejercicio aplicación del modelo de capacidades de CobiT 5

| Modelo CobiT 5 Proceso | Nivel Actual | | | | | | EXPLICACIÓN |
|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | |
| EDMo1 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno | | | | | | | |
| EDMo2 Asegurar la entrega de beneficios | | | | | | | |
| EDMo3 Asegurar la optimización del riesgo | | | | | | | |

# Bibliografía

CobiT Mapping: Mapping of ITIL v3 with CobiT 4.1: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/ Pages/COBIT-Mapping-Mapping-of-ITIL-V3-With-COBIT-4-1.aspx

IT Governance Institute®: www.itgi.org

ISACA: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-spanish.pdf

FERNANDES, A. A; ABREU, V. F. Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços. Rio de Janeiro: Brasport, 2006.

Modelo Cobit 4.1.

NTC-ISO/IEC 38500: 2008. Norma Técnica colombiana de Gobierno corporativo de la tecnología de la información

WEILL, Peter; ROSS, Jeanne W. Governança de Tecnologia da Informação. São Paulo: M. Books, 2006.

Val IT and Related: http://www.isaca.org/bookstore/Pages/Val-IT-and-Related.aspx

Val IT Framework 2.0:http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/ Pages/Val-IT-Framework

CobiT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la organización, ISACA 2012.

CobiT 5: Procesos facilitadores, ISACA 2012.

CobiT 5: Implementación, ISACA 2012.

## Lista de figuras

## Lista de tablas

# Planeación y Gestión Estratégica de las TI

## Versión ESR-Colombia
## Escuela Superior de Redes, ESR - Colombia

Se publicó en el mes de julio de 2014,
Publicado por RENATA,
Universidad Nacional de Colombia,
Facultad de Ingeniería
Bogotá D. C., Colombia.
En su diagramación se utilizaron caracteres DaxlinePro

Esta versión está adaptada para Ecuador gracias a CEDIA.

www.cedia.org.ec

# GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

renata Colombia

redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Calle La Condamine 12-109 "Casa Rivera"
Teléfono (+593) 7 405 1000 Ext. 4220
info@cedia.org.ec • Cuenca - Ecuador
/FundacionCEDIA @FundacionCEDIA