

# Boletín de Asesoría Gerencial\*

Aplicabilidad de estándares internacionales y mejores prácticas:  
CobIT®, ITIL®, Serie ISO / IEC 27000

No. 3 - 2009

Contenido Cerrar Imprimir Página anterior Página siguiente



*ESPIÑEIRA, SHELDON Y ASOCIADOS*

Firma miembro de

*PRICEWATERHOUSECOOPERS* 

# Contenido

Haga click en los enlaces para navegar a través del documento



Haga click en los enlaces para llegar directamente a cada sección

▶ [Introducción](#)

---

▶ [Conceptos](#)

---

▶ [Las mejores prácticas y la Organización](#)

---

▶ [Importancia de las mejores prácticas en el Gobierno de TI](#)

---

▶ [Algunos estándares y mejores prácticas](#)

---

▶ [Alineando ISO 27001:2005 e ITIL® con CobiT®](#)

---

▶ [Conclusión](#)

---

▶ [Créditos / Suscribirse](#)

---

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT®, ITIL®, Serie ISO / IEC 27000

### Introducción

El Gobierno de TI es parte integral del éxito de la gestión empresarial, al asegurar mejoras en la eficiencia y efectividad de los procesos relacionados. El Gobierno de TI provee las estructuras que unen los procesos y los recursos de TI con las estrategias y los objetivos de la organización tomando como base el marco de procesos CobiT®, las mejores prácticas de ITIL® y los estándares en materia de seguridad de información que ofrece la Serie ISO/IEC 27000. En la Figura N° 1 se observa marco de estándares y referencias internacionales que apoyan la gestión de TI en pro de dirigir y controlar a la empresa con el fin que ésta pueda cumplir sus metas.



Para visualizar la Figura No. 1 haga click en el icono.

Figura N°1 Marco de estándares y referencias internacionales relacionadas con Gobernabilidad de TI

Las organizaciones deben delimitar las áreas a optimizar, y en ellas, identificar los procesos de TI que son críticos para administrar adecuadamente los diferentes riesgos y analizar la capacidad actual de prestación de servicios de TI respecto a las necesidades del negocio, usando como base el marco de Procesos de CobiT, en ITIL® para el apoyo en la definición de procesos de entrega de servicios críticos y en el estándar ISO 27001 para los objetivos de seguridad. Ver Figura N° 2

Para ampliar: haga click sobre la imagen

Retorno

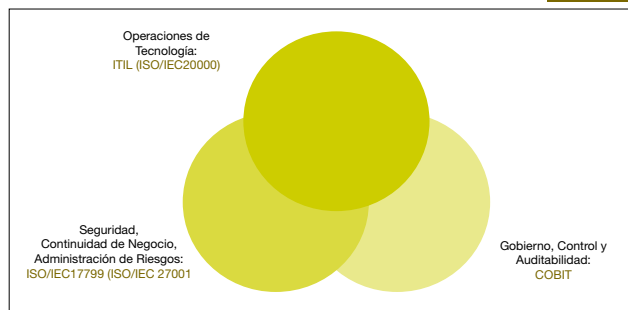


Figura N° 2. Marco de procesos de CobiT

### Conceptos

#### Las mejores prácticas y la Organización

Las mejores prácticas son directrices que permiten a las empresas modelar sus procesos en la procura de un ajuste a sus necesidades y una adopción de esquemas que han demostrado ser eficientes en otras organizaciones, proporcionando métodos estándares y administrar de una mejor manera los entornos de TI.

Los beneficios de implementar mejores prácticas de seguridad son:

- Incrementar la productividad y la eficiencia
- Incrementar la rentabilidad
- Incrementar la concientización del empleado
- Mitigar riesgos innecesarios de activos
- Incrementar la confianza del cliente
- Asegurar el cumplimiento de regulaciones
- Reducción de la dependencia en el “experto”

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT<sup>®</sup>, ITIL<sup>®</sup>, Serie ISO / IEC 27000

### Conceptos (continuación)

#### Importancia de las mejores prácticas en el Gobierno de TI

El uso de mejores prácticas permite a las organizaciones mantener un gobierno efectivo de las actividades de TI, además permiten crear un marco de gestión el cual es necesario para que cada parte de la organización esté en conocimiento de como hacer sus actividades mediante el uso de políticas, control interno y prácticas definidas. Por ejemplo, CobiT<sup>®</sup>, ITIL<sup>®</sup> e ISO 27001 son marcos de trabajos basados en la administración de los recursos de TI y proporcionan:

- Orientación de estrategias
- Valor en la entrega de servicios
- Administración de riesgos
- Administración de recursos
- Medición de desempeño

#### Algunos estándares y mejores prácticas

ITIL<sup>®</sup> : Las siglas ITIL significan: Information Technology Infrastructure Library lo que podría traducirse como biblioteca de infraestructuras de tecnologías de la información. ITIL es un modelo para gestionar servicios de TI, desarrollado a finales de los años 80 por la administración del Reino Unido. En la Figura N° 3 se puede observar la evolución de ITIL hasta su versión actual.

Es un conjunto de procesos que se enmarcan en la provisión, entrega y gestión de servicios a una organización, con sus infraestructuras y actividades correspondientes. En su más reciente versión, ITIL V3, presenta el concepto de gestión del ciclo de vida del servicio. Con este enfoque, se abarca la gestión del servicio desde la solicitud hasta la liberación del servicio.



Para visualizar la Figura No. 3 haga click en el icono.

Figura N° 3: Evolución ITIL

Esta versión contempla cinco ciclos de vida para los servicios de TI:

**Estrategias:** El alcance del ciclo de vida de la Estrategia del Servicio considera aspectos de cultura y procesos de negocio, cultura y procesos de TI, entendiendo al cliente, cambios futuros en requerimientos, entendiendo a la competencia y sus diferencias y entendiendo el valor.

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT®, ITIL®, Serie ISO / IEC 27000



### Conceptos (continuación)

**Diseño:** Existen cinco aspectos individuales del Diseño del Servicio que son considerados en este ciclo de vida, siendo estos los servicios nuevos o modificados, sistemas y herramientas de gestión de servicios, portafolio, arquitecturas de tecnología y sistemas de gestión, los procesos requeridos y las métricas y métodos de medición.

**Transición:** El alcance de la Transición del Servicio incluye la gestión y coordinación de los procesos, sistemas y funciones a empaquetar, construir, probar e implementar un desarrollo en producción y establecer el servicio especificado.

**Operaciones:** Es el responsable por todas las actividades requeridas para soportar y ofrecer los servicios. Esto incluye a los servicios como tal, el proceso de gestión de los servicios, la tecnología y la misma gente.

**Mejora continua:** La mejora continua del negocio abarca la salud general de la administración de servicios de TI como una disciplina, la alineación continua del portafolio de servicios de TI con las necesidades actuales y futuras del negocio así como la madurez de los procesos de TI por cada servicio en un modelo de ciclo de vida de servicio continuo.

El ciclo de vida del servicio de ITIL V3 puede ser observado en la Figura N°4.



Para visualizar la Figura No. 4 haga click en el icono.

Figura N° 4: Ciclo de Vida del Servicio de ITIL

### CobIT®:

CobIT® es un conjunto de mejores prácticas para la gestión de Tecnología de Información creada por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA – Information Systems Audit and Control Association) y el Instituto de Gobernabilidad de la Tecnología de Información (ITGI – IT Governance Institute) con el fin de proveer a Gerentes, Auditores y usuarios de TI un grupo de objetivos, controles, procesos e indicadores que apoyen en la maximización de beneficios derivados del uso de la Tecnología de Información y el apropiado control y Gobernabilidad de TI

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT®, ITIL®, Serie ISO / IEC 27000

### Conceptos (continuación)

Presentado en 1996, CobiT es una herramienta para la gobernabilidad de TI que ha sentado bases importantes sobre los conceptos de control

y gestión en las operaciones de TI, el cual ha evolucionado de una herramienta de auditoría a un marco de Gobernabilidad de TI, atendiendo a las demandas actuales. Ver figura N° 5.,

CobiT establece un marco de referencia que permite definir metas desde el punto de vista de seguridad y control que serán de utilidad a la organización para establecer un plan de acción y lograr mejoras, y posteriormente identificar los lineamientos para sustentar un proceso de monitoreo y mejora continua sobre las soluciones implementadas.

En la Figura N° 6 se puede observar la estructura de cubo de CobiT, donde se muestra su capacidad para enfocar sus objetivos de control desde tres puntos de vista diferentes: los procesos, los recursos de TI y las características que debe reunir la información para ser considerada adecuada a las necesidades de la organización.

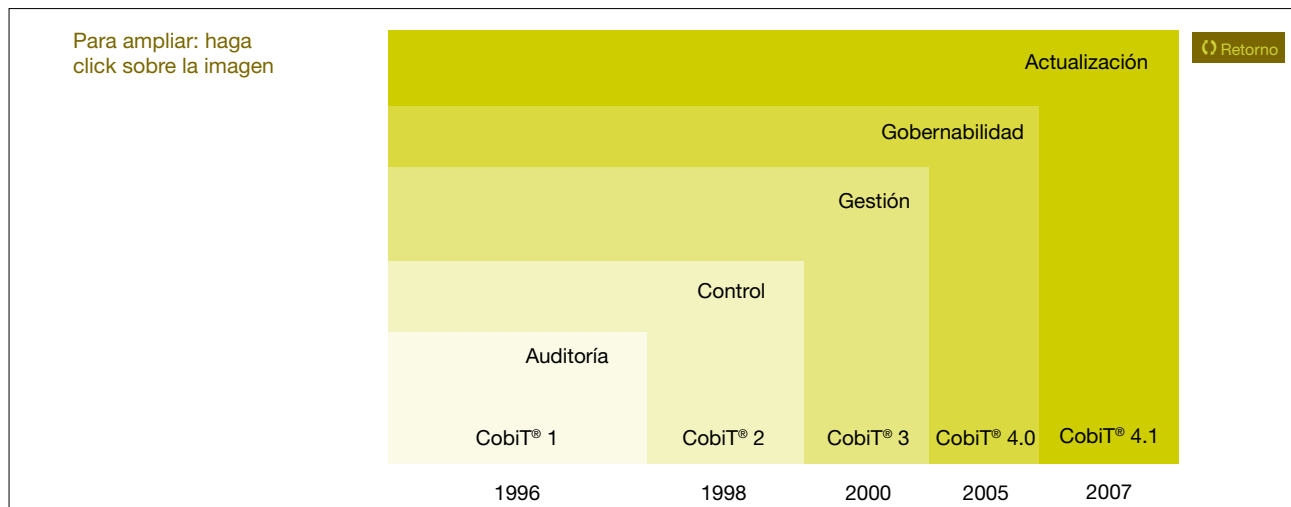


Figura N° 5: Evolución de COBIT

 Para visualizar la Figura No. 6 haga click en el icono.

Figura N° 6: Componentes tres vistas de CobiT

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT®, ITIL®, Serie ISO / IEC 27000

### Conceptos (continuación)

Esta estructura permite vincular las expectativas de la Dirección con las de la Gerencia de TI, manejando lineamientos comprensibles por las Gerencias de negocio y los dueños de los procesos.

CobiT permite agrupar los objetivos de control en distintas áreas de actividad de la organización. Los cuatro dominios principales son: Planificación y organización, Adquisición e implantación, Soporte y servicios, y Monitoreo.

Como su nombre indica, cada uno de estos dominios se dividen en procesos que están enfocados a los diferentes niveles y departamentos que pueden existir en una organización:

#### Planeación y Organización

- Definir plan estratégico de TI
- Definir arquitectura de información

- Determinar la dirección tecnológica
- Definir la organización de las relaciones de TI
- Manejar la inversión en TI
- Comunicar la dirección y aspiraciones de la gerencia
- Administrar recurso humano
- Asegurar el cumplimiento de requerimientos externos
- Evaluar riesgos
- Administrar proyectos
- Administrar calidad

#### Adquisición e implementación

- Identificar Soluciones
- Adquirir y mantener software de aplicación
- Adquirir y mantener arquitectura de tecnología
- Desarrollar y mantener procedimientos relacionados con TI
- Instalar y acreditar sistemas
- Administrar cambios

#### Entrega y soporte

- Definir Nivel de Servicio
- Administrar servicios prestados por terceros
- Administrar desempeño y capacidad
- Asegurar servicio continuo
- Garantizar seguridad de sistemas
- Identificar y asignar costos
- Educar y formar a los usuarios
- Apoyar y asistir a los clientes de TI
- Administrar la configuración
- Administrar problemas e incidentes
- Administrar datos
- Administrar instalaciones
- Administrar operaciones

#### Monitoreo

- Monitorear los procesos
- Evaluar lo adecuado del control interno
- Obtener aseguramiento independiente
- Proporcionar auditoría independiente

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT®, ITIL®, Serie ISO / IEC 27000

### Conceptos (continuación)

#### Serie ISO/IEC 27000

ISO/ IEC 27000 se define como el conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco para la gestión de la seguridad de la información en las organizaciones. La serie contiene las mejores prácticas recomendadas para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información. (Ver Figura No. 7)



Para visualizar la Figura No. 7 haga click en el icono.

Figura N° 7. Definición de estándares ISO 27000

ISO 27001 siendo el estándar principal de la serie, publicado en Octubre de 2005 y especifica los requisitos para la implantación de un Sistema de Gestión de la Seguridad de la Información, siguiendo los principios de calidad continua propuestos en el PDCA -acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Ver Figura N° 7. Es consistente con las mejores prácticas descritas en ISO/IEC 27002 y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002 de 2002.

Para ampliar: haga click sobre la imagen

Retorno

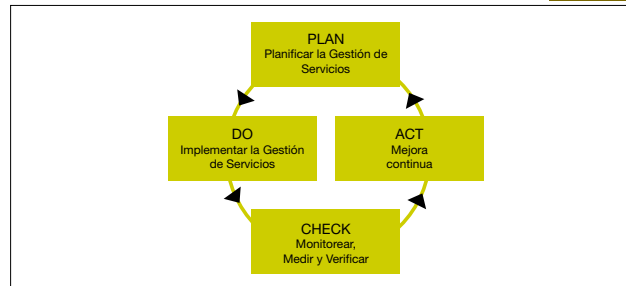


Figura N° 8: Ciclo PDCA

El ISO 27001:2005, al definirse como una guía en la implementación, operación, monitoreo, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI) para cualquier tipo de organización, mientras que ISO 27002 representa la guía de buenas prácticas que describe los objetivos de control y controles óptimos en el marco de la Seguridad de la Información, en conjunto se orientan a preservar los siguientes principios de la seguridad informática:

**Confidencialidad.** Asegurar que únicamente personal autorizado tenga acceso a la información. **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

**Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT<sup>®</sup>, ITIL<sup>®</sup>, Serie ISO / IEC 27000



### Conceptos (continuación)

El primer paso es definir el ámbito de aplicación de la política del SGSI. Este paso es crítico para identificar los peligros potenciales a los que se enfrenta y decidir una metodología sistemática para evaluar esos riesgos. Un SGSI apropiado incluye los pasos de implantación, puesta en funcionamiento, revisión, mantenimiento y mejora del sistema y que están descritos en el estándar.

La certificación del estándar internacional ISO 27001:2005 incrementa el prestigio de una organización, considerando que la norma indica la obligación general de mantener, monitorear, revisar y mejorar la seguridad de la información lo que demuestra la validez de ésta, creando nuevas oportunidades de negocio con partes conscientes de la importancia de la seguridad y la ética. Asimismo, permite reducir el posible riesgo de fraude, pérdida de información y revelación.

Cada una de las áreas de la normativa establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

### Alineando ISO 27001:2005 e ITIL con CobiT

Las organizaciones de TI, apoyadas en estándares y mejores prácticas, deben estar orientadas a satisfacer las necesidades del negocio, en la Figura N° 9, se observa esquemáticamente como las estrategias de las organizaciones y la directriz de TI deben estar alineadas, considerando que los procesos internos contemplan como base los estándares y mejores prácticas de TI.



Para visualizar la Figura No. 9 haga click en el icono.

Figura N° 9: Alineación del negocio con los estándares y mejores prácticas.

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT<sup>®</sup>, ITIL<sup>®</sup>, Serie ISO / IEC 27000



### Alineando ISO 27001:2005 e ITIL con CobiT (Continuación)

Para llevar a cabo la implantación de las mejores prácticas de seguridad en su empresa se debe tomar en cuenta las siguientes etapas:

#### Análisis:

- Seleccionar el marco o marcos de referencia, según las funciones a optimizar
- Realizar evaluaciones en:
  - Controles en la plataforma tecnológica y aplicaciones
  - Nivel de concientización de los usuarios
  - Servicios de outsourcing y contratos con terceros
  - Controles físicos en las instalaciones
  - Nivel de documentación existente (políticas y procedimientos)

#### Herramientas:

- Self Assessment
- Evaluación por terceros

#### Planificación:

- Obtener una comparación del programa de seguridad de la organización contra el estándar seleccionado o contra referencias en el mercado
- Preparar la declaración de aplicabilidad del estándar

#### Herramientas:

- Benchmarking
- Gap Analysis

#### Diseño e implantación:

- Seleccionar los objetivos de control y controles a ser implantados
- Establecer un plan de acción para implantar los controles seleccionados
- Desarrollar la documentación (excepciones y controles aplicables)
- Evaluar hasta donde se quiere llegar (un cumplimiento total, parcial, etc.)

#### Medición:

- Establecer métricas e indicadores (Ej. KPI's, KGI's)
- Considerar los cambios de tecnología, de procesos y de estructura organizacional
- Definir y aplicar revisiones periódicas del cumplimiento del estándar seleccionado

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT<sup>®</sup>, ITIL<sup>®</sup>, Serie ISO / IEC 27000



### Conclusión

La aplicación de mejores prácticas de TI, así como el uso de estándares internacionales, permite que las organizaciones puedan incrementar sus niveles de confianza en la obtención de un marco de operatividad de servicios, estable y continuo.

La eficacia de la aplicación de normas y mejores prácticas depende de cómo han sido implementadas y sustentadas, tomando en cuenta que son el punto de partida para adaptar procedimientos específicos de la gestión de TI. CobiT y los estándares de la serie ISO/IEC 27000 representan herramientas básicas que permiten a las organizaciones de TI definir que estrategias deben seguir para garantizar la satisfacción de las necesidades del negocio, en tanto que ITIL proporciona un marco referencial sobre la eficiencia y calidad de la gestión de los servicios de TI a la organización.

Sin embargo, es fundamental que su adopción esté alineado a los requerimientos del negocio y se adapten, sin alterar sus fundamentos, a los requerimientos de la organización. El crecimiento en la adopción de los referidos estándares, debe ser orquestados en la atención de las exigencias según su prioridad y manteniendo los principios de calidad de sus procesos, y debe mantener consistencia con las iniciativas de gobernabilidad y gestión de riesgos.

# Boletín de Asesoría Gerencial

## Aplicabilidad de estándares internacionales y mejores prácticas: CobiT<sup>®</sup>, ITIL<sup>®</sup>, Serie ISO / IEC 27000

Si desea suscribirse haga click en la barra

El Boletín Asesoría Gerencial es publicado por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. \*connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados  
Depósito Legal pp 1999-03CS141  
Teléfono master: (58-212) 700 6666



© 2009 . Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3

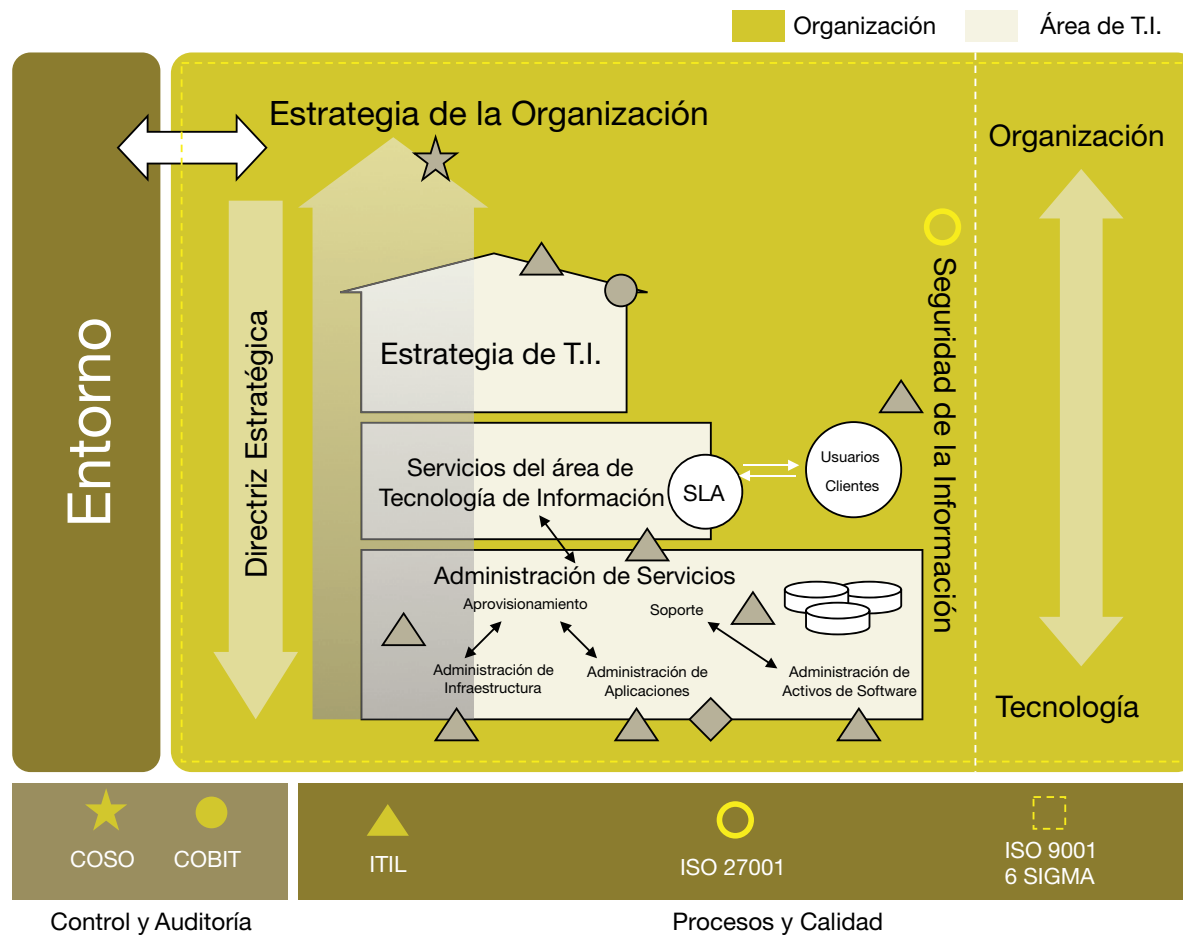
## Figura N° 7. Definición de estándares ISO 27000

Regresar al boletín    Aumentar    Imprimir



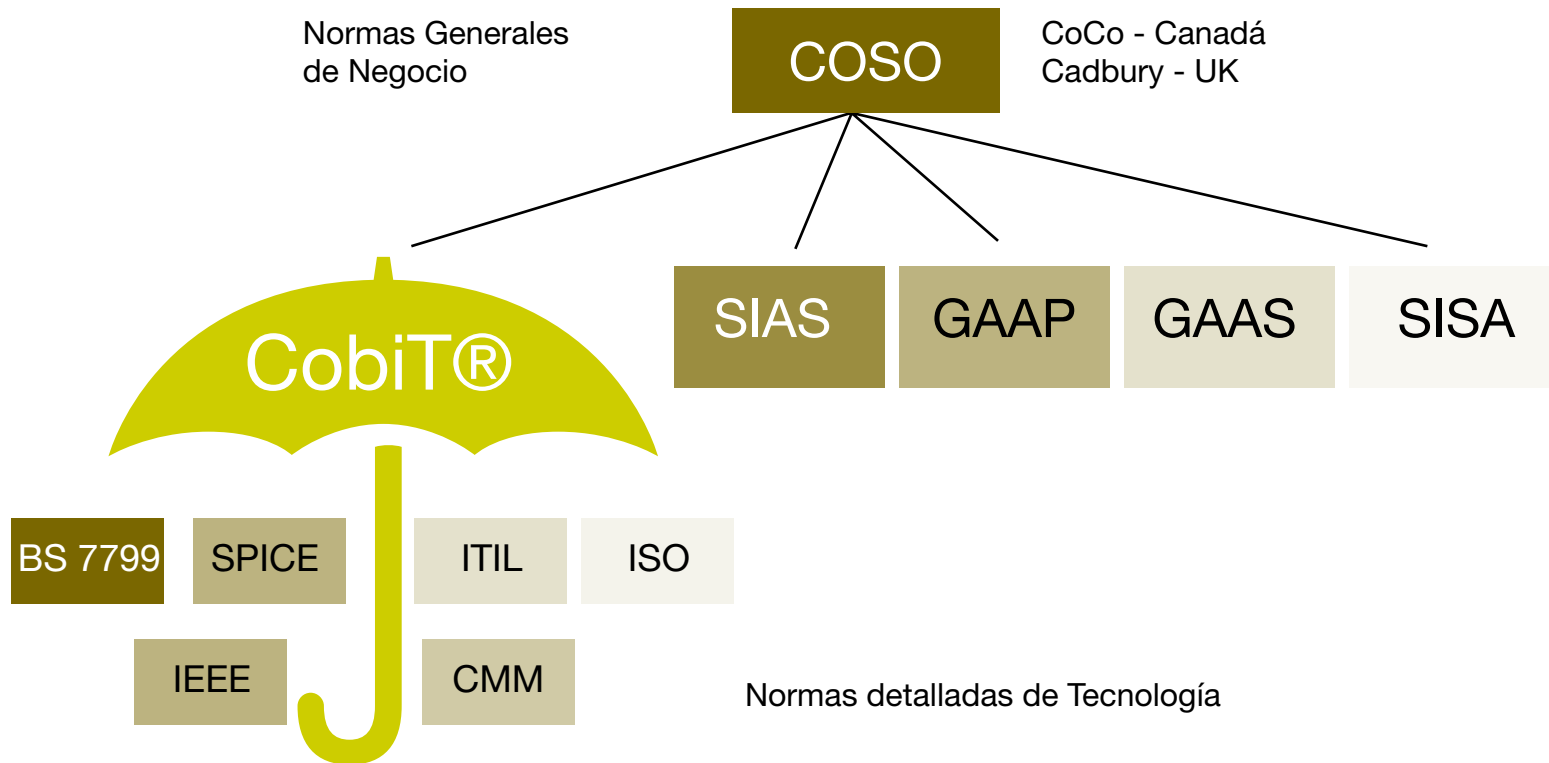
| Objetivo de control | Descripción   |
|---------------------|---|
| ISO/IEC 27001       | Estándar principal de la serie, que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) (Publicación: Oct 2005)             |
| ISO/IEC 27002       | Anteriormente ISO/IEC 17799, representa el código de buenas prácticas para la Gestión de Seguridad de la Información (Publicación: Julio 2007)                                      |
| ISO/IEC 27003       | Directrices para la implementación de un sistema de Gestión de Seguridad de la Información. Es el soporte de la norma ISO/IEC 27001 (Aún no ha sido publicada)                      |
| ISO/IEC 27004       | Métricas para le gestión de la Seguridad de la Información (Aún no ha sido publicada)   |
| ISO/IEC 27005       | Gestión de Riesgos de la Seguridad de la Información. Proporciona lineamientos para la evaluación de riesgos de Seguridad de la Información (Publicación: Junio de 2008)            |
| ISO/IEC 27006       | Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los Sistemas de Gestión de la Seguridad de la Información (Publicación: Febrero de 2007) |

# Figura N° 9: Alineación del negocio con los estándares y mejores prácticas.



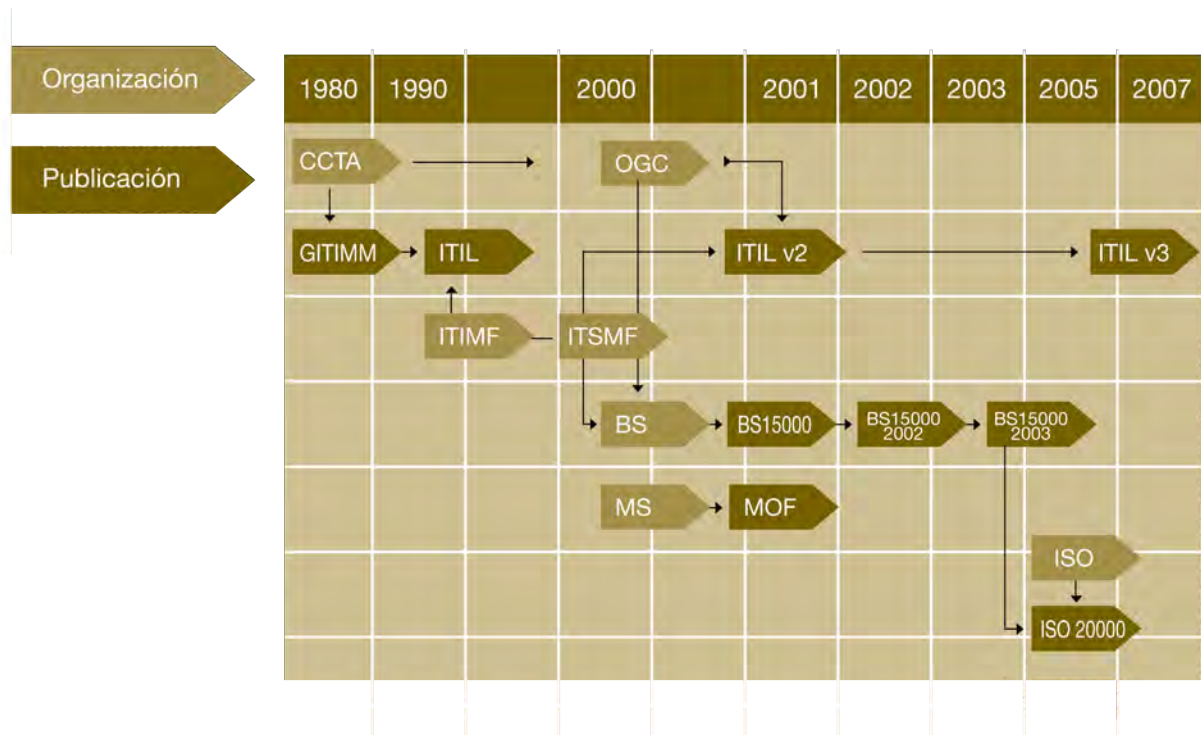
# Figura N°1: Marco de estándares y referencias internacionales relacionadas con Gobernabilidad de TI

Regresar al boletín    Aumentar    Imprimir



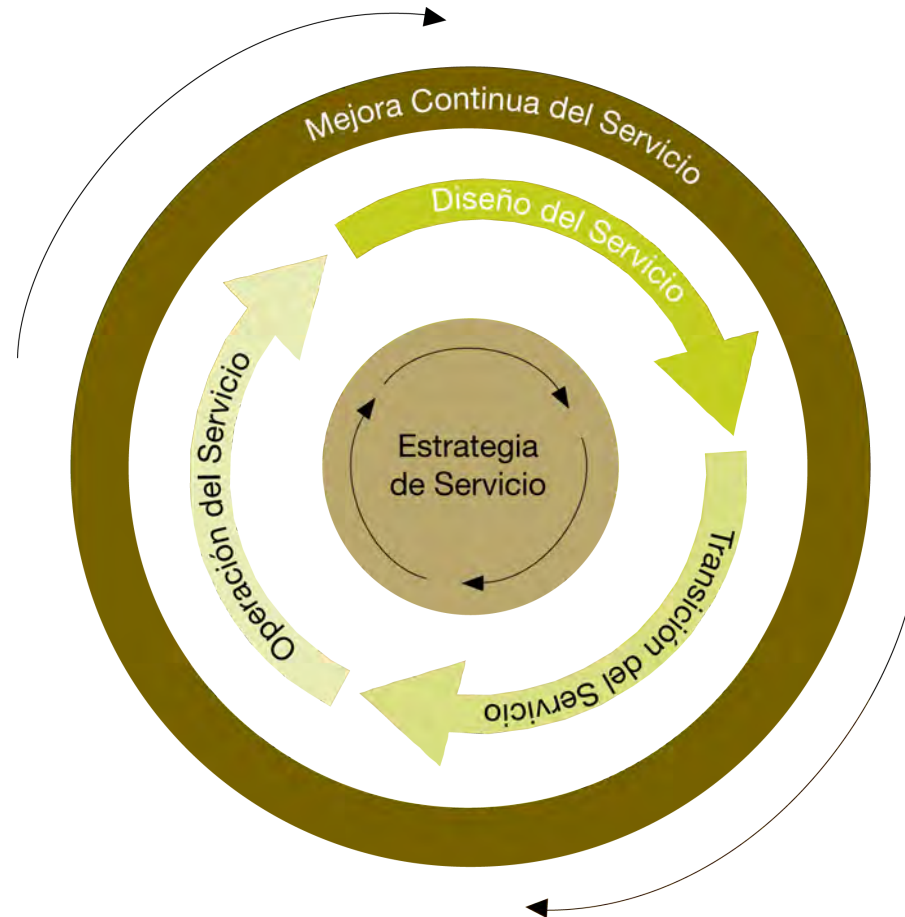
# Figura N° 3: Evolución ITIL

Regresar al boletín Aumentar Imprimir



# Figura N° 4: Ciclo de Vida del Servicio de ITIL

Regresar al boletín    Aumentar    Imprimir



# Figura N° 6: Componentes tres vistas de CobIT

Regresar al boletín    Aumentar    Imprimir

