



# Comunicación

# 333

## **CÓMO CONSTRUIR UN SISTEMA DE GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (SGTI)**

**Manuel Narbona Sarria**

Gabinete de Sistema

Servicio de Producción

Dirección General de Sistemas de Información Económico-Financiera

Consejería de Economía y Hacienda

Junta de Andalucía

---

## Palabras clave

*Sistema, gestión, tecnologías de la información.*

## Resumen de su Comunicación

*¿Se pueden gestionar las Tecnologías de la Información (TI) de modo que ofrezcan suficientes garantías para los ciudadanos que se hacen uso de ellas en sus trámites con la Administración a través de las oficinas virtuales?.*

*Afortunadamente en los últimos años han surgido y madurado estándares, metodologías y buenas prácticas que hacen posible la gestión de las TI, aunque quizá debido a la proliferación de las metodologías no parece claro por dónde empezar:*

*Este documento es una propuesta para la construcción de un Sistema de Gestión de las Tecnologías de la Información (SGTI) que vaya más allá de particularidades de aplicación de cada metodología, estándar o buenas prácticas, pero que se apoye en ellas en los ámbitos donde pueden ser útiles.*

---

## CÓMO CONSTRUIR UN SISTEMA DE GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (SGTI)

### 1. Introducción

Cuando cruzamos un puente no somos consciente de los aspectos de gestión que fueron necesario para su construcción. Lo más que vemos es su aspecto estético. Sin embargo, para la construcción de un puente es necesario realizar un análisis de viabilidad, un análisis de la solución adoptada, un diseño, construirlo, probarlo, y finalmente, usarlo. Hasta aquí nada nuevo respecto a lo que hacemos con el desarrollo del software: las etapas son las mismas. Por otra parte, en paralelo a estas etapas hay que buscar los recursos humanos y materiales, hay realizar el plan de construcción, hay que disponer de financiación, hay que realizar planes de emergencia, contratar seguros, etc. Estos aspectos se corresponden con la gestión de proyectos, que también conocemos en la ingeniería del software.

Pero la ingeniería del software no es el único aspecto de las tecnologías de la información que tenemos que gestionar: Aspectos como la calidad, la seguridad de la información, los planes de contingencias, los recursos humanos, la conformidad con la legislación, etc., forman también parte del ámbito de las TI.

Además, cuando cruzamos un puente, a parte de su aspecto estético confiamos en que sea sólido y no se vaya a hundir bajo nuestros pies: confiamos que se han realizado las pruebas necesarias, que los inspectores han analizado el proceso de construcción y han sugerido las mejoras oportunas, etc.

Desde el punto de vista de las TI, cuando un ciudadano se acerca a nuestras oficinas virtuales confía en que no sólo la fachada sea adecuada, usable, etc., sino que espera que lo que hay detrás de la fachada, y que el no ve, no sea como las casas de los escenarios de las películas del oeste: fachadas sujetas por cuatro palos.

En los últimos años se han ido consolidando estándares, metodologías y buenas prácticas<sup>1</sup> para la gestión TI. Vamos a tratar de centrar la cuestión y ver cómo podemos hacer uso de estas metodologías para gestionar nuestras organizaciones TI.

### 2. Estándares, metodologías y buenas prácticas

Lo que sigue es una relación, no exhaustiva, de algunas de las metodologías propuestas para diversos aspectos de las TI. No todas ellas son exclusivas de las TI.

---

<sup>1</sup>En adelante agruparemos bajo el termino metodologías a los estándares, metodologías y buenas prácticas

| Metodología                                    | Ámbito   | Observaciones  |
|--|--|--|
| IT BSC   | Planificación estratégica.<br>Cuadro de Mando Integral para las TI | Es una implementación para las TI de la metodología Balanced Scorecard de Kaplan y Norton  |
| ISO 9000 - EFQM                                | Calidad  | No son exclusivas de la TI   |
| COBIT  | Gobierno TI  | El Gobierno TI es el sistema por el cual se dirigen y controlan las TI en la organización. La estructura del Gobierno TI especifica la distribución de derechos y responsabilidades de los diferentes participantes tales como directivos, gestores TI y de negocio, e indica las reglas y procedimientos para la toma de decisiones sobre las TI. Esto también provee la estructura a través de la cual los objetivos TI son fijados, y el medio de lograr esos objetivos y monitorizar su ejecución. |
| ITIL - ISO/IEC 20000                           | Gestión de Servicios TI  | ITIL tiene un ámbito más amplio pero el que se ha desarrollado y se aplica en profundidad es el de la Gestión de Servicios TI La norma ISO/IEC 20000 define el sistema de gestión de servicios TI  |
| PRINCE2  | Gestión de proyectos   | PRINCE2 no es exclusivo de las TI.   |
| CMMi   | Desarrollo de Aplicaciones   | El modelo de madurez de la Carnegie Mellon University como metodología para asegurar la calidad en el desarrollo de aplicaciones   |
| ISO/IEC 17799 -<br>ISO/IEC 27001 -<br>MAGERIT2 | Seguridad de la Información  | La ISO/IEC 27001 es equivalente a la española UNE 71502, a la que pronto sustituirá. Define el SGSI <sup>2</sup>   |
| SARBANE OXLEY                                  | Conformidad Financiera   | Esta norma obliga a las empresas financieras de EEUU a demostrar objetivamente responsabilidad social, integridad y ética en la administración de las organizaciones, especialmente financieras y bursátiles, pero está siendo aplicada a cualquier empresa que tenga presencia en el mercado. Está siendo adaptada en otros países  |

Tabla 1 - Metodologías para la Gestión TI

### 3. ¿Qué hay que gestionar?. El ámbito TI: COBIT

Lo primero que es preciso conocer es el ámbito de las TI. No podemos hacer una buena gestión si desconocemos qué tenemos que gestionar.

<sup>2</sup>SGSI: Sistema de Gestión de la Seguridad de la Información

De las metodologías mencionadas sólo una plantea una visión global de las TI: COBIT. El Marco de Referencia COBIT define 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios: Planificación y organización, Adquisición e Implementación, Entrega y Soporte del Servicio y Monitorización y Evaluación. Esta estructura cubre todos los aspectos de la información y de la tecnología que la soporta.

Administrando adecuadamente estos 34 Objetivos de Control de alto nivel, el propietario de los procesos del negocio podrá asegurar que se proporciona un sistema de control adecuado en el ámbito de las tecnologías de la información.

COBIT provee una guía o lista de verificación para el gobierno de TI. Para cada uno de los 34 objetivos de control de alto nivel, existe una guía o directriz de auditoría o de aseguramiento que permite la revisión de los procesos de TI contra los más de 300 objetivos detallados de control recomendados por COBIT, proporcionando así a la dirección la certeza de su cumplimiento y/o el método para su mejora.

## 4. Cómo podemos crear un SGTI

Vamos a tomar como referencia la norma ISO 9000:2005, aunque igual valdrían las normas ISO/IEC 20000:2005 para la Gestión de Servicios TI o la ISO/IEC 27001:2005 para la Gestión de la Seguridad de la Información, para definir cómo tiene que ser un sistema de gestión por de las TI (SGTI).

Todas comparten la misma estructura formal en lo que al ámbito organizativo se refiere: Estándares de la organización, buenas prácticas, control de la documentación, políticas, prácticas y procedimientos.

### Principios de gestión

Los sistemas de gestión pueden ayudar a las organizaciones a aumentar el control sobre los procesos TI y la satisfacción del cliente.

El enfoque a través de un SGTI anima a las organizaciones a analizar los requisitos del cliente, definir los procesos que contribuyen al logro de servicios aceptables para el cliente y a mantener estos procesos bajo control.

Se han identificado ocho principios de gestión de las TI que pueden ser utilizados por la alta dirección con el fin de conducir a la organización hacia una mejora en el desempeño: (1) Enfoque al cliente, (2) Liderazgo, (3) Participación del personal, (4) Enfoque basado en procesos, (5) Enfoque de sistema para la gestión, (6) Mejora continua, (7) Enfoque basado en hechos para la toma de decisión y (8) Relaciones mutuamente beneficiosas con el proveedor.

### Requisitos para los SGTI y requisitos para los servicios

Los requisitos para los SGTI son genéricos y aplicables a organizaciones de cualquier sector económico e industrial con independencia de la categoría del servicio ofrecido.

Los requisitos para los servicios pueden ser especificados por los clientes o por la organización, anticipándose a los requisitos del cliente, o por disposiciones reglamentarias.

### Enfoque de SGTI

Un enfoque para desarrollar, implementar o mantener un SGTI comprende diferentes etapas tales como: (1) Determinar las necesidades y expectativas de los clientes y de otras partes interesadas, (2) Establecer

---

la política y objetivos TI de la organización, (3) Determinar los procesos y las responsabilidades necesarias para el logro de los objetivos TI, (4) Determinar y proporcionar los recursos necesarios para el logro de los objetivos TI, (5) Establecer los métodos para medir la eficacia y eficiencia de cada proceso, (6) Aplicar estas medidas para determinar la eficacia y eficiencia de cada proceso, (7) Determinar los medios para prevenir no conformidades y eliminar sus causas y (8) Establecer y aplicar un proceso para la mejora continua del SGTI.

## Política TI y objetivos TI

La política TI proporciona un marco de referencia para establecer y revisar los objetivos TI. Los objetivos TI tienen que ser coherentes con la política TI y el compromiso de mejora continua y su logro debe poder medirse. El logro de los objetivos TI puede tener un impacto positivo sobre la calidad del servicio, la eficacia operativa y el desempeño financiero y, en consecuencia, sobre la satisfacción y la confianza de las partes interesadas.

## Papel de la alta dirección dentro del SGTI

Los principios de la gestión pueden ser utilizados por la alta dirección como base de su papel, que consiste en: (1) Establecer y mantener la política TI y los objetivos TI de la organización, (2) Promover la política TI y los objetivos TI a través de la organización para aumentar la toma de conciencia, la motivación y la participación, (3) Asegurarse del enfoque hacia los requisitos del cliente en toda la organización, (4) Asegurarse de que se implementan los procesos apropiados para cumplir con los requisitos de los clientes y de otras partes interesadas y para alcanzar los objetivos TI, (5) Asegurarse de que se ha establecido, implementado y mantenido un SGTI eficaz y eficiente para alcanzar los objetivos TI, (6) Asegurarse de la disponibilidad de los recursos necesarios, (7) Revisar periódicamente el SGTI, (8) Decidir sobre las acciones en relación con la política y con los objetivos TI y (9) Decidir sobre las acciones para la mejora del SGTI.

## Documentación

Su utilización contribuye a: (1) Lograr la conformidad con los requisitos del cliente y la mejora de los servicios TI, (2) Proveer la formación apropiada, (3) Contribuir a la repetibilidad y la trazabilidad, (4) Proporcionar evidencias objetivas y (5) Evaluar la eficacia y la adecuación continua del SGTI.

Dependiendo del ámbito de la metodología que se aplique, calidad, seguridad, gestión de servicios, etc., la documentación a controlar bajo el sistema de gestión puede ser diferente. Así si hablamos de calidad, la norma ISO 9000, indica que debemos controlar los siguientes tipos de documentos: (1) manuales, (2) planes, (3) especificaciones, (4) guías, (5) procedimientos e instrucciones y (6) registros. Para la norma 27001 los documentos son: (1) políticas del SGSI, (2) procedimiento y controles del SGSI, (3) metodología de evaluación del riesgo, (4) informe de evaluación del riesgo, (5) el plan para la gestión del riesgo, (6) procedimientos que aseguren la efectividad del plan, etc. A esto la norma ISO 20000 añade el ANS y otros documentos específicos.

Junto a esta documentación existe otra necesaria para la confección de la documentación anterior (informes, análisis, estudios, memorias, ...), para la comunicación dentro de la organización (convocatorias, actas, solicitudes, ...), etc., que debe estar bajo la gestión de un sistema de gestión documental. Por eso, es conveniente disponer de una única visión de la documentación, que puede estar basada en COBIT, aunque se puede establecer la correspondencia desde las perspectivas de los diferentes sistemas de gestión particulares<sup>3</sup>.

---

<sup>3</sup> En el Servicio de Producción se está usando un esquema de clasificación documental basado en los procesos de COBIT, apoyado además por una descripción de las posibles categorías de documentos. Se ha creado una plantilla estándar en OpenOffice que permite automatizar la catalogación documental.

---

## Evaluación de los SGTI

El SGTI debe estar bajo revisión continua, ya sea mediante auditorías o auto-evaluaciones. Los hallazgos de las revisiones se utilizan para evaluar la eficacia del SGTI y para identificar oportunidades de mejora. Es responsabilidad de la dirección llevar a cabo de forma regular evaluaciones sistemáticas de la conveniencia, adecuación, eficacia y eficiencia del SGTI con respecto a los objetivos y a la política TI.

## Mejora continua

El objetivo de la mejora continua del SGTI es incrementar la probabilidad de aumentar la satisfacción de los clientes y de otras partes interesadas.

Las siguientes son acciones destinadas a la mejora: (1) Análisis y evaluación de la situación existente para identificar áreas para la mejora, (2) El establecimiento de los objetivos para la mejora, (3) La búsqueda de posibles soluciones para lograr los objetivos, (4) La evaluación de dichas soluciones y su selección, (5) La implementación de la solución seleccionada, (6) La medición, verificación, análisis y evaluación de los resultados de la implementación para determinar que se han alcanzado los objetivos, (6) La formalización de los cambios.

## 5. Cómo debemos usar las metodologías existentes

Tenemos que tener claro que COBIT ofrece un marco de referencia genérico para la gestión TI, pero no cubre en profundidad aspectos concretos de las TI como son la calidad, la seguridad de la información, la gestión de servicios o la gestión de proyectos.

Para estos casos concretos debemos recurrir a metodologías específicas, pero tratando de que encajen, sin forzarlo, en el marco general de COBIT.

Lo que tienen en común todas las metodologías que propugnan la creación de un sistema de gestión es que éste debe basarse en los procesos que la organización ejecuta.

COBIT define los siguientes recursos TI: (1) Las personas, (2) la información, (3) las aplicaciones y (4) la infraestructura. Estos recursos necesitan ser manejados por los procesos TI para alcanzar las metas TI propuestas. Los servicios TI son las salidas de los procesos TI y la infraestructura TI, los cuales son ejecutados y controlados por personas que trabajan en una estructura organizativa que está soportada y gestionada por la tecnología.

## 6. ¿Qué metodologías podemos usar?

### El Gobierno TI

COBIT es ante todo una metodologías para el Gobierno TI, y por tanto, los objetivos estratégicos TI deben estar alineados con los objetivos estratégicos de la Organización. Así pues, lo primero que tenemos que hacer es conectar la función TI con el resto de la organización. Para ello podemos utilizar IT BSC. Además, la función TI, como cualquier otra función de la organización, tiene que demostrar que es valiosa para la organización. Si no es así, disminuirá el presupuesto TI.

El Balance Scorecard, BSC, fue introducido por Kaplan y Norton en el ámbito empresarial (desde 1992). Su idea básica es que la evaluación de una organización no debe restringirse a evaluación financiera tradicional sino que debería ser complementada con medidas concernientes a la satisfacción de los clientes, a los

procesos internos y a la capacidad de innovar. Estas medidas adicionales deberían asegurar el futuro financiero de la empresa y conducir a la empresa hacia sus metas estratégicas mientras mantiene equilibradas estas 4 perspectivas (financiera, cliente, proceso e innovación). Kaplan y Norton proponen una estructura en 3 capas para estas 4 perspectivas: misión (por ejemplo, para convertir a los clientes en su suministrador preferido), objetivos (por ejemplo, para proveer a los clientes de nuevos productos) y medida (por ejemplo, porcentaje de facturación generado por los nuevos productos). La aplicación de BSC a las TI fue descrita por Van Grembergen and Van Bruggen (1997) and Van Grembergen and Timmerman (1998).

La Tabla 2 resume las 4 perspectivas de IT BSC.

| Perspectiva   | Misión  | Estrategia  |
|---|---|---|
| ORIENTACIÓN A LOS USUARIOS<br>¿Cómo los usuarios ven el departamento TI?                      | Ser los suministradores de sistemas de información preferidos | Suministradores preferidos de aplicaciones<br>Suministradores preferidos de operaciones o sugerir de la mejor solución de cualquier fuente<br>Asociación con los usuarios<br>Satisfacción de los usuarios |
| EXCELENCIA OPERACIONAL<br>¿Cómo de efectivos y eficientes son los procesos TI?                | Ofrecer servicios y aplicaciones TI efectivas y eficientes    | Desarrollo eficiente y efectivo<br>Operaciones eficientes y efectivas   |
| CONTRIBUCIÓN AL NEGOCIO<br>¿Cómo ve la dirección el departamento TI?                          | Obtener de la organización una inversión razonable en TI      | Control del gasto en TI<br>Valor para la organización de los proyectos TI<br>Proveer nuevas capacidades de negocio  |
| ORIENTACIÓN FUTURA<br>¿Cómo están posicionadas las TI para satisfacer la necesidades futuras? | Desarrollar oportunidades para contestar a desafíos futuros   | Entrenamiento y educación de la dirección TI<br>Experiencia de la dirección TI<br>Investigación en tecnologías emergentes<br>Antigüedad de las aplicaciones   |

**Tabla 2** –IT Balanced Scorecard

Cada una de estas perspectivas deben ser trasladadas en sus correspondientes métricas y medidas. Estas medidas se deben repetir periódicamente y deben ser confrontadas con las metas y puntos de control que han sido fijados con anterioridad. Es muy importante en un IT BSC que se establezcan las relaciones causa-efecto y que las conexiones entre los 2 tipos de medidas, de resultado y de desempeño o habilitadora, estén claras. Un IT BSC bien construido necesita de estos 2 tipos de medidas. Las medidas de resultados sin medida de desempeño no indica cómo los resultados pueden ser alcanzados. Y medidas de desempeño sin medidas de resultados pueden inducir a inversiones sin saber si la estrategia es efectiva. Esta relación causa-efecto debe ser definida para toda la IT BSC.

La relación entre BSC para la organización y IT BSC para las TI se establece a través de la perspectiva de contribución al negocio, como se muestra en la Figura 1 respecto de COBIT. Así pues, ya sabemos cómo podemos establecer la relación entre las TI y el resto de la organización.



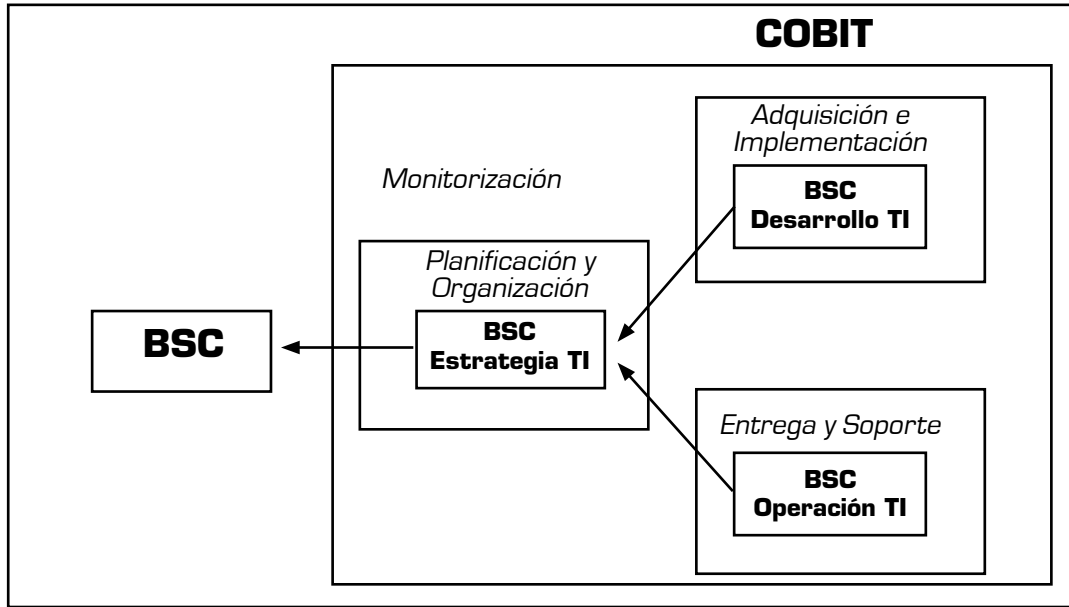


Figura 1 –Relación entre COBIT e IT BSC

## Gestión TI

Una vez establecida la relación entre la función TI y el resto de las organización, podemos ver cómo pueden ayudar el resto de las metodologías a la Gestión TI.

En este caso no se van a describir estas metodologías ampliamente conocidas. Me limitaré, a modo de orientación, a indicar dónde puede encajar cada una de ellas, analizando los 4 dominios de COBIT.

La Tabla 3 muestra la relación entre COBIT y otras metodologías (no se detallan los procesos correspondientes en las otras metodologías, sólo se indica que existe relación con algún proceso o control descrito en las otras metodologías) para cada proceso TI de COBIT. La relación indicada no implica que se pueda sustituir el proceso TI de COBIT por el de la metodología correspondiente, ni tampoco que la metodología correspondiente cubra completamente el proceso TI de COBIT con el que está relacionado.

| CD | DOMINIO                      |   | OTRAS METODOLOGÍAS, ESTÁNDARES Y BUENAS PRACTICAS |
|----|------------------------------|---|---|
|    | CP                           | Proceso   |   |
| PO | PLANIFICACIÓN Y ORGANIZACIÓN |   |   |
|    | 1.0                          | Definición del Plan Estratégico TI                          | IT BSC  |
|    | 2.0                          | Definición de la Arquitectura de Información                |   |
|    | 3.0                          | Determinación de la Dirección Tecnológica                   |   |
|    | 4.0                          | Definición de la Organización y de las Relaciones TI        |   |
|    | 5.0                          | Gestión de la Inversión TI                                  | ITIL  |
|    | 6.0                          | Comunicación de los Objetivos y Aspiraciones de la Gerencia |   |
|    | 7.0                          | Gestión de Recursos Humanos                                 |   |
|    | 8.0                          | Gestión de Calidad  | ISO 9000  |
|    | 9.0                          | Análisis y Gestión de Riesgos TI                            | MAGERIT V2, ISO 17799, ISO 27001                  |
|    | 10.0                         | Gestión de Proyectos  | PRINCE2   |

| CD                           | DOMINIO                               |   | OTRAS METODOLOGÍAS, ESTÁNDARES Y BUENAS PRACTICAS |
|------------------------------|---------------------------------------|---|---|
|                              | CP                                    | Proceso   |   |
| <b>AI</b>                    | <b>ADQUISICIÓN E IMPLEMENTACIÓN</b>   |   |   |
|                              | 1.0                                   | Identificación de Soluciones Automatizadas                    | CMMi  |
|                              | 2.0                                   | Adquisición y Mantenimiento de Software de Aplicación         | CMMi  |
|                              | 3.0                                   | Adquisición y Mantenimiento de la Infraestructura Tecnológica | ITIL  |
|                              | 4.0                                   | Habilitar la operación y el uso de los SI                     | CMMi  |
|                              | 5.0                                   | Procurar los recursos TI                                      | PRINCE2   |
|                              | 6.0                                   | Gestión de Cambios  | ITIL  |
|                              | 7.0                                   | Instalación y Acreditación de Soluciones y Cambios            | ITIL  |
| <b>DS</b>                    | <b>ENTREGA DE SERVICIOS Y SOPORTE</b> |   |   |
|                              | 1.0                                   | Definición y Gestión de Niveles de Servicio                   | ITIL  |
|                              | 2.0                                   | Gestión de Servicios prestados por Terceros                   |   |
|                              | 3.0                                   | Gestión del Desempeño y Capacidad                             | ITIL  |
|                              | 4.0                                   | Aseguramiento de Servicio Continuo                            | ITIL  |
|                              | 5.0                                   | Garantizar la Seguridad de Sistemas                           | ISO/IEC 17799                                     |
|                              | 6.0                                   | Identificación y Asignación de Costos                         | ITIL  |
|                              | 7.0                                   | Educación y Entrenamiento de Usuarios                         |   |
|                              | 8.0                                   | Gestión del Service Desk y de los Incidentes                  | ITIL  |
|                              | 9.0                                   | Gestión de la Configuración                                   | ITIL  |
|                              | 10.0                                  | Gestión de Problemas  | ITIL  |
|                              | 11.0                                  | Gestión de Datos  |   |
|                              | 12.0                                  | Gestión del Entorno Físico (Instalaciones)                    |   |
|                              | 13.0                                  | Gestión de Operaciones  |   |
| <b>ME</b>                    | <b>MONITORIZACIÓN Y EVALUACIÓN</b>    |   |   |
|                              | 1.0                                   | Monitorización y Evaluación de la Ejecución                   | IT BSC  |
|                              | 2.0                                   | Monitorización y Evaluación del Control Interno               |   |
|                              | 3.0                                   | Aseguramiento del Cumplimiento de la Normativa                |   |
|                              | 4.0                                   | Proveer el Gobierno TI  | IT BSC  |
| <b>CD: Código de Dominio</b> |                                       |   | <b>CP: Código de Proceso</b>                      |

Tabla 3 -Relación de COBIT con otras metodologías

## 7. Conclusiones

### Dirección estratégica

Como hemos visto IT BSC es la metodología que mejor se adapta para realizar la dirección estratégica de las TI. IT BSC se fundamenta en las métricas como base para saber si los objetivos estratégicos se están alcanzando, por eso también es útil en dominio ME.

### Organización TI y RRHH

ITIL da indicaciones sobre la organización necesaria para soportar la gestión de servicios TI, y COBIT en su

---

última versión, la 4, cruza los procesos TI con los RRHH habituales en los centros TI, pero ninguno de las 2 metodologías dice cómo debería ser la estructura de un centro TI.

## **Monitorización y Evaluación**

ITIL define muy bien como son los procesos para la gestión de servicios TI pero no incluye ni métricas ni controles. COBIT, en cambio, define como elementos de control y medida de los procesos los siguientes: un Modelo de Madurez para el control de los procesos de TI de modo que la organización puede saber que grado de madurez ha alcanzado, donde está en relación con los “mejores de su clase” y con respecto a los estándares internacionales y, así mismo, decidir hasta donde quiere llegar.

Factores Críticos de Éxito, FCE, (Critical Success Factors, CSF) que definen o determina cuales son las directrices más importantes que deben ser tenidas en cuenta por la dirección para lograr el control de los procesos de TI.

Indicadores Claves del logro / Objetivos o de Resultados, ICL, (Key Goal Indicators, KGI) los cuales definen los mecanismos de medición que indicarán a la dirección—después del hecho— si un proceso de TI ha satisfecho los requerimientos del negocio.

Indicadores Clave de desempeño, ICD, (Key Performance Indicators, KPI) que son indicadores primarios que definen la métrica para saber como de bien se está ejecutando el proceso TI en comparación al objetivo buscado.

## **Seguridad de la Información**

La norma ISO/IEC 17799 define controles específicos para la seguridad de la información, y la norma ISO/IEC 27001:2005 certifica el SGSI contra los controles establecidos en la norma ISO/IEC 17799. Sin embargo, no se especifican los procesos relacionados con la seguridad de la información.

## **Gestión de la Infraestructura**

En cuanto a la infraestructura TI sólo ITIL define la Gestión de la Infraestructura e indica como los procesos de gestión de servicios TI se relacionan con la infraestructura almacenada en CMDB (Configuration Management Database). Si la infraestructura está bien relacionada y conectada a los procesos TI es posible definir adecuadamente los servicios TI y realizar una adecuada gestión de los mismos.

## **Gestión de Servicios TI**

ITIL está especialmente diseñado para la Gestión de Servicios TI, aunque le faltan los elementos de medida y control que si tiene COBIT para los procesos equivalentes. Así pues, ITIL y COBIT se complementan muy bien en la Gestión de Servicios TI.

## **Gestión de Proyectos y Desarrollo de Aplicaciones**

PRINCE2 es una metodología de Gestión de Proyectos, no necesariamente proyectos TI, ampliamente usada y reconocida.

Igualmente, en cuanto al desarrollo de aplicaciones, CMMi es posiblemente la opción con más fuerza actualmente.

---

## Auditoría

Tanto COBIT como ISO/IEC 17799 a través de los controles que ambas metodologías establecen, permiten la evaluación de la función TI.

## Conformidad

El aspecto más preocupante respecto a la conformidad de las TI con la legislación es el desconocimiento que, en general, se tiene de la legislación aplicable. Propuestas en la línea de Sarbane Oxley serían muy bien recibidas, ya que los controles normativos están dispersos en las distintas normas aplicables a las TI.

## 8. Anexo: Definiciones

Seguridad de la Información: Consiste en preservar la:

- Confidencialidad: Sólo quienes estén autorizados pueden acceder a la información
- Integridad: La información y sus métodos de proceso son exactos y completos
- Disponibilidad: Los usuarios autorizados TI tienen acceso a la información y a sus activos asociados cuando lo requieran. (ISO 17799:2002)

Información: Datos que poseen significado (ISO9000:2000); En soportes magnéticos y no magnéticos

Sistema: Una colección de componentes organizados para llevar a cabo una función o un grupo de funciones (ISO 9000)

Sistema de Información (SI): Colección organizada de HW, SW, aplicaciones, políticas, procedimientos y personas, que almacenan, procesan y proporcionan acceso a la información: Manuales, Semi-automáticos y Automáticos

Gestión: Actividades coordinadas para dirigir y controlar una organización (ISO 9000)

Sistema de Gestión: Sistema para establecer la política y los objetivos y para lograr dichos objetivos (ISO 9000)