Mantenimiento del Software

S5

Francisco Ruiz, Macario Polo

Grupo Alarcos

Dep. de Informática

ESCUELA SUPERIOR DE INFORMÁTICA

UNIVERSIDAD DE CASTILLA-LA MANCHA

http://alarcos.inf-cr.uclm.es/doc/mso/

Ciudad Real, 2000/2001

Índice - Sesión 5

- Introducción a la Auditoría.
  - Concepto de Auditoría
  - Clases de Auditoría
  - Auditoría de Sistemas de Información
  - Control Interno y Auditoría
- El Proceso de Auditoría según ISO (i)
- La Metodología CobiT
  - Audiencia
  - Fundamentos
  - Estructura
  - Objetivos de Control Generales
- Adaptación de CobiT al PMS
  - Objetivos de Control para el PMS

- Bibliografía:
  - Rafael Bernal, Óscar Coltell: Auditoría de los Sistemas de Información. Edic. UPV.
  - ISACF, CobiT: Governance, Control and Audit for Information and Related Technology, 2nd edition. Information Systems Audit and Control Foundation. USA, 1998.

Concepto de Auditoría (i)

- Actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.
- Sus principales características son:
  - *Contenido*: una opinión.
  - *Condición*: profesional.
  - *Justificación*: sustentada en determinados procedimientos (la opinión profesional se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma).
  - *Objeto*: una determinada información obtenida en un cierto soporte.
  - *Finalidad*: determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.
- Siempre es un proceso que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

Clases de Auditoría (i)

- Las principales **Clases de Auditoría** son:
  - a) Por el sujeto que la efectúa:
    - *Interna*: auditores que forman parte de la propia organización.
    - *Externa*: auditores ajenos a la organización.
  - b) Por su contenido y fines:
    - *De Gestión*: afecta a la situación global de la empresa.
    - *Organizativa*: analiza la adecuación de la estructura organizativa.
    - *Operacional*: hasta qué punto se están cumpliendo los objetivos establecidos e identificación de los puntos que necesitan mejorar.
    - *Financiera*: examen y verificación del estado financiero, acompañado de una opinión sobre su fiabilidad.
    - *Contable*: adecuación de los criterios empleados para recoger los hechos mediante apuntes contables en los estados financieros.
    - *Informática*: examen y verificación del correcto funcionamiento y control del sistema informático.
    - *Económico-Social*: diagnóstico sobre el proceso económico y los resultados sociales obtenidos.

Clases de Auditoría (ii)

  - c) Por su amplitud:
    - *Total*: afecta a todos los elementos de la organización.
    - *Parcial*: se concentra en determinados elementos.
  - D) Por su frecuencia:
    - *Permanente*
    - *Ocasional*
- Es más correcto y más genérico hablar de **Auditoría de Sistemas de Información** (ASI) que de Auditoría Informática. El primer término engloba al segundo y también a los procesos y medios no automáticos que forman parte del Sistema de Información de una Organización:
  - *Auditoría*: Herramientas y métodos para establecer criterios que permitan medir la eficacia, eficiencia y conformidad con los objetivos deseados de un determinado sistema (el control del control).
  - *de Sistemas de Información*: eficacia, eficiencia y conformidad con los objetivos del sistema de un información.

Auditoría de Sistemas de Información (i)

- Los objetivos fundamentales de la ASI son:
  - **De Protección de los Activos y Recursos**: Verificar que existe un sistema de control interno que protege los activos materiales e inmateriales de la instalación informática de cualquier posible amenaza o riesgo.
  - **De Integridad de Datos**: el sistema de control interno debe tener mecanismos que vigilen constantemente el mantenimiento de la integridad de los datos.
  - **De Efectividad del Sistema**: Un sistema de información efectivo alcanza sus objetivos. Estos objetivos dependen de las características y necesidades de los usuarios y de los canales y procedimientos de decisión.
  - **De Eficiencia del Sistema**: Un sistema de información eficiente utiliza el mínimo de recursos necesarios para obtener las salidas requeridas. LA eficiencia no debe medirse de forma aislada sino considerando el conjunto de procesos y los recursos disponibles.

Auditoría de Sistemas de Información (ii)

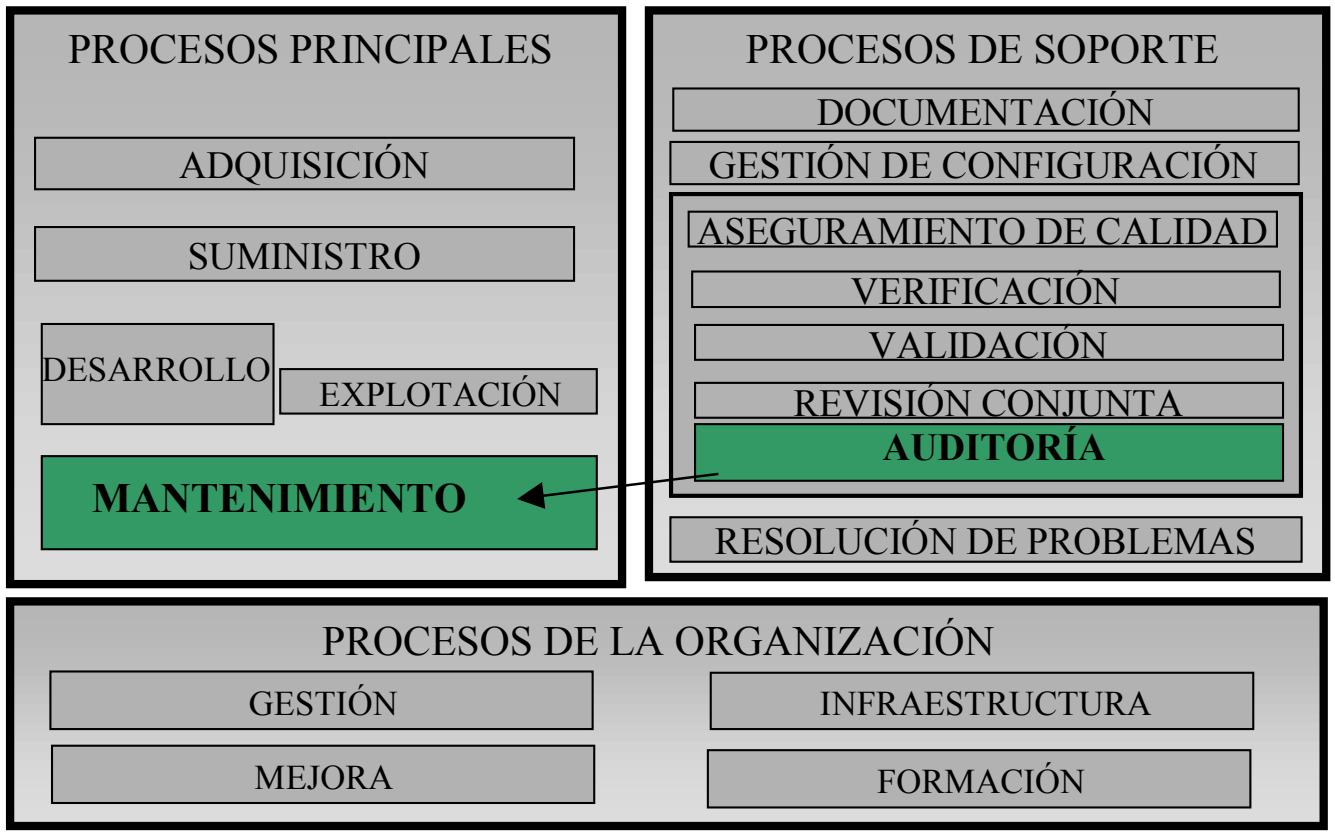
- Los principales tipos de ASI son:
  - de la **Organización y Gestión del Departamento de Informática**: políticas, estructuras de gestión y organizativas, procedimientos operativos y entorno de control.
  - De la **Seguridad Física y Lógica**: políticas, procedimientos y planes para proteger la información y el sistema de información.
  - De las **Tecnologías de la Información**:
    - de los computadores,
    - de bases de datos,
    - de proceso de datos distribuido y control de datos en red,
    - de redes locales,
    - del desarrollo de un proyecto <= **(AQUI se incluye la Auditoría del PMS)**
    - de intercambio electrónico de datos,
    - de herramientas (CASE, etc.),

Control Interno y Auditoría

	CONTROL INTERNO INFORMÁTICO	AUDITOR INFORMÁTICO
SIMILITUDES	✓ Conocimientos especializados en Tecnología de la Información. ✓ Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información.	
DIFERENCIAS	✓ Análisis de los controles en el día a día. ✓ Informa a la Dirección del Departamento de Informática. ✓ Sólo personal interno. ✓ El alcance de sus funciones es únicamente sobre el Departamento de Informática.	✓ Análisis de un momento informático determinado. ✓ Informa a la Dirección General de la Organización. ✓ Personal interno y/o externo. ✓ Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.

El Proceso de Auditoría según ISO (i)

- Recordemos el modelo de procesos de ISO 12207:



El Proceso de Auditoría según ISO (ii)

- Según la norma **ISO 12207**, el Proceso de **Auditoría del Software** (PAS) es uno de los procesos de soporte.
- Se define como el proceso para determinar el cumplimiento con los requerimientos, los planes o los contratos.
- Debe ser realizado por personas autorizadas con el propósito de mantener una valoración independiente de los productos y procesos del software.
- Intervienen dos participantes: la parte auditora y la parte auditada.
- La norma **ISO 14764** determina que el PAS da soporte en las siguientes actividades del PMS:
  - Aceptación/Revisión del Mantenimiento.
  - Migración.
  - Retirada.

El Proceso de Auditoría según ISO (iii)

- Consta de dos actividades:
  - *Implementación del Proceso*; y
  - *Auditoría*.
- Durante la **Implementación del Proceso** se realizan las siguientes tareas:
  - Se realizarán auditorías de los hitos predeterminados en el plan del proyecto.
  - El personal auditor no tendrá responsabilidad directa sobre los productos software y actividades auditados.
  - Todos los recursos necesarios para realizar la auditoría deberán ser acordados por las partes (incluyendo personal de apoyo, locales, infraestructura, hardware, software y herramientas).
  - Para cada auditoría las partes deberán acordar siguientes puntos: agenda; productos software (y resultados de alguna actividad) que serán revisados; alcance y procedimientos de la auditoría; y criterios de entrada y salida para la auditoría.
  - Los problemas descubiertos durante las auditorías se registrarán y se pasarán al Proceso de Resolución de Problemas.
  - Después de completar una auditoría, los resultados se documentarán y se proporcionarán a la parte auditada.
  - Las partes deberán acordar el resultado de la auditoría y cualquier responsabilidad y criterio de cierre.

El Proceso de Auditoría según ISO (iv)

- La actividad de auditoría propiamente dicha consta de una única tarea tendente a garantizar que:
  - Los elementos software (código, etc.) reflejan la documentación de diseño.
  - La revisión de aceptación y los requerimientos de prueba prescritos por la documentación son adecuados para la aceptación de los productos software.
  - Los datos de prueba cumplen con la especificación.
  - Los productos software fueron suficientemente probados y sus especificaciones cumplidas.
  - Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas.
  - La documentación de usuario cumple los estándares especificados.
  - Las actividades han sido conducidas de acuerdo con los requerimientos, planes y contratos aplicables.
  - Los costes y calendarios se ajustan a los planes establecidos.

La Metodología CobiT

- **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnologies.
- Propuesta por la **ISACF** (Information Systems Audit and Control Foundation).
- Es la principal propuesta metodológica realizada a nivel internacional para abordar la **Auditoría de Sistemas de Información**.
- Supone un paso muy importante al considerar que, a efectos de auditoría, el sistema de información de una organización es **UNICO**, aunque ciertos procesos se realicen de forma manual y otros mediante el uso de la informática.
- La filosofía de CobiT asimila los principios de **reingeniería de empresas** (BPR) y divide las funciones que ha de realizar un sistema de información en procesos que, a su vez, están subdivididos en actividades y tareas más simples.
- Los sistemas de información están **orientados a los procesos** y por tanto su auditoría se debe adaptar a estos conceptos.

La Metodología CobiT - Audiencia

- CobiT esta diseñado para ser utilizado por tres audiencias distintas:
  - **Gestores**:
    - Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de Tecnologías de la Información (TI) frecuentemente impredecible.
  - **Usuarios**:
    - Para obtener una garantía en cuanto a la seguridad y control de los servicios de TI proporcionados internamente o por terceras partes.
  - **Auditores de Sistemas de Información**:
    - Para dar soporte a las opiniones mostradas a los Gestores sobre los controles internos.

- También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquéllos con responsabilidades en el campo de las TI en las empresas.

La Metodología CobiT - Fundamentos (i)

- *El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.*

La Metodología CobiT - Fundamentos (ii)

- Para alcanzar los requerimientos de negocio, la **información** necesita satisfacer ciertos **criterios**:
  - Requerimientos de **Calidad**:
    - Calidad
    - Coste
    - Entrega (servicio)
  - Requerimientos **Fiduciarios**:
    - Efectividad y eficiencia de las operaciones
    - Fiabilidad de la información
    - Cumplimiento de leyes y normas
  - Requerimientos de **Seguridad**:
    - Confidencialidad
    - Integridad
    - Disponibilidad

La Metodología CobiT - Fundamentos (iii)

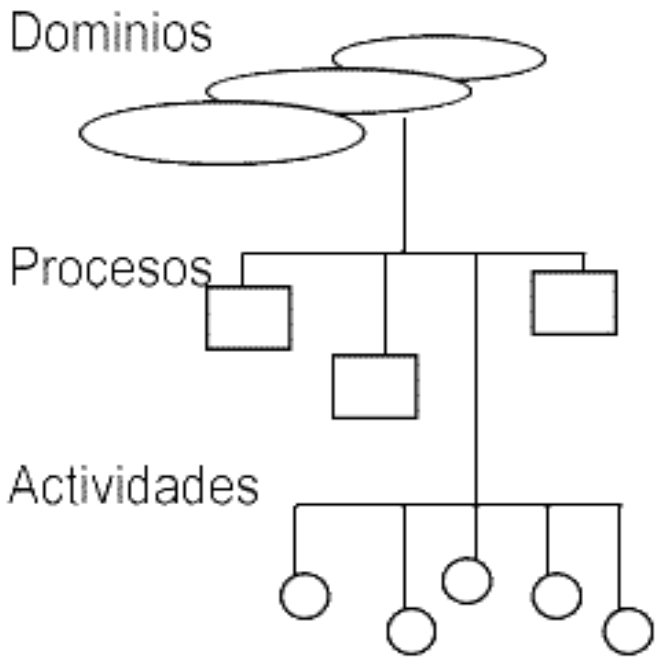
- En CobiT se establecen los siguientes **recursos en TI** necesarios para alcanzar los objetivos de negocio:
  - **Datos**:
    - Los objetos de datos en el sentido más amplio, externos e internos, estructurados y no estructurados, gráficos, sonidos, etc.
  - **Aplicaciones**:
    - Suma de procedimientos manuales y automatizados.
  - **Tecnología**:
    - Hardware, sistemas operativos, SGBD's, redes, multimedia, etc.
  - **Infraestructura**:
    - Recursos para instalar y soportar los sistemas de información.
  - **Personas**:
    - Habilidades, conocimientos y productividad para planificar, organizar, adquirir, entregar, soportar y supervisar sistemas y servicios de información.

La Metodología CobiT - Estructura (i)

- La estructura de CobiT se define a partir de una premisa simple y pragmática: "*Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos*".

Se definen 34 **objetivos de control generales** (OCGs), uno para cada uno de los **procesos** de las TI. Estos procesos están agrupados en cuatro grandes **dominios**:

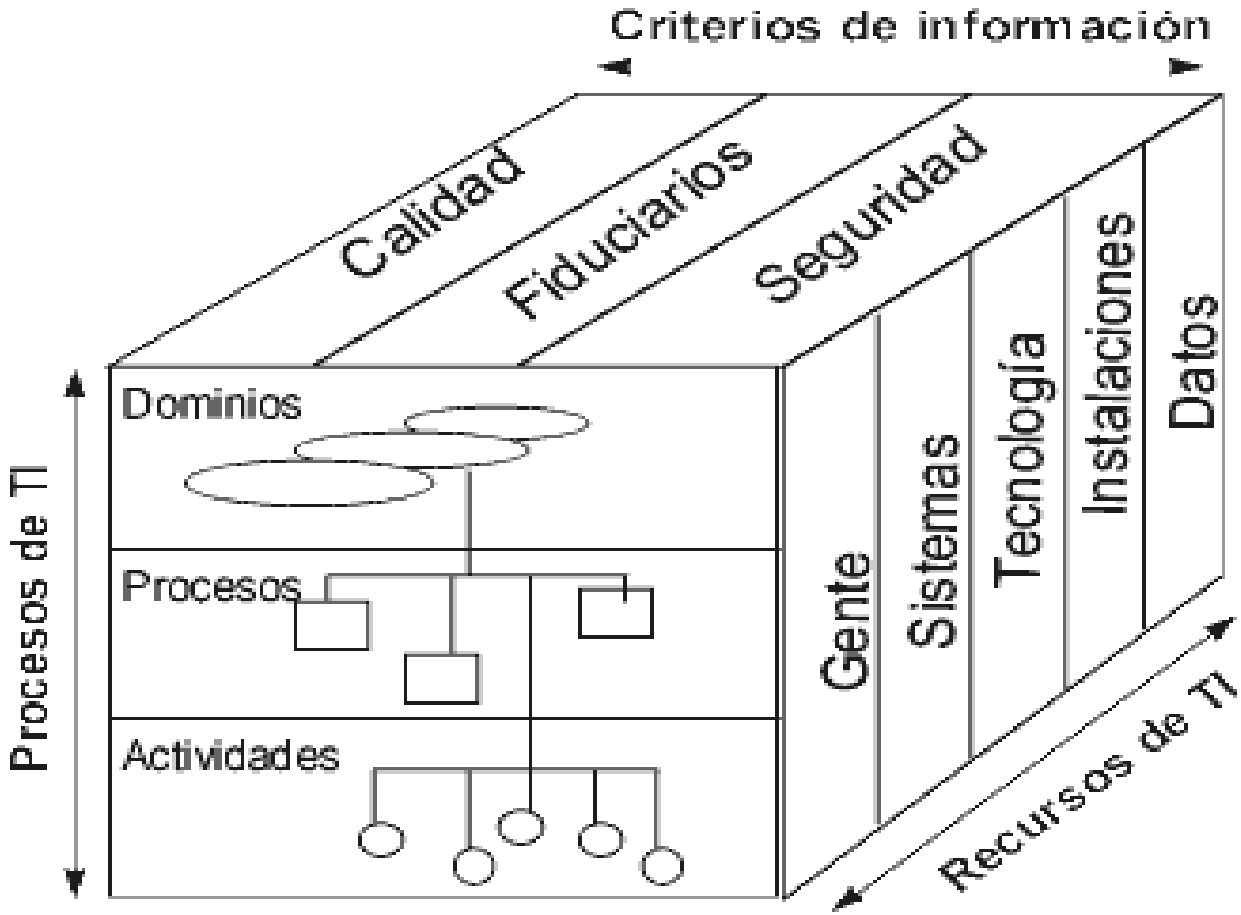
- *planificación y organización*,
- *adquisición e implantación*,
- *suministro y soporte*, y
- *supervisión*.



La metodología CobiT - Estructura (ii)

- Los 34 OCGs propuestos se concretan en 302 objetivos de control detallados (OCDs).
- Un **control** se define como "*las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzarán y que los eventos no deseados se preverán o se detectarán, y corregirán*".
- Un **objetivo de control** se define como "*la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de las TI*".
- En suma, la estructura conceptual se puede enfocar desde **tres puntos de vista** (ver figura):
  - Los ***recursos*** de las TI,
  - Los ***criterios empresariales*** que debe satisfacer la ***información***, y
  - Los ***procesos*** de las TI.

La metodología CobiT - Estructura (iii)



Las tres dimensiones conceptuales de CobiT

Objetivos de Control Generales (i)

- **Planificación y Organización**
  - PO 1 Definir un Plán Estratégico de TI
  - PO 2 Definir la Arquitectura de la Información
  - PO 3 Determinar la Dirección Tecnológica
  - PO 4 Definir la Organización e Interrelaciones en TI
  - PO 5 Gestionar la Inversión en TI
  - PO 6 Comunicar Objetivos y Dirección a la Gerencia
  - PO 7 Gestionar los Recursos Humanos
  - PO 8 Asegurar Cumplimiento de los Requerimientos Externos
  - PO 9 Evaluar Riesgos
  - PO 10 Gestionar los Proyectos
  - PO 11 Gestión de la Calidad

Objetivos de Control Generales (ii)

- **Adquisición e Implantación**
  - AI 1 Identificación de Soluciones
  - AI 2 Adquisición y Mantenimiento de Aplicaciones Software
  - AI 3 Adquirir y Mantener la Infraestructura Tecnológica
  - AI 4 Desarrollar y Mantener los Procedimientos de TI
  - AI 5 Instalación y Acreditación de Sistemas
  - AI 6 Gestión de Cambios

- **Supervisión**
  - M 1 Supervisar los Procesos
  - M 2 Evaluar la Idoneidad del Control Interno
  - M 3 Obtener Estimaciones Independientes
  - M 4 MAntener una Auditoría Independiente

Objetivos de Control Generales (iii)

- **Suministro y Soporte**
  - DS 1 Definir Niveles de Servicio
  - DS 2 Gestionar los Servicios a Terceros
  - DS 3 Gestionar el Rendimiento y la Capacidad
  - DS 4 Asegurar un Servicio Continuo
  - DS 5 Garantizar la Seguridad de los Sistemas
  - DS 6 Identificar y Asignar Costes
  - DS 7 Formar y Entrenar a los USuarios
  - DS 8 Asistir y Aconsejar a los Clientes de TI
  - DS 9 Gestión de la Configuración
  - DS 10 Gestionar Problemas e Incidentes
  - DS 11 Gestionar los Datos
  - DS 12 Gestionar las Infraestructuras
  - DS 13 Gestionar las Operaciones

Adaptación de CobiT al PMS (i)

- La **Metodología MANTEMA** versión 2 incluye una propuesta para abordar la auditoría del proceso de mantenimiento del software basada en:
  - el modelo de procesos del software definido en la norma ISO 12207,
  - el estándar ISO 14764 para el proceso de mantenimiento del software, y
  - la metodología CobiT para la auditoría de sistemas de información.
- En CobiT no se especifica cómo debe realizarse la auditoría del PMS. Esta laguna se intenta resolver con la propuesta formulada en MANTEMA.
- Esta propuesta se ha obtenido realizando un análisis de todos los objetivos de control incluidos en CobiT y seleccionando los que tienen relación con el proceso de mantenimiento del software. La lista resultante ha sido cambiada definiendo un objetivo de control general llamado *'Gestión del proceso de mantenimiento del software'*. Este objetivo general ha sido concretado en 14 objetivos de control detallados que amplían considerablemente los incluidos en CobiT.

Adaptación de CobiT al PMS (ii)

- En el dominio AI (**Adquisición e Implantación**), los OCGs y OCDs útiles para el Mantenimiento del Software son:
  - AI01 - Identificación de soluciones
    - 1.15 Mantenimiento del software por terceros
  - AI02 - Adquisición y mantenimiento de aplicaciones software
    - 2.2 Cambios grandes en sistemas existentes
  - AI05 - Instalación y acreditación de sistemas
    - 5.3 Conversión
  - AI06 - Gestión de cambios
    - 6.1 Iniciación y control de los requerimientos de cambio
    - 6.2 Valorar impacto
    - 6.3 Definir el control de cambios
    - 6.4 Actualización de documentación y procedimientos
    - 6.5 Autorización del mantenimiento
    - 6.6 Política de versiones del software
    - 6.7 Distribución del software

Adaptación de CobiT al PMS (iii)

- En el dominio DS (**Suministro y Soporte**), los OCGs y OCDs útiles para el Mantenimiento del Software son:
  - DS09 - Gestión de la configuración
    - 9.1 Registrar la configuración
    - 9.2 Configuración básica
    - 9.3 Contabilizar los estados pasados
    - 9.4 Control de la configuración
    - 9.6 Almacenar el software

- Los dominios PO (**Planificación y Organización**) y M (**Supervisión**) no contienen ningún objetivo de control relacionado directamente con el Mantenimiento del Software.

Adaptación de CobiT al PMS (iv)

- El OCG más relacionado con el PMS es la Gestión de Cambios (AI06):

Objetivos de Control Detallados (CobiT)	**Actividades PMS relacionadas**
6.1 Iniciación y control de los requerimientos de cambio	Implementar el Proceso
6.2 Valorar impacto	Análisis del Problema y Modificación Realización de la Modificación
6.3 Definir el control de cambios	Implementar el Proceso
6.4 Actualización de documentación y procedimientos	Realización de la Modificación
6.5 Autorización del mantenimiento	Revisión/Aceptación del mantenimiento
6.6 Política de versiones del software	Implementar el Proceso
6.7 Distribución del software	Realización de la Modificación

OCDs de la Gestión de Cambios vs Actividades del PMS

- Las disfunciones se deben a que CobiT e ISO utilizan un diferente modelo de procesos.
  - Por ello, se hace necesaria la adaptación de CobiT al modelo de ISO.

Objetivos de Control para el PMS (i)

- En la Metodología MANTEMA para la Gestión Integral del PMS se ha incluido la siguiente propuesta de adaptación:
  - La gestión del PMS pasa a ser un objetivo de control general (OCG) dentro del dominio de 'Adquisición e Implantación' ya que el MS es un proceso básico para la correcta implantación (explotación) de un sistema de información.
- A continuación se resume el resultado de la primera versión de objetivos de control detallados incluidos en MANTEMA:
  - Dominio: Adquisición e Implantación
  - Objetivo General: AI06 - Gestión del proceso de mantenimiento del software.
  - Descripción: *las actividades del negocio se realizan sin interrupciones imprevistas y el software de los sistemas de información existentes se adapta a las nuevas necesidades.*

Objetivos de Control para el PMS (ii)

- La Gestión del PMS (el OCG) incluye 14 objetivos de control detallados:
  - **6.1 Cambios en el entorno operativo**: existe un procedimiento organizado para realizar la migración de un producto software desde un entorno operativo antiguo a otro nuevo.
  - **6.2 Retirada del software**: la metodología de desarrollo y/o mantenimiento de software incluye un procedimiento formal para la retirada de un producto software cuando ha concluido su ciclo de vida útil.
  - **6.3 Tipos de mantenimiento**: están categorizados los tipos de mantenimiento del software y para cada tipo se han planificado las actividades y tareas a realizar.
  - **6.4 Acuerdo de mantenimiento**: las relaciones entre el mantenedor y el cliente y las obligaciones de cada uno están establecidas en un acuerdo o contrato de mantenimiento.
  - **6.5 Mejora de la calidad del proceso**: la metodología empleada para el mantenimiento del software incluye técnicas para aumentar la mantenibilidad (facilidad de mantenimiento).
  - **6.6 Planificación del mantenimiento**: Existe un plan de mantenimiento que incluye el alcance del mantenimiento, quién lo realizará, una estimación de los costes y un análisis de los recursos necesarios.
  - **6.7 Procedimientos para solicitudes de modificación (SM)**: existen procedimientos normalizados para iniciar, recibir y registrar SMs.

Objetivos de Control para el PMS (ii)

- **6.8 Gestión y control de cambios**: el mantenedor tiene establecido un interface organizacional para que el proceso de mantenimiento pueda verse beneficiado por el proceso de gestión de la configuración.
- **6.9 Análisis y valoración de las SMs**: las SMs son categorizadas y priorizadas, y existen mecanismos bien estructurados para evaluar su impacto, costes y criticidad.
- **6.10 Verificación de los problemas**: el mantenedor replica o verifica que realmente existe el problema que originó la SM.
- **6.11 Registro de las SMs**: el mantenedor documenta y registra las SMs, con sus análisis, valoraciones y verificaciones.
- **6.12 Aprobación**: dependiendo del tipo de mantenimiento de una SM, existen procedimientos formales que detallan el tipo de aprobación que el mantenedor debe obtener antes y después de realizar la modificación.
- **6.13 Realización de las modificaciones**: para realizar las modificaciones, el mantenedor utiliza la misma metodología establecida para el proceso de desarrollo del software adaptada al proceso de mantenimiento.
- **6.14 Actualización de la documentación**: la documentación (informes técnicos, manuales, etc.) afectada por una SM es actualizada después de realizada la modificación.