Objetivos de Control para la Auditoría del Proceso de Mantenimiento del Software

Francisco Ruiz,

Mario Piattini,

Macario Polo

Ponente: Francisco Ruiz

Grupo Alarcos - Dep. de Informática

Escuela Superior de Informática – Universidad de Castilla-La Mancha

Ronda de Calatrava, 7 – 13071, Ciudad Real (España)

tlf: 34-926-295300; fax: 34-926-295354

{fruiz, mpiattin, mpolo}@inf-cr.uclm.es

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

EVENTO:

V SEMINARIO IBEROAMERICANO DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Temática:

Auditoría Informática

Resumen:

En este documento presentamos una propuesta de objetivos de control para la auditoría del proceso de mantenimiento del software. Esta propuesta está basada en los estándares oficiales (ISO 12207, ISO 14764) y en la metodología CobiT para la auditoría de sistemas de información propuesta por la ISACF (Information Systems Audit and Control Foundation). El trabajo se enmarca dentro de los proyectos MPM [1] y MANTIS cuyo objetivo general es construir un marco metodológico y unas herramientas para abordar el mantenimiento del software de forma general e integrada.

1. Introducción

Múltiples estudios señalan que el mantenimiento es la parte más costosa del ciclo de vida del software (CVS). Estadísticamente está comprobado que el coste de mantenimiento de un producto software a lo largo de toda su vida útil supone más del doble que los costes de su desarrollo. La tendencia es creciente con el paso del tiempo y, en general, el porcentaje de recursos necesarios para mantenimiento se incrementa a medida que se produce más software [Hanna, 1993].

Una causa directa de los grandes costes del mantenimiento del software (MS) es que el coste relativo de reparar un defecto aumenta considerablemente en las últimas etapas del CVS [Piattini et al, 1998], de forma que la relación entre el coste de detectar y reparar un defecto en la fase de análisis de requisitos y en la fase de mantenimiento es de 1 a 100 respectivamente (ver figura 1).

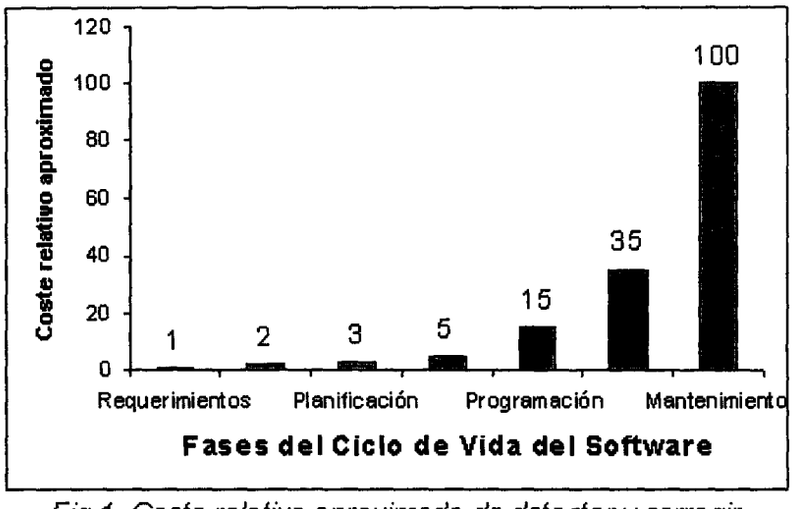


Fig 1. Coste relativo aproximado de detectar y corregir defectos

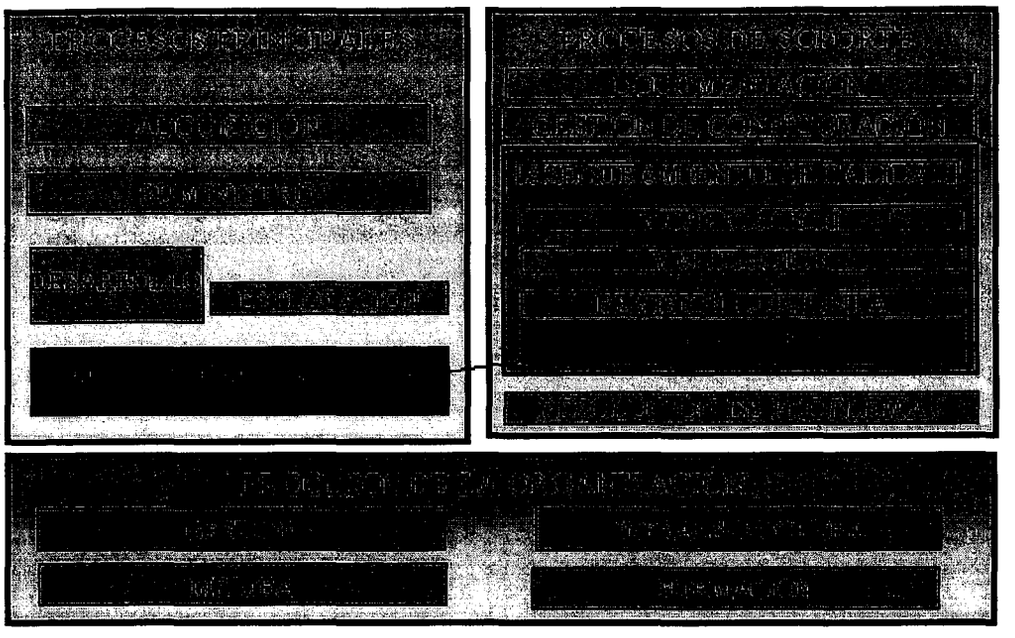
Un coste indirecto del MS es la reducción que se produce en la productividad. Algunos autores [Pigoski, 1996] han calculado reducciones de la productividad -medida en líneas de código (LDC) por persona y mes- de 40 a 1, es decir, el coste de mantener una línea de código puede llegar a ser 40 veces más alto que en el proceso de desarrollo.

A la vista de la importancia del MS (en términos económicos y de recursos consumidos), parece necesario que se tenga especialmente en cuenta al realizar auditoría de sistemas de información (ASI) y, especialmente, cuando se trata de auditar los procesos para producir y poner en producción los productos software. Frente a esta evidencia, la realidad es que hasta ahora el MS casi no ha sido considerado en los procedimientos y normas establecidos para la ASI.

Entre otras posibles causas de esta situación, creemos que se encuentra el hecho de que es muy reciente la atención prestada al MS desde el mundo de la ingeniería del software. Prueba de ello es que los estándares internacionales para el proceso de mantenimiento del software (PMS) tienen muy pocos años [IEEE, 1993] o acaban de elaborarse [ISO/IEC, 1998] y que casi no existen metodologías para abordar las particularidades que dicho proceso tiene respecto del proceso de desarrollo de software [Polo et al, 1999].

En este trabajo presentamos una propuesta para la Auditoría del proceso de mantenimiento del software (PMS) que toma como punto de partida la arquitectura de procesos del ciclo de vida del software definida en el estándar ISO 12207 [ISO/IEC, 1995]. En este estándar, el MS

y la auditoría son dos procesos definidos. El MS es uno de los cinco procesos principales (junto con la adquisición, el suministro, el desarrollo y la explotación), mientras que la auditoría es uno de los ocho procesos de soporte (ver figura 2).



A continuación nos centramos en el segundo (la auditoría) como soporte o herramienta de control para el primero (el MS). Para ello, en los apartados 2 y 3 se presentan los conceptos y marcos utilizados:

- Para el proceso de mantenimiento del software: el estándar ISO 14764 [ISO/IEC, 1998], y
- Para la auditoría de sistemas de información: la metodología CobiT [ISACF, 1998].

Después, en el apartado 4 se presenta la propuesta de adaptación de la metodología CobiT para cumplir con la norma ISO 14764. En el apartado 5 se detallan los objetivos de control propuestos para el PMS, y por último, en el apartado 6, concluimos realizando unas conclusiones y la exposición de trabajos actuales y futuros.

1. El Proceso de Mantenimiento del Software (PMS).

El PMS incluye las actividades y tareas cuyo objetivo es modificar un producto software existente y ya puesto en explotación preservando su integridad. Este proceso es activado cuando el producto software sufre modificaciones en el código o en la documentación asociada con el objetivo de:

- Localizar y eliminar defectos, normalmente detectados por un funcionamiento incorrecto (mantenimiento correctivo);
- Adaptar el software a cambios en el entorno operativo (hardware y/o software) (mantenimiento adaptativo);
- Mejorar o añadir nuevas funcionalidades requeridas por los usuarios (mantenimiento perfectivo); o
- Mejorar las propiedades del software (calidad, mantenibilidad, etc.) sin alterar las

especificaciones funcionales (mantenimiento preventivo).

El estándar ISO 14764 establece cuatro tipos de mantenimiento que coinciden con los cuatro objetivos anteriores. En algunas metodologías se amplían y precisan estos tipos de mantenimiento [Ruiz et al, 1999a] y se establecen diversos aspectos del PMS que deberemos tener en cuenta al planificar la auditoría de dicho proceso.

El PMS propiamente dicho consta de las actividades y tareas necesarias para modificar un producto software existente preservando su integridad (ver figura 3). Dichas actividades y tareas son responsabilidad del mantenedor.

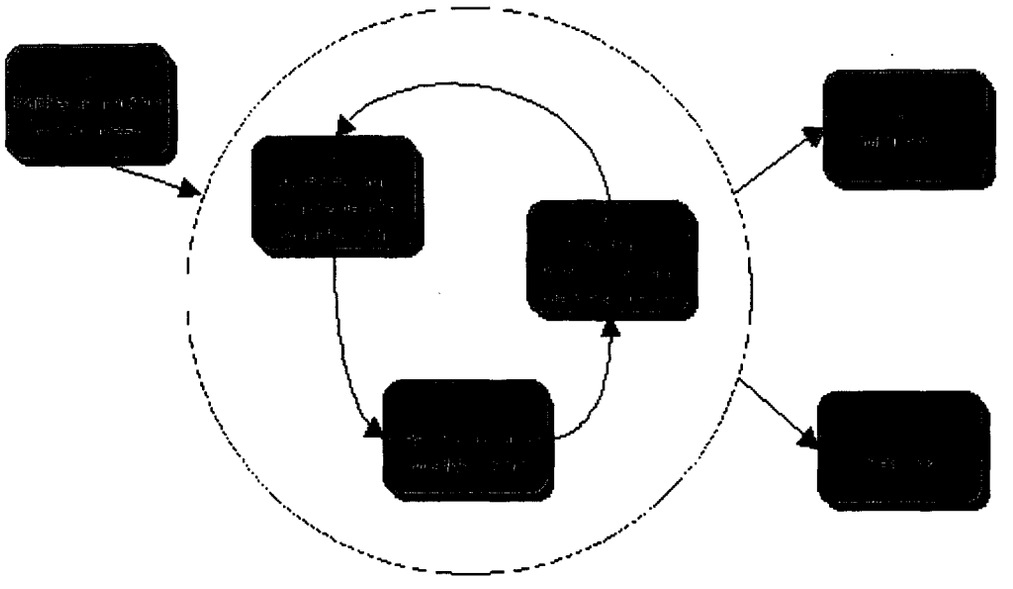


Fig 3. Actividades del Proceso de Mantenimiento del Software

1. La metodología CobiT para Auditoría de Sistemas de Información (ASI).

El sistema de información de una organización es único, aunque ciertos procesos se realicen de forma manual y otros mediante la informática. Por tanto, a la hora de realizar la auditoría, es necesario un enfoque que considere dicho sistema de información globalmente; es decir, que tenga en cuenta de manera conjunta, los procesos manuales y los informáticos. El auditor utilizará, en cada caso, las herramientas y los procedimientos más adecuados en función de la realización manual o informática de las actividades.

La propuesta CobiT [ISAFC, 1998] supone un paso, seguramente el más importante, en dicho camino. La filosofía de CobiT asimila los principios de la reingeniería de procesos de negocio (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 estructura (*framework*) de CobiT comienza a partir de una premisa simple y pragmática:

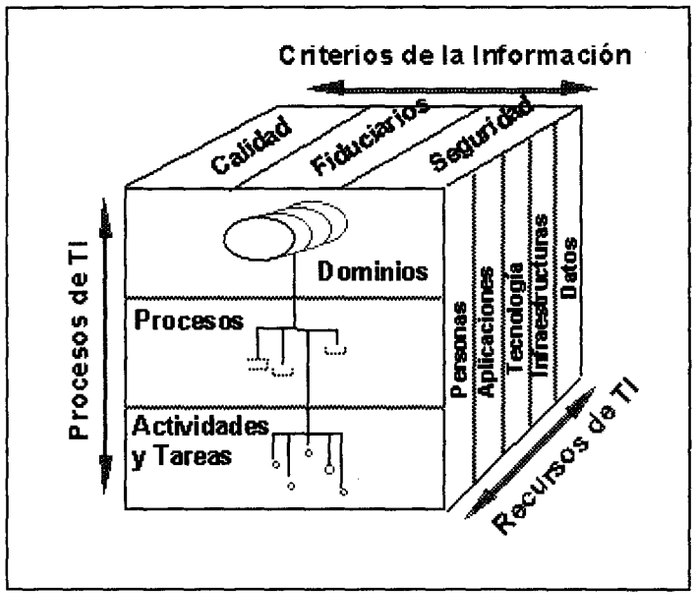
> *"Los recursos en Tecnologías de la Información y Comunicaciones (TIC) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".*

Para ello, se definen 34 objetivos de control generales (OCGs)[2], uno para cada uno de los procesos definidos. Estos procesos están agrupados en cuatro grandes dominios: planificación y organización, adquisición e implantación, suministro y soporte, y supervisión. Esta estructura cubre todos los aspectos de la información y de las tecnologías que le sirven de soporte [Peña, 1998].

Además, en la estructura de CobiT se destacan los efectos de los recursos en TIC (datos, aplicaciones, tecnología, instalaciones y personal) junto con los requisitos o criterios que debe satisfacer la información:

- Requisitos de calidad: calidad, coste, suministro;
- Requisitos fiduciarios [COSO, 1994]: efectividad y eficiencia de las operaciones, fiabilidad de la información, cumplimiento de las leyes y normas;
- Requisitos de seguridad: confidencialidad, integridad, disponibilidad.

En suma, la estructura conceptual se puede enfocar desde tres puntos de vista (ver figura 4):



1) Los recursos de las TIC,

2) Los criterios organizacionales de la información, y

3) Los procesos de las TIC.

Estas diferentes vistas permiten que se pueda acceder a la estructura de manera eficiente desde la óptica de interés de cada implicado: directivo, gestor de TIC, responsable de procesos, técnico en TIC o usuario.

1. Adaptación de CobiT al Proceso de Mantenimiento del Software.

Las fuentes bibliográficas más recientes dedicadas a la auditoría de sistemas de información [Weber, 1999], [Champlain, 1998], [Piattini y Peso, 1998] dedican muy poca o ninguna atención a la auditoría del MS. Ante esta situación, hemos estado trabajando en una propuesta que presentamos a continuación.

En CobiT, los 34 OCGs propuestos se concretan en 302 objetivos de control detallados (OCDs). En la metodología MANTEMA [Polo et al, 1999] hemos utilizado como punto de partida para la auditoría del PMS los siguientes objetivos de control (seleccionados y extraídos entre los 34 generales y los 302 detallados):

Dominio / Objetivos Generales / Objetivos Detallados:

AI - Adquisición e Implantación

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

DS - Suministro y Soporte

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

Además de los anteriores, existen otros objetivos de control generales y detallados que se relacionan fundamentalmente con el proceso de desarrollo de software, pero que

también son de aplicación al mantenimiento debido a que durante la actividad de realización de la modificación el mantenedor tiene que realizar algunas de las tareas típicas del desarrollo del software (análisis, diseño, codificación, prueba, etc.).

No todos los objetivos incluidos en la lista anterior tienen la misma importancia dentro del PMS (según se define en el estándar ISO 14764). El dominio en el que se incluyen la mayoría de las actividades del PMS es el de "Adquisición e Implantación". Dentro de este dominio, el OCD AI01.15 (Mantenimiento del software por terceros) pertenece realmente - a pesar del nombre- al proceso de adquisición, en este caso adquiriendo (contratando) el servicio de mantenimiento mediante externalización u 'outsourcing'. Como ya se ha dicho, el análisis de los objetivos detallados del OCG AI02 (Adquisición y mantenimiento de aplicaciones software) permite comprobar que, también a pesar de incluir la palabra mantenimiento en el nombre, no se corresponde realmente con el PMS salvo en el OCD AI02.2 (Cambios grandes en sistemas existentes) que se refiere a situaciones que requieren mucho mantenimiento adaptativo. El OCD AI05.3 (Conversión) está relacionado con la actividad de migración dentro del PMS.

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

Tabla 1. Objetivos de Control de la Gestión de Cambios vs Actividades del PMS.

En realidad, dentro del dominio de "Adquisición e Implantación", el OCG que realmente está asociado al PMS es el AI06 (Gestión de cambios). Todos los OCDs que lo integran están directamente asociados con las actividades del PMS. En la tabla 1 se muestran los siete OCDs de la 'Gestión de cambios' junto con las actividades del PMS relacionadas. No aparece la actividad de 'migración' porque dicha actividad se produce sólo en el caso de mantenimiento adaptativo (OCD AI02.2 ya comentado). Tampoco aparece la actividad de retirada porque no se puede considerar directamente relacionada con la gestión de cambios.

En el dominio de Suministro y Soporte, el OCG DS09 (Gestión de la configuración) está directamente relacionado con el PMS, pero se corresponde con el proceso del mismo nombre definido en la norma ISO 12207 como uno de los procesos de soporte. Por tanto, no debe ser tenido en cuenta en para el proceso de mantenimiento.

2. Propuesta de Objetivos de Control para el PMS.

Todas estas disfunciones se deben, fundamentalmente, al diferente modelo de procesos utilizado por CobiT y por los estándares ISO 12207 y 14764. Por esta razón, en la versión 2.0 de la metodología MANTEMA [Ruiz et al, 1999b], para poder utilizar la propuesta CobiT de manera coherente con el PMS propuesto por ISO, se propone modificar la lista de OCGs sustituyendo el AI06 'Gestión de cambios' por 'Gestión del proceso de mantenimiento del software', en el cuál se incluyen también los OCDs AI02.2 (Cambios grandes en sistemas existentes) y AI05.3 (Conversión) por las razones ya comentadas. Además, los OCDs del OCG AI06 se reestructuran en función de las actividades y tareas del PMS en ISO 14764.

La gestión del PMS pasa a ser un objetivo de control general 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. La lista siguiente muestra los 14 objetivos de control detallados propuestos.

Dominio: Adquisición e Implantación

Objetivo General : AI06 - Gestión del proceso de mantenimiento del software

Requisito del negocio: *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 Detallados:

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.

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.

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.

4. Acuerdo de mantenimiento: las relaciones entre el mantenedor[3] y el cliente y las obligaciones de cada uno están establecidas en un acuerdo o contrato de mantenimiento.

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. 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.

7. Procedimientos para solicitudes de modificación (SM): existen procedimientos normalizados para iniciar, recibir y registrar SMs.

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.

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.

10. Verificación de los problemas: el mantenedor replica o verifica que realmente existe el problema que originó la SM.

11. Registro de las SMs: el mantenedor documenta y registra las SMs, con sus análisis, valoraciones y verificaciones.

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.

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.

14. Actualización de la documentación: la documentación (informes técnicos, manuales, etc.) afectada por una SM es actualizada después de realizada la modificación.

En conclusión: el objetivo de control general propuesto busca que la gestión del proceso de mantenimiento del software que realiza la organización auditada permita que las actividades del negocio se realicen sin interrupciones imprevistas y que el software de los sistemas de información existentes se adapte a las nuevas necesidades; teniendo en consideración los cambios en el entorno operativo, cómo se hace la retirada del software, los tipos de mantenimiento, ...

Para cualquier organización que tenga responsabilidades de mantenimiento de algún producto software, ya sean internas (un departamento de la propia organización es el responsable del mantenimiento) o externas (el servicio se ofrece a otra organización diferente), los objetivos de control propuestos se pueden utilizar al estilo de una lista de comprobación o 'check-list'. Por ejemplo, si se utiliza la metodología general de Auditoría de Sistemas de Información propuesta por [Weber, 1999], los 14 objetivos de control anteriores serán útiles en las tareas siguientes:

- Estimación de la calidad de los controles implementados sobre el PMS; y
- Comprobación de que los controles sobre el PMS son realmente cumplidos en todos los sitios donde se realiza el mantenimiento.

Los auditores deberán ser cuidadosos de no centrarse exclusivamente en la seguridad e integridad de datos (los dos aspectos más frecuentes en la ASI), ya que en el caso del PMS, la gran cantidad de recursos consumidos habitualmente en las actividades de mantenimiento, obliga a los auditores a considerar también la efectividad y eficiencia con que cada actividad de mantenimiento es realizada por cada mantenedor.

1. Conclusiones y trabajos pendientes.

El mantenimiento es la fase más costosa de todo el ciclo de vida del software. Por esta razón, es importante que desde el ámbito de la auditoría de sistemas de información se le dedique la atención que merece. Con este objetivo, presentamos una propuesta para abordar la auditoría del proceso de mantenimiento del software basada en:

- El estándar ISO 14764 para el proceso de mantenimiento del software, y
- La metodología CobiT para la auditoría de sistemas de información.

En dicha propuesta hemos realizado un análisis de todos los objetivos de control incluidos en CobiT y hemos seleccionado los que tienen relación con el proceso de mantenimiento del software. La lista resultante la hemos cambiado definiendo un objetivo de control general llamado 'Gestión del proceso de mantenimiento del software'. Este objetivo general lo hemos precisado en 14 objetivos de control detallados que modifican y amplían considerablemente los incluidos en CobiT.

Con esta propuesta establecemos un marco formal (en el cual la auditoría es uno de los procesos de soporte al proceso de mantenimiento) que hemos incluido como parte de la versión 2 de la metodología MANTEMA para la gestión integral del mantenimiento del software.

Los resultados obtenidos están siendo validados en entornos reales de mantenimiento de grandes proyectos software mediante la colaboración de la empresa Atos ODS, una de las principales compañías europeas en el campo de la externalización y *'outsourcing'* de servicios informáticos. Los comentarios y sugerencias obtenidos serán utilizados para mejorar la lista de objetivos de control, para cambiar sus descripciones y para elaborar una colección de técnicas de control útiles para detectar si se satisface cada objetivo de control.

1. Referencias.

[Champlain, 1998] Champlain, J., Auditing Information Systems. A Comprehensive Reference Guide. John Wiley & Sons. USA, 1998.

[COSO, 1994] Commitee of Sponsoring Organizations oh the Treadway Commison. *Internal Control - Integrated Framework* . American Institute of Certified Accountants. New Jersey, USA 1994.

[Hanna, 1993] Hanna, M., Maintenance "Burden Begging for a Remedy". *Datamation,* abril 1993, pp. 53-63.

[IEEE, 1993] IEEE, std 1219: *Standard for Software Maintenance*. IEEE Computer Society Press. USA, 1993.

[ISACF, 1998] ISACF, CobiT: Governance, Control and Audit for Information and Related Technology, 2nd edition. Information Systems Audit and Control Foundation. USA, 1998.

[ISO/IEC, 1995] ISO/IEC 12207: *Information Technology – Software life cycle processes*. ISO/IEC JTC1/SC7 Secretariat. Canadá, 1995.

[ISO/IEC, 1998] ISO/IEC 14764: *Software Engineering – Software Maintenance*. ISO/IEC JTC1/SC7 Secretariat. Canadá, 1998.

[Peña, 1998] Peña, E., Objetivos de Control y Estructura de CobiT. JAI'98, *I Jornadas de Auditoría Informática* . Grupo Alarcos (editores). Ciudad Real, España 1998.

[Piattini et al, 1998] Piattini, M. G., Ruiz, F., Polo, M., Villalba J., Fernández, I., Bastanchury, T. y Martínez, M.A., Mantenimiento del Software. Conceptos, métodos, herramientas y outsourcing. Ed. Ra-Ma. Madrid, España 1998.

[Piattini y Peso, 1998] Piattini, M., del Peso, E., Auditoría Informática. Un enfoque práctico. Ed. Ra-Ma. Madrid, España 1998.

[Pigoski, 1996] Pigoski, T. M., Practical Software Maintenance. Best Practices for Managing Your Investment. Ed. John Wiley & Sons. USA, 1996.

[Polo et al, 1999] Polo, M., Piattini, M., Ruiz, F., Calero, C. MANTEMA: A Complete Rigorous Methodology for Supporting Maintenance based on the ISO/IEC 12207 Standard. CSMR'99, *Third European Conference on Software Maintenance and Reengineering*. IEEE Computer Society Press. Amsterdam, Holanda 1999.

[Ruiz et al, 1999a] Ruiz, F., Piattini, M., Polo, M., Calero, C. Maintenance Types in the MANTEMA Methodology. ICEIS'99, *First International Conference on Enterprise Information Systems* . Setúbal, Portugal 1999.

[Ruiz et al, 1999b] Ruiz, F., Piattini, M., Polo, M., y Calero, C., Propuesta de un Marco Formal para la Auditoría del Proceso de Mantenimiento del Software. CIICC'99, *VI Congreso Internacional de Investigación en Ciencias Computacionales*. Cancún, México 1999.

[Weber, 1999] Weber, R., Information Systems Control and Audit. Prentice-Hall. USA 1999.

Notas

1 El proyecto MPM (Mejora del Proceso de Mantenimiento) está financiado por la empresa Atos ODS y por el Ministerio de Industria y Energía de España (iniciativa ATYCA, TA15/1999). El proyecto MANTIS está financiado por la Unión Europea (CICYT 1FD-1997-1698TIC).

2 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 TIC* ".

3 El mantenedor y el cliente (propietario o usuario del software mantenido) pueden pertenecer a la misma organización.