AUDITORÍA INFORMÁTICA DEL DESARROLLO DE APLICACIONES

Darío Usamentiaga[1], Isabel Sevilla[2], Javier Tuya[2]

[1]*Escuela Técnica Superior de Ingenieros Industriales e Ingenieros Informáticos de Gijón*
e-mail: zz98f049@opalo.etsiig.uniovi.es

[2]*Universidad de Oviedo. Departamento de Informática*
e-mail: [sevilla|tuya]@lsi.uniovi.es

RESUMEN: Este trabajo pretende continuar con la auditoría llevada a cabo el pasado año, de los trabajos realizados para la asignatura de "Ingeniería del Software" de 3°. En el nuevo estudio realizado son auditados todos los proyectos entregados por los alumnos de 4° curso de la Escuela Técnica Superior de Ingenieros Industriales e Ingenieros Informáticos para la asignatura de Ingeniería del Software I, en un ámbito de desarrollo más similar al de una organización de desarrollo. Los proyectos son realizados por equipos formados por alumnos, los cuales tienen por usuarios y equipos de aseguramiento de calidad a distintos alumnos de "Ingeniería del Software II" (de 5° curso). Los directores de los proyectos son los profesores responsables de las asignaturas. Para el desarrollo del ciclo de vida de los proyectos software, se sigue un Manual de Procedimientos que define el proceso de desarrollo y adapta la metodología Métrica Versión 2.1 al entorno en que se realizan los proyectos

1.- INTRODUCCIÓN.

La auditoría de los sistemas de información se define como "el conjunto de Procedimientos y Técnicas para evaluar y controlar total o parcialmente un sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente" [ACHA1994, p. 21]. En resumen, un estudio metódico con vistas a mejorar la rentabilidad, seguridad y eficacia.

Los objetivos fundamentales de la auditoría que da lugar a esta comunicación son, en primer lugar, comprobar el grado de comprensión alcanzado por los alumnos de la metodología utilizada, y la obtención de una práctica adecuada en el desarrollo software. Por otra parte, se evalúa la adecuación del Manual de Procedimientos seguido, así como las normas establecidas por los responsables de la asignatura y la estructura fijada durante el curso.

2.- METODOLOGÍA ISACA

Para la realización de la auditoría se ha utilizado la metodología propuesta por la ISACA™ (*Information Systems Audit and Control Asociation*) [ISAC2000]. Es la asociación que se ha instituido para desempeñar el papel de fuente central coordinadora de estándares de prácticas de control para tecnologías de información. Sus actividades de estándares establecen una base de calidad según la cual se miden las actividades de auditoría y de control. La ISACA ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información y éstas son las que se han seguido.

3.- TÉCNICA UTILIZADA.

En cuanto a las herramientas que son utilizadas, la principal son los Objetivos de Control [PALA1990]. Estos objetivos de control, deben ser coherentes con la metodología utilizada, además tienen que ser específicos y muy completos de acuerdo con el tipo de auditoría que se realice. Como en este caso la auditoría es de Desarrollo de Aplicaciones, se sigue el Manual de Procedimientos [TUYA1999] para las fases de Análisis, que tiene como guía la metodología Métrica versión 2.1, y para las fases de Diseño e Integración nos basaremos principalmente en la metodología Métrica [MAP1995] debido a que el Manual en estas fases es una síntesis de ella. Un ejemplo, tanto del Manual de Procedimientos como de los Objetivos de Control, se puede ver en la Figura 1 y en la Figura 2, respectivamente.

1.2.2.3. Tarea T.RTF-ARS Revisión Técnica Formal del ARS
Revisión técnica formal del ARS. La revisión se realizará de forma independiente por parte del EGC y del USR. Una vez entregado el documento de revisión tendrá lugar una reunión conjunta de revisión con todos los integrantes del proyecto.
Para la segunda versión del ARS 1se realizará otra revisión para comprobar si todos los problemas encontrados han sido resueltos y/o se han introducido nuevos defectos. En esta ya no participará el USR y no existirá reunión de revisión

Procedimientos asociados	*Productos*
I.ERTF Elaboración de una Revisión Técnica Formal I.RRCR Realización de Reuniones Conjuntas de Revisión	D.ARS-HCR Hoja de Comentarios de Revisión del ARS D.ARS-HCU Hoja de Comentarios de Usuario del ARS D.ARS-LAC Lista de Acciones Correctivas del ARS

Figura 1. Ejemplo del Manual de Procedimientos

- **CONTROL B3-2**: Se debe especificar el modelo lógico de datos del nuevo sistema identificando las entidades de datos implicadas y las relaciones existentes entre ellas. Se debe comprobar que:

  1. Existe el modelo lógico de datos del sistema a desarrollar.
  2. El modelo lógico de datos está normalizado al menos en 3ª forma normal.
  3. Existe una descripción de las claves de acceso a las entidades, así como de los atributos característicos de las entidades definidas.
  4. Existe un catálogo de entidades.
  5. Son especificadas las relaciones entre las entidades y los almacenes.

Figura 2. Ejemplo de Objetivos de Control

4.- FASES.

Como ya se indicó anteriormente, se auditan los trabajos presentados en el año 1998/99 para la asignatura de Ingeniería del Software de 4º de la Escuela Técnica Superior de Ingenieros Industriales e Informáticos de Gijón (Universidad de Oviedo). Estos trabajos o proyectos son realizados por equipos de desarrollo formados por grupos de alumnos de la asignatura. Concretamente se trata de 16 equipos, formados por grupos de entre 5 y 8 alumnos, los cuales desarrollaron un proyecto por cada equipo. Los usuarios de dichos trabajos son alumnos de Ingeniería del Software II de 5º de la misma escuela, quienes propusieron dichos proyectos. Todos ellos fueron revisados por equipos de calidad compuestos también por alumnos de esta misma asignatura. Los directores de los desarrollos son los profesores responsables de la asignatura.

Los equipos de desarrollo deben realizar al menos dos versiones para las etapas de Análisis de Requisitos del Sistema y de Especificación Funcional del Sistema dentro de la fase de Análisis. Para la fase de Diseño deben entregar al menos una versión de los 4 documentos asociados al Diseño de los Componentes del Sistema y para finalizar un documento de Integración. Las pruebas de Integración son realizadas por los equipos de calidad. Entre cada una de las versiones entregadas se realizan los cambios necesarios que los equipos de garantía de calidad estiman oportunos. Al final del curso, deben entregar todo el desarrollo del proyecto integrado con todos lo cambios realizados y actualizados. Todo ello está planificado de antemano en el Manual de Procedimientos que deben seguir para la realización de los trabajos.

a) Estudio inicial

El alcance de este estudio es auditar todas las fases del ciclo de vida de los proyectos software desarrollados. Esto implica, por lo tanto, la auditoría del Análisis, Diseño, Construcción e Implantación de los distintos sistemas. También son auditados los documentos entregados en cada fase en cuanto a su forma y aspecto. Las pautas a seguir a este respecto, así como las distintas entregas en formato electrónico y las fechas de entrega, se encuentran debidamente contempladas y documentadas en el Manual de Procedimientos.

Los objetivos fundamentales para la realización de la presente auditoría son:

- La comprensión por parte de los alumnos de las metodologías existentes en la actualidad y la obtención de la práctica suficiente en el campo del desarrollo software y de proyectos.

- En segundo lugar, comprobar la corrección de las normas establecidas por los responsables de la asignatura de Ingeniería del Software I en la Escuela así como la estructura fijada de la asignatura durante el curso y la adecuación del Manual de Procedimientos seguido.

b) Actividad del auditor

Describimos en este apartado las acciones propias de la auditoría, en donde se especifican las técnicas concretas que han sido utilizadas y las herramientas de que nos servimos. Como ya mencionamos previamente, la técnica utilizada son la definición de los objetivos de control necesarios y suficientes para abarcar todo el ciclo de vida de los proyectos. El trabajo de campo consiste en analizar el cumplimiento íntegro de todos los objetivos de control definidos sobre las aplicaciones estudiadas, proporcionándonos una serie de indicadores sobre lo bueno o lo malo que la docencia suministra acerca de la Ingeniería del Software, además de identificar posibles carencias en los temas tratados en los cursos de 4º y 5º de la Escuela.

c) Redacción de informes

La función auditora se materializa con la entrega de los informes finales correspondientes, exclusivamente por escrito y avalando personalmente el juicio del auditor de forma documental. Esta es la única referencia constatable de toda la auditoría y el exponente de su calidad. En este informe se pone de manifiesto la situación actual, las tendencias, los puntos débiles y amenazas encontradas, las recomendaciones y planes de acción correspondientes. Es importante destacar, que el auditor sólo debe incluir los hechos importantes y consolidados. El destinatario final del informe es el cliente promotor de la auditoría, que en este caso es Isabel Sevilla, coautora de este estudio.

5.- RESULTADOS

Los resultados obtenidos en la propia auditoría son muy satisfactorios para el alumnado en cuanto al desarrollo software de proyectos informáticos. Los alumnos adquieren un alto conocimiento de la metodología Métrica versión 2.1 así como una gran experiencia en el desarrollo de aplicaciones y proyectos software. Han sido comprobados un total de 278 Objetivos de Control de los cuales el 67,96 % se han cumplido, el 10,86 % No se han cumplido y el 21,18 % no han podido ser aplicados debido a no estar contemplados en el Manual de Procedimientos seguido.

Como se puede observar en la Tabla 1, los resultados para la fase de Análisis son bastante buenos, mientras que para las fases de Diseño e Integración los resultados no son tan satisfactorios, debido al alto número de objetivos de control No Aplicables.

	Objetivos de Control Estudiados	Porcentaje de Objetivos Cumplidos	Porcentaje de Objetivos No Cumplidos	Porcentaje de Objetivos No Aplicables
ARS	55	87,27 %	12,73 %	0 %
EFS	65	91,15 %	8,85 %	0 %
DTS	46	54,08 %	4,62 %	41,30 %
DCS	43	69,04 %	17,01 %	13,95 %
DPU	30	51,25 %	15,42 %	33,33 %
PIA	39	54,97 %	6,57 %	38,46 %

Tabla 1. Resumen de los resultados obtenidos para cada fase del desarrollo

Este buen resultado seguramente es fruto del entorno en el que se desarrollan dichos proyectos, ya que por una parte son aleccionados en las clases de teoría por los responsables de la asignatura de Ingeniería del Software, y por otra parte, son guiados y evaluados por los directores de proyecto, y como complemento, aprenden de sus propios errores gracias a las revisiones de los equipos de garantía de calidad. Todo ello se puede decir que forma una estructura bastante bien definida para garantizar un alto grado de aprendizaje en las asignaturas de Ingeniería del Software.

Otro aspecto relevante encontrado es la buena aceptación por parte de los alumnos en lo que se refiere al seguimiento del Manual de Procedimientos existente para la realización de los trabajos. Aunque inicialmente les resulta algo confuso en cuanto a su estructura y contenido, una vez que se acostumbran a su uso y lo utilizan más frecuentemente, se convierte en una herramienta muy potente, que sirve como guía y apoyo para sus desarrollos. De esta forma, los alumnos se han acostumbrado perfectamente a la realización de proyectos reales con una planificación inicial bastante estricta en

cuanto a plazos de entrega, a documentos realizados y entregados, y a las distintas versiones realizadas para cada fase del desarrollo.

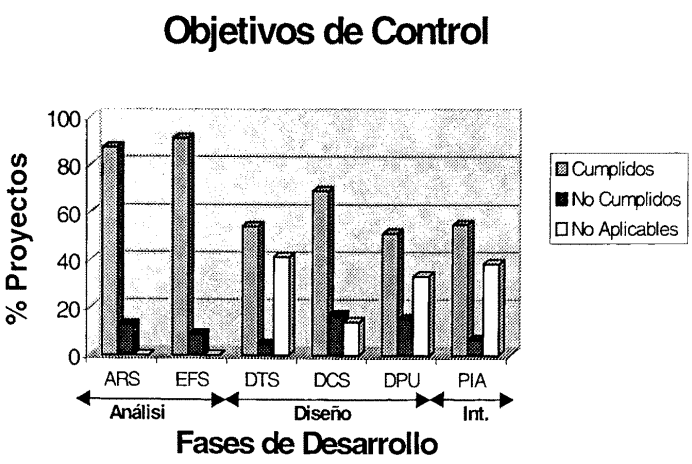

Figura 3. Resumen de Objetivos de Control estudiados para cada fase

A continuación se presenta un gráfico resumen, Figura 3, de la media de objetivos de control alcanzados satisfactoriamente para cada una de las fases del ciclo de vida del desarrollo de los 16 proyectos, tomando este valor como el 100%.

Como se puede observar en la Figura 3, los resultados obtenidos por los alumnos en la fase de Análisis son muy satisfactorios. En cuanto a la fase de Diseño e Integración, los resultados no son tan favorables. Además se puede comprobar que el Manual de Procedimientos se aleja levemente de la metodología Métrica en la fase de Diseño e Integración, como se puede observar por los objetivos de control con resultado "No Aplicable". Esto supone un riesgo evidente en el desarrollo de estos proyectos para dichas fases. Un ejemplo de la carencia de algunos aspectos importantes son los riesgos que provienen de no realizar un completo análisis del Modelo Físico de Datos o del Entorno Tecnológico de desarrollo, pudiendo provocar graves inconsistencias para el nuevo sistema.

Se debería mejorar realizando una actualización del Manual de Procedimientos, de forma que se incluyan estos apartados importantes en las fases de Diseño e Integración para asegurar el correcto funcionamiento del producto final.

6.- CONCLUSIONES.

Una vez concluidas las fases descritas anteriormente, podemos recoger e interpretar los resultados obtenidos tras la realización del trabajo de campo al aplicar el conjunto de objetivos de control a los proyectos estudiados de los alumnos.

Una primera reflexión personal que se extrae de la realización de la auditoría es la dificultad que conlleva esta actividad en cuanto a la obtención de resultados lo más eficientes posibles.

Un reto inicial es la realización de buenos cuestionarios de control, que incluyan todos los posibles casos y aspectos y que sean lo más completos posibles sin redundar en el estudio realizado. Este punto es muy importante porque de él dependen en gran medida los resultados que se puedan extraer, repercutiendo a su vez en las decisiones que se puedan tomar. Por ello, la fase de definición de objetivos de control y del trabajo de campo de cada una de las fases del desarrollo de proyectos, se ha tenido que realizar casi en paralelo ya que siempre aparecen nuevos objetivos a ser auditados, lo que se traduce en una revisión constante y refinamiento continuo de los cuestionarios.

Otra dificultad supone la propia interpretación que se dé a los distintos puntos que componen los proyectos estudiados a la hora de evaluar el conjunto de controles definidos. Es muy importante que el auditor tenga un alto grado de conocimiento general y de experiencia en el campo del desarrollo software.

7.- REFERENCIAS

[PALA1990] Palao, Manuel, *Objetivos de Control*, Ed. The EDP Auditors Foundation. Illinois, 1990

[ACHA1994] Acha Iturmendi, J.J., *Auditoría Informática en la empresa*, Ed. Paraninfo, 1994

[MAP1995] Ministerio para las Administraciones Públicas, Metodología de planificación y desarrollo de sistemas de información MÉTRICA,Versión 2.1, Ed. Tecnos, 1995.

[TUYA1999] Tuya, Javier, "Manual de Procedimientos para las prácticas de Ingeniería del Software I y II", http://opalo.etsiig.uniovi.es/~tuya/is/procedimientos/index.html, (accedido el 30-05-2000)

[ISAC2000] ISACA, The Information Systems Audit and Control Association & Foundation, http://www.isaca.org (accedido el 30-05-2000)