AUDITORÍA INFORMÁTICA DEL DESARROLLO DEL SOFTWARE

Marta Hermida[1], Isabel Sevilla[2]

[1]*E.T.S.I.I.I.G. (Escuela Técnica Superior de Ingenieros Industriales e Informáticos de Gijón.)*
e-mail: ***hermida@lsi.uniovi.es***

[2]*E.T.S.I.I.I.G. (Escuela Técnica Superior de Ingenieros Industriales e Informáticos de Gijón.)*
e-mail: ***sevilla@lsi.uniovi.es***

Resumen: En esta comunicación se presenta una experiencia piloto llevada a cabo en el marco de la asignatura de "Ingeniería del Software II", perteneciente al segundo ciclo de la Escuela Técnica Superior de Ingenieros Industriales e Informáticos de Gijón, y más concretamente en lo referente al tema de su programa relativo a la Auditoría Informática. Consiste en una auditoría del desarrollo del software sobre las prácticas presentadas para la asignatura "Ingeniería del software" del tercer curso de la Escuela Técnica Universitaria de Ingeniería de Gestión y Sistemas. Su finalidad es comprobar el grado de asimilación de conceptos que ha tenido el alumnado tras recibir un año completo de clases sobre dicha disciplina.

Para efectuar el trabajo se ha realizado en primer lugar un estudio teórico sobre la auditoría en base al cual se desarrollarán posteriormente las diferentes fases de la misma y cuya finalidad es chequear la corrección del desarrollo del software en todas sus fases (análisis de requisitos, especificación funcional, etc). Finalmente, se describen algunos de los resultados obtenidos sobre sistemas desarrollados por el alumnado.

1.- INTRODUCCIÓN.

Teniendo en cuenta que la informática va a ser el soporte tecnológico de todo el sistema de información de la empresa y que ésta es fundamental para la toma de decisiones habrá que auditarla. Así pues, la auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean fiables y con un buen nivel de seguridad. Por ello ya es considerada un factor de interés monetario que puede influir enormemente en la correcta evolución de la empresa.

También se podría justificar su existencia por los tres puntos siguientes:

- Para controlar los riesgos y problemas inherentes a la actividad informática.
- Para la protección de las fuertes inversiones: se trata de salvaguardar las grandes inversiones en informática que hacen hoy en día las empresas.
- Como apoyo a la auditoría financiera, ya que la elevada automatización de las tareas de las empresas hoy en día hace que se pierda fácilmente el control sobre determinadas acciones financieras (transferencias bancarias por ejemplo) y es preciso llamar a especialistas para que colaboren en la parte informatizada.

2.- FASES.

Dado el enorme campo a cubrir en toda auditoría, ésta se realiza siguiendo una planificación previa. Así pues, se siguen una serie de fases que intentan cubrir la mayor parte posible de la disciplina a auditar.

a) Trabajo previo

Un primer paso es situarse en el entorno a auditar, y según el mismo establecer un programa a seguir para efectuar el trabajo.

- Planificación general: Para llevar a cabo correctamente una auditoría ésta debe ser planeada totalmente con anterioridad. En el caso práctico que nos ocupa se ha realizado una planificación general estableciéndose en la misma un código anónimo para cada proyecto (con el fin de salvaguardar la identidad de sus autores). Además se han fijado

responsabilidades, se ha realizado un análisis de los objetivos a cubrir así como su alcance y marco temporal/económico.

- Revisión general del control interno: Revisar la forma de funcionamiento de la empresa.
- Programa de trabajo: Establecer qué conocimientos y recursos son necesarios, las fuentes de información, centros y áreas a auditar por prioridad según riesgo/objetivos y los pasos a seguir en la auditoría. En este experimento se han tenido en cuenta básicamente los manuales de Metrica V.2.

b) Trabajo de campo

Este paso constituye la ejecución de las pruebas y análisis realizados por el auditor.

- Pruebas de cumplimiento, en las que se determina si el sistema de control interno funciona adecuadamente según las políticas, los procedimientos de la entidad, etc.
- Pruebas sustantivas, para verificar todo lo anterior. Para ello se debe planificar y determinar el tamaño de la muestra para obtener suficiente evidencia y que el auditor se forme un juicio. Existen múltiples técnicas y herramientas para realizar las pruebas sustantivas, como pueden ser cuestionarios, entrevistas, flujogramas, utilidades, tomas instantáneas, codificación incrustada, etc.

Para el caso práctico que nos compete se ha fijado un tamaño de muestra que pudiese cubrir tanto trabajos de distintas convocatorias como de las distintas carreras (gestión y sistemas) para así poder establecer a posteriori si existen diferencias entre ellos a la hora de cumplir las fases de desarrollo del software. Para efectuar la auditoría se han empleado básicamente cuestionarios, puesto que es considerada la técnica más útil para auditores no experimentados. Dichos cuestionarios se han elaborado en base a los objetivos de control de la ISACA (Information Systems Audit and Control Association).

c) Fase de informe

Finalmente hay que realizar una valoración por escrito de la situación, indicando las debilidades de control interno, riesgos y posibles mejoras. A lo largo de la auditoría se van realizando dos informes, uno inicial (informe

borrador) y otro final (definitivo) tras haberlo discutido con los auditados. De cada auditoría realizada para este experimento se ha escrito un informe que tiene carácter de borrador ya que no se consideró factible reunir a los alumnos autores de los proyectos (de los que una gran parte ha terminado ya la carrera) para así poder hacer un informe definitivo. En cualquier caso dichos informes constan de una valoración completa del sistema haciéndose las oportunas recomendaciones.

3.- CUESTIONARIOS EMPLEADOS.

Se ha elaborado un cuestionario en el que se chequean todos los aspectos concernientes a las fases de desarrollo de un producto software siguiendo la metodología Metrica V.2. Consta de un total de 365 cuestiones que intentan cubrir en la mayor medida posible tanto la corrección de cada fase del desarrollo como la corrección en el empleo de la metodología.

4.- RESULTADOS OBTENIDOS.

Tras aplicar el cuestionario a los trabajos del alumnado una de las primeras conclusiones sacadas es la dificultad que supone realizar una auditoría que detecte un alto porcentaje de los fallos. A medida que se va aplicando el cuestionario se localizan nuevos aspectos que no han sido chequeados mediante el mismo y por tanto se van refinando los check-list. Este hecho es de gran relevancia porque supone un trabajo constante de revisión y refinamiento de los cuestionarios, lo cual explica que cada auditor tenga los que ha desarrollado guardados con gran recelo ya que son el resultado de años de trabajo continuado.

Así pues, es importante reseñar que lo que hace bueno a un auditor es, por orden de importancia:

- Experiencia.
- Elevada intuición.
- Conocimientos teóricos sobre el tema.

En cuanto a los resultados obtenidos en la auditoría del desarrollo de los trabajos podría decirse que el nivel medio es bastante bueno. En este resultado puede haber sido determinante el sistema empleado en la asignatura de Ingeniería del Software de la Ingeniería Técnica Informática de Gijón para la organización de estas prácticas, ya que los alumnos

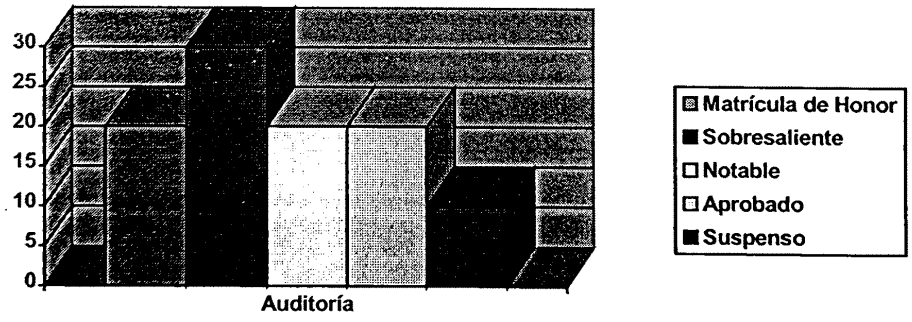
entregan el sistema tras haber recibido ayuda y asesoramiento de los profesores de la misma en horario de prácticas durante todo el curso. Este hecho redunda en beneficio de la calidad del desarrollo aunque la materialización del mismo sea competencia del alumnado.

Teniendo este hecho en cuenta, las conclusiones a que se han llegado han sido:

a) El nivel de los trabajos obtenido es bueno

El resultado obtenido de la auditoría se ha subdividido en las 5 calificaciones posibles. De tal forma que tras aplicarle el cuestionario a un trabajo se le clasifica en una de ellas en base a los resultados obtenidos en el mismo. Siguiendo este modo de trabajo, los resultados de la clasificación final han sido:

CALIFICACIÓN	PORCENTAJE
Suspenso	10 %
Aprobado	20 %
Notable	20 %
Sobresaliente	30 %
Matricula de Honor	20 %



No existe diferencia de calidad entre los trabajos de distintas convocatorias ni entre los de alumnos de Ingeniería Técnica de Informática de Gestión o Ingeniería Técnica de Informática de Sistemas.

b) La comparación con las notas otorgadas a dichos trabajos

Se han comparado las notas que se les otorgaron en su día a dichos trabajos con las que se obtuvieron tras esta auditoría del desarrollo del software y las calificaciones son muy similares lo que no hace sino dar mayor validez a la auditoría. En algún caso excepcional la auditoría ha sido algo más negativa de lo que lo fue la nota pero esto puede ser consecuencia de que el profesor de la asignatura haya tenido en cuenta también otros factores como el esfuerzo realizado por el alumno y su grado de interés por aprender.

c) A nivel empresarial interesa monetariamente realizar un buen desarrollo de los sistemas

Los sistemas peor puntuados han sido precisamente los que más costó auditar ya que no era tarea fácil llegar al entendimiento de qué tenía que hacer ese sistema dado el pésimo desarrollo del mismo. Además el informe final era bastante extenso al tener que mencionar las deficiencias del sistema y las recomendaciones para su mejora.

Estos mismos sistemas serían los menos mantenibles a posteriori ya que cualquier cambio en ellos conllevaría la necesidad de estudiar nuevamente el problema a fondo y las posibles soluciones al mismo, perdiéndose tiempo y dinero. Luego un buen desarrollo de un producto software interesa monetariamente ya que incrementa su calidad y mantenibilidad.

Invertir en un buen desarrollo del software es invertir en futuro.

5.- REFERENCIAS.

- Objetivos de control. Manuel Palao. The EDP Auditors Foundation. Illinois, 1990

- Auditoria Informática en la empresa. Juan José Acha Iturmendi. Editorial Paraninfo, 1994

- Auditoría Informática. Un enfoque práctico. Mario Piattini y Emilio del Peso. Editorial RA-MA, 1998