Reflexiones sobre la enseñanza de la Auditoría de Sistemas de Información en las escuelas de informática

Eduardo Fernández-Medina, Mario Piattini
Grupo Alarcos. Departamento de Informática.
Universidad de Castilla-La Mancha.
Paseo de la Universidad nº 4. 13071. Ciudad Real.
{eduardo.fdezmedina, mario.piattini}@uclm.es

Resumen

La auditoría de sistemas de información se está convirtiendo en un factor crucial para la sociedad, debido a la gran dependencia que las organizaciones tienen de sistemas que gestionen su información, y debido también a la necesidad derivada de verificar la calidad de los servicios ofrecidos por estos sistemas de información, así como la de garantizar una adecuada seguridad que consista en una correcta confidencialidad, integridad y disponibilidad de los datos que gestionan y que son uno de los activos más importantes de las organizaciones. En este artículo se hace un estudio de los principales currículos internacionales y de varias escuelas de informática para analizar cómo consideran la materia de auditoría de sistemas de información. Como presentamos en este artículo, la situación no es muy alentadora, y nos invita a otorgar un mayor peso a esta materia en la formación de profesionales de los sistemas de información.

1. Introducción

A pesar de que históricamente la auditoría ha sido siempre de *cuentas* (o *financiera*), la informática ha pasado a tomar un papel relevante en esta actividad, primero sirviendo como soporte automatizado para su realización, y después, precisamente para verificar el funcionamiento correcto, eficaz y eficiente de la informática, dando lugar a la *auditoría informática* (o de *sistemas de información*). En los últimos años, esta auditoria se está denominando, cada vez con más asiduidad, *Auditoría de Sistemas y Tecnologías de la Información y las Comunicaciones*.

En la actualidad es evidente que la información se ha convertido en uno de los activos principales de las organizaciones, representando en muchos casos su principal elemento estratégico para la realización de sus objetivos, y como soporte de su actividad. Las organizaciones invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información (de ahora en adelante SI) que les ofrezcan la mayor productividad y calidad posible. Es por eso que los temas relativos a la auditoría de sistemas de información (de ahora en adelante ASI) cobran cada vez más relevancia tanto a nivel internacional como nacional.

La ASI es el proceso sistemático de recoger, agrupar y evaluar evidencias para determinar si un SI salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos [9]. La ASI tiene como objetivo brindar a la Dirección de una organización, una opinión independiente y una seguridad razonable sobre el nivel de realización de sus objetivos de control, la detección de las debilidades de control críticas, la fundamentación de los riesgos identificados, y las recomendaciones oportunas para la toma de acciones correctivas en relación a los SI de la organización [3]. Por lo tanto, un auditor de SI es un experto tanto en organización como en control de sistemas y tecnologías de la información [13] que tiene que entender claramente a la organización y sus SI, y en consecuencia descubrir los riesgos y deficiencias detectados, así como elaborar un conjunto de recomendaciones útiles.

Así, dado lo importante que es para las organizaciones contar con ese juicio experto e independiente sobre los SI, y debido al cada vez mayor potencial que están adquiriendo las tecnologías de la información para mejorar la productividad de las organizaciones, asegurar su supervivencia, e incluso, cambiar nuestra forma de vida (administración electrónica, comercio

electrónico, etc., etc.), queda justificada la gran importancia que tiene la ASI en nuestra sociedad moderna y conectada.

Parece lógico por tanto pensar que debería existir una correspondencia entre la importancia que tiene la ASI, y el peso que recibe en los planes de estudio de nuestras universidades. Ya en [10] se observaba que en realidad no existe tal correspondencia, ignorando en muchos casos la materia de ASI en los planes de estudios de Informática, y en los mejores casos, incluyendo la materia en asignaturas optativas o de libre configuración, dedicando una cantidad de créditos muy reducida.

En este artículo se analiza cuál es la situación actual de la ASI tanto en las escuelas de informática como en los principales currículos internacionales, llegando a la conclusión de que de momento la ASI no recibe la atención que parece demandar en el mercado.

2. La ASI y los currículos internacionales

Dentro de los principales currículos internacionales utilizados para la definición de los planes de estudio de Ingeniería Informática (ACM/IEEE CS 2001, IRMA/DAMA 2000, ACM/AIS MSIS 2000, ISCC 1999, e IFIP/UNESCO ICF-2000), vamos a analizar si se aborda el tema de la ASI o, al menos, si se citan algunos aspectos relacionados con la misma.

2.1. Currículo ACM/IEEE CS 2001

En 1998 ACM y la *Computer Society* de IEEE formaron un comité científico denominado *Year 2001 Model Curricula for Computing* (CC2001), al que se le pidió que revisara el currículo de 1991 y desarrollara un conjunto de guías curriculares que abordara los desarrollos más recientes de las tecnologías informáticas en la década pasada y que resista a la siguiente década [2]. El informe CC2001 se encuentra dividido en cinco partes: Un volumen general (de principios generales y partes comunes a todos los tomos de disciplinas específicas) y cuatro tomos de disciplinas específicas.

- Ciencia de la Computación (*Computer Science*).
- Ingeniería de Ordenadores (*Computer Engineering*).
- Ingeniería del Software (*Software Engineering*).
- Sistemas de Información (*Information Systems*)

En el volumen de Ciencia de la Computación no aparece explícitamente la auditoría, aunque sí se propone una asignatura sobre *riesgos y responsabilidades de los sistemas basados en ordenador*. La ASI podría encajar también, en cierta manera, dentro del tema de las cuestiones sociales y profesionales que señala este currículo. Los otros volúmenes todavía están en elaboración, pero creemos que al menos el de *Sistemas de Información* debería abordar el tema de la auditoría.

2.2. Currículo IRMA/DAMA 2000

Este currículo [6] es el resultado de dos años de esfuerzo conjunto de dos asociaciones profesionales norteamericanas de gran relevancia en el área de bases de datos: IRMA[1] y DAMA[2], que empezaron en 1998 la revisión de la edición existente anteriormente.

En este currículo se insiste en la necesidad de que los ingenieros en informática no limiten sus conocimientos a los aspectos técnicos de los SI, sino que posean una visión más completa de ellos, incluyendo aspectos de gestión. Para ello propugnan adoptar un enfoque más global que la gestión de los datos, considerando a ésta como parte de la *Gestión de los Recursos de Información* (en siglas inglesas IRM).

En cuanto a la ASI, no se cita explícitamente en el documento.

2.3. Currículo ACM/AIS MSIS 2000

La necesidad de revisar los currículos en SI, especialmente el de ACM de 1982 (por los años transcurridos y por los cambios que habían tenido lugar en el campo de la Informática en tan largo periodo de tiempo) y el IS'97 (entre otras razones, por ser un currículo de pregrado y considerarse que se necesitaba también la titulación superior en SI), lleva a la creación, en enero de 1998, de un *Comité Curricular Conjunto* (*Joint Curricular Committee -JCC-*) de ACM y AIS, a fin de

[1] Information Resources Management Association

[2] Data Administration Management Association

elaborar un currículo de Master para SI, el MSIS 2000 [1].

El desarrollo de este currículo se ha basado en un conjunto de principios, cuidando la formación en ciertas capacidades, conocimientos y valores: un núcleo de conocimiento de SI, integración de SI y fundamentos empresariales, perspectiva amplia de negocios y mundo real, habilidades de comunicación, interpersonal y trabajo en equipo, habilidades de pensamiento analítico y crítico, y habilidades específicas conducentes a una carrera.

En este currículo se detallan algunas *carreras profesionales* como la de Gestión de la función de SI (que incluye un curso de seguridad), la de Consultoría o la de Gestión Global de tecnologías de la información, a las que -sin duda- les sería indispensable algunos conocimientos de ASI aunque no se incluya explícitamente en este currículo.

2.4. ICF-2000 de IFIP/UNESCO

IFIP[3] y UNESCO[4] han diseñado el *Informatics Curriculum Framework* (ICF-2000) con el fin de abordar la situación de cambio constante a la que se enfrenta la informática. Como indica su nombre, realmente se trata de un marco (*framework*), a partir del cual se pueden construir diferentes implementaciones de currículos de una manera directa. En el propio documento [5] se presentan ocho especificaciones de currículos para ocho categorías de roles profesionales.

Lamentablemente, en todo este marco curricular no aparece referenciado el auditor de SI ni la ASI.

2.5. ISCC´99

El currículo ISCC'99 (*Information Systems-Centric Curriculum*) pretende preparar especialistas de información para el desarrollo y utilización de grandes SI, y ha sido desarrollado por un equipo compuesto tanto por miembros de la comunidad universitaria como empresarial [8].

Este currículo propone un modelo invertido de aprendizaje en el cual los alumnos experimentan en primer lugar en el contexto de un SI para posteriormente estudiar los detalles, destacando la información como el principal activo de las organizaciones. Además propone, entre otras cosas, la utilización de un aprendizaje *just-in-time* basado en mentores, y en el que se integran explícitamente las habilidades interpersonales y el pensamiento sistémico. Por todo ello, la ASI encaja perfectamente en este tipo de currículo. Si bien no se cita la ASI, sí que se abordan temas relacionados en los cursos Computer Ethics I y II (propiedad intelectual, privacidad, crímenes informáticos, etc.).

2.6. SWEBOK

El SWEBOK [12] ha sido promovido originalmente por el *Software Engineering Coordinating Committee* de la *IEEE Computer Society* y ACM, aunque el año pasado la ACM le retiró su apoyo. Entre sus fines se incluyen la acreditación de los currículos universitarios y la certificación de profesionales, para lo que identifica un cuerpo básico de conocimiento que caracteriza el contenido de la disciplina de la Ingeniería del Software.

Como es lógico debido a su alcance, en el SWEBOK sólo se trata de auditorías y revisiones de calidad del software, en el sentido del estándar IEEE 1028:1997, y de la auditoría de la configuración del software, pero no realmente de la ASI.

3. Los modelos de currículo de la ISACF

En 1998 la ISACF propuso dos modelos de currículum para graduados y pregraduados sobre ASI. *Estos modelos se basan en las necesidades y expectativas de la profesión de ASI, y la investigación previa de los científicos, profesionales, organizaciones de auditoría, y sociedades profesionales* [7].

A continuación resumimos brevemente el contenido de estos currículos.

3.1. Modelo para pregraduados

Este modelo incluye tres grupos de cursos:

- Contabilidad, que abarca: Principios de Contabilidad, Gestión Contable, Control Interno y Sistemas de Información Contable.

[3] International Federation on Information Processing

[4] United Nations Educational, Scientific and Cultural Organization

- Sistemas de Información: Introducción a los Ordenadores, Programación de Ordenadores, Análisis y Diseño de Sistemas, Sistemas de Gestión de Bases de Datos, Redes de Comunicaciones basadas en Ordenador, y Gestión de SI.
- Auditoría, incluyendo Auditoría Interna, Introducción a los SI y Herramientas de Auditoría Asistida por Ordenador (CAAT) y *Temas especiales* (Confidencialidad e Integridad de SI, Ética de la Auditoría, etc.).

En general, en las Escuelas de Informática se tratan, en asignaturas de Contabilidad, Economía o Administración de Empresas, casi todos los temas del primer grupo, excepto los de Control Interno que –a nuestro juicio- no se les da la importancia ni extensión necesaria requerida por un auditor de SI. En cuanto al segundo bloque, se imparten prácticamente todas las asignaturas en una titulación de informática, así como la Introducción a los SI y la Confidencialidad e Integridad de los mismos (del tercer bloque); aunque hay que tener en cuenta que en algunas de ellas se hace mucho más énfasis –siguiendo la clasificación del ACM/IEEE CC- en la Ciencia de la Computación o a la Ingeniería del Software que realmente en los Sistemas de Información.

En cuanto a los aspectos específicos de ASI los analizaremos en el próximo apartado.

3.2. Modelo para graduados

Este modelo incluye cuatro tipos de cursos:

- Conocimientos básicos sobre Gestión de SI, Teoría y Práctica de la Auditoría y Organización de Empresas y Economía.
- Cursos obligatorios relacionados con la ASI: Entorno Legal de los SI, ASI, CAAT, Seguridad y Privacidad en SI, Cuestiones de Comunicaciones y Redes Avanzadas, y Auditoría de SI avanzados.
- Optativas, entre las que señalan como ejemplo: Sistemas de Información para la Dirección (EIS), Planificación de SI, Aseguramiento de la Calidad del Software, Gestión de Redes, Procesamiento y Diseño de BD, Gestión y Toma de Decisiones, Gestión Financiera Avanzada, etc.
- Métodos de investigación empresariales y proyecto.

En cuanto al primer grupo vale lo dicho para el modelo anterior. Por lo que respecta a los temas relacionados, afortunadamente en la mayoría de las universidades suelen existir una asignatura sobre Derecho Informático o Aspectos Legales de la Informática que cubre el primer tema (aunque al ser optativa muchos alumnos no la escogen ya que no aprecian la importancia que puede llegar a tener para el desempeño profesional). En cuanto a la Seguridad y Privacidad en SI, suele existir en casi todas las carreras una asignatura en la que se tratan los aspectos de Criptografía, y en determinadas universidades también alguna otra que se preocupa de aportar una visión de más alto nivel sobre la seguridad y su gestión. Por lo que respecta a las Cuestiones de Comunicaciones y Redes Avanzadas, y a las optativas del bloque 3, se tratan –salvo aquellas específicas relacionadas con las Ciencias Empresariales- en un abanico de asignaturas optativas y obligatorias en la mayor parte de las universidades. El grupo 4 se cubriría por medio de los Trabajos de Fin de Carrera que existen en nuestras universidades.

Además [7] señala la necesidad (que personalmente pensamos que no es sólo específica del auditor de SI sino de cualquier Ingeniero en Informática) de que se complemente esta formación con habilidades de comunicación –escrita y oral-, negociación, entrevista, psicología, gestión del tiempo, etc.

4. La Enseñanza de la ASI en las escuelas de informática

Se han estudiado las asignaturas de ASI de varias universidades españolas, teniendo en cuenta la información disponible en las páginas web de las titulaciones de informática a fecha de diciembre de 2003: Universidad de Almería (UAL), Universidad Carlos III (UC3M), Universidad de Castilla-La Mancha (UCLM), Universidad de Granada (UGR), Universidad de las Islas Baleares UIB), Universidad de Málaga (UMA), Universidad Politécnica de Madrid (UPM), Universidad Politécnica de Valencia (UPV), Universidad de Sevilla (US), Universidad de Vigo (UVI).

TEMAS	UAL	UC3M	UCLM	UIB	UGR	UMA	UPM	UPV	UVI
Auditoría interna	X	X	X	X	X	X	X	X	X
CAAT					X				X
Ética auditoría			X				X		
Teoría y práctica ASI		X	X	X	X	X	X	X	X
Auditoría SI		X	X	X	X	X	X	X	X
Auditoría SI avanzados		X	X					X	
Organización depto. auditoría			X				X		
Metodología COBIT	X	X	X	X	X	X		X	
Informe de auditoría		X	X			X	X		
Auditoría seguridad física	X		X				X	X	
Auditoría ofimática			X						
Auditoría dirección	X	X	X	X			X	X	
Auditoría explotación	X	X	X	X			X	X	
Auditoría desarrollo	X	X	X				X		
Auditoría mantenimiento			X				X	X	
Auditoría BD/datos	X	X	X				X	X	
Auditoría técnicas de sistemas	X		X	X				X	
Auditoría calidad			X		X		X		
Auditoría seguridad lógica	X	X	X		X		X	X	
Auditoría redes	X		X						
Auditoría aplicaciones	X		X		X		X		X
Audit. EIS			X						

Tabla 1. Análisis de contenido de ASI en algunas universidades españolas.

Hay que destacar que existen varias universidades en las que se ignora sorprendentemente la ASI dentro de los planes de estudio de las titulaciones de informática; mientras que en otras aparece dentro de las Licenciaturas en Administración y Dirección de Empresas. En algunas universidades la ASI depende del Departamento de Organización de Empresas, o Economía Financiera, mientras que en otras depende del Departamento de Informática, esto influye bastante en el enfoque que se da a la asignatura e incluso a los conocimientos que van desde un extremo *empresarial* hasta uno más *tecnológico*. Hay que destacar que en algunas universidades se imparte en tercer curso, lo que no permite aportar una visión muy amplia (ya que el alumno todavía no ha visto varias asignaturas relacionadas con la ASI), teniendo en cuenta además la madurez del alumno. Creemos, con el fin de paliar estos dos problemas, que la ASI debería ser una asignatura del último curso de la carrera.

La asignatura suele tener de 4,5 a 6 créditos, lo que no es suficiente para entrar en detalle en los diferentes tipos de auditoría, pero sí para transmitir los conocimientos básicos tanto *filosóficos* como *metodológicos* de la ASI. En la Tabla 1 detallamos los contenidos que aparecen en los temarios de las universidades analizadas.

Se confirma por tanto que la idea de dotar de formación sobre ASI tanto básica, como avanzada, complementaria y continuada la carrera de Ingeniero en Informática [4] no ha sido conseguida satisfactoriamente.

Hay que destacar también que en algunas universidades se imparten cursos de especialista o *masters* sobre ASI. Así, por ejemplo, en la Escuela Superior de Informática de Ciudad Real en colaboración con ASIA[5] (Asociación de

[5] www.auditoresdesistemas.com

Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones) y la codirección de Marina Touriño hemos impartido un curso de especialista en Auditoría de las TIC. En la Tabla 2 se resume el contenido de este curso de 15 créditos.

Módulo 1	Objetivos de la función de ASI. Alcance de responsabilidades de auditores de SI. Normas técnicas y metodologías generalmente aceptadas en el desarrollo de las tareas de la ASI
Módulo 2	Evaluación de riesgos de SI y tecnologías de la información (TI) para la empresa. Modelos de evaluación y análisis de riesgos. Utilización de estos métodos en la ASI
Módulo 3	Prácticas generalmente aceptadas y consensuadas en la gestión de SI. La ASI y el control interno de SI
Módulo 4	Auditoría de las funciones directivas de los SI y TI. Evaluación de los riesgos de estas funciones y actividades relacionadas con ellas
Módulo 5	Auditoría de las actividades relacionadas con los servicios brindados por los SI y TI. Evaluación de riesgos de estas actividades
Módulo 6	Auditoría de los planes de continuidad del negocio y su relación con los SI y TI. Evaluación de riesgos de estos planes y actividades relacionadas.
Módulo 7	Auditoría del cumplimiento de requerimientos técnicos de la legislación vigente y normativa relativa a los SI y TI. Evaluación de los riesgos en el grado de cumplimiento.
Módulo 8	Auditoría de las actividades del desarrollo, adquisición e implantación de SI y TI. Evaluación de los riesgos de esta actividad
Módulo 9	Auditoría de los SI para la gestión y soporte de la actividad empresarial. Evaluación de los riesgos en estos sistemas
Módulo 10	Auditoría de las actividades relacionadas con la seguridad lógica y física de SI y TI. Evaluación de los riesgos en estas actividades
Módulo 11	Auditoría de las actividades de supervisión, control de las actividades de SI y TI. Evaluación de los riesgos en estas actividades
Módulo 12	Técnicas de auditoría, manuales y herramientas automatizadas, proceso de calidad en el desarrollo del trabajo del auditor de SI. Proceso detallado de una auditoría de sistemas de información, documentación de las tareas realizadas y generación de informes de auditoría

Tabla 2. Contenido del curso de Especialista en Auditoría de la UCLM

5. Conclusiones

Debido al peso que están tomando los SI en el entorno empresarial, tanto en el ámbito nacional como internacional, y debido también a la necesidad que hay de controlar su correcto uso, funcionamiento y seguridad, la ASI resulta fundamental para conseguir que los SI sean fiables, seguros, estables, que cumplen con las leyes de protección de datos, etc., y por tanto que exista una *confianza* en su uso. No hay que olvidar que las tecnologías de la información alcanzan desde el conjunto de datos, hasta los elementos humanos, procedimientos de trabajo y de tecnología que de forma coordinada y alineada a una estrategia institucional, proporcionan soporte a la operación, a la toma de decisiones y al servicio de los clientes de una empresa, por lo que evidentemente representan un factor crítico para cualquier organización [11].

En este artículo hemos analizado el tratamiento de la ASI en los principales currículos internacionales, así como los contenidos de ASI impartidos en algunas universidades españolas, y hemos observado cómo efectivamente no se le da la importancia que tiene para nosotros la correcta formación de profesionales de los SI.

Creemos por lo tanto, que es fundamental que en una Ingeniería Informática se incluya la ASI (al menos como asignatura optativa), con un peso en créditos adecuado que permita una formación extensa tanto en teoría como en casos prácticos,

debido a la necesidad que se está observando en el mercado de profesionales con amplios conocimientos en ASI. Porque una adecuada docencia en ASI tiene el valor añadido (fundamental bajo nuestro punto de vista) de incorporar una visión global del gobierno o dirección de las tecnologías de la información, y la importancia de esta función en el entramado de los procesos de la organización.

Adicionalmente, creemos que hay que tener en cuenta que por muy buena y completa que sea la formación en ASI en las universidades (tanto en el primero como de segundo ciclo), ésta deberá ser forzosamente complementada de manera continuada tanto mediante programas de entrenamiento específico en las empresas, másters o cursos de especialización, y la participación en seminarios y conferencias organizadas por asociaciones profesionales, como ASIA.

Agradecimientos

Queremos agradecer a Marina Touriño las sugerencias y comentarios que han contribuido a mejorar este artículo.

Referencias

[1] ACM/AIS. *MSIS. Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems.* Disponible en http://cis.bentley.edu/isa/pages/documents/msis2000jan00.pdf. 2000.

[2] ACM/IEEE. *Computing Curricula 2001. Computer Science. Final Report (15 de Diciembre).* Disponible en www.computer.org/education/cc2001/final/index.htm. 2001.

[3] COBIT. *Control Objectives for Information and related Technology.* Disponible en www.isaca.org. 2003.

[4] Coltell, O. y Bernal, R. *La Auditoría Informática en la Universidad Española. Consideraciones Docentes y Académicas*. en *Auditoría y Control de Sistemas de Información para el Tercer Milenio.* 1999. Valencia: II Congreso Nacional de Auditoría y Control de Sistemas de Información.

[5] IFIP/UNESCO. *Informatics Curriculum Framework 2000 for Higher Education.* Disponible en www.ifip.or.at. 2000.

[6] IRMA-DAMA. *Curriculum Model 2000 of the Information Resource Management Association and the Data Administration Managers Association.* Disponible en www.irma-international.org. 2000.

[7] ISACF. *Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Levels. Information Systems Audit and Control Foundation.* Disponible en www.isaca.org. 1998.

[8] ISCC. *Information System-Centric Curriculum.* Disponible en www.cs.unomaha.edu. 1999.

[9] Piattini, M. y Del Peso, E., *Auditoría Informática: Un enfoque práctico. 2ª edición.* 2001, Madrid: Ra-Ma.

[10] Sanchís, F. *La Enseñanza Universitaria de la Auditoría Informática en España*. en *Auditoría y Control de Sistemas de Información para el Tercer Milenio.* 1999. Valencia: II Congreso Nacional de Auditoría y Control de Sistemas de Información.

[11] Solís, G.A., *Reingeniería de la Auditoría Informática.* 2002: Editorial Trillas.

[12] SWEBOK. *Guide to the Software Engineering Body of Knowledge. Stone Man Trial Version 1.00.* Disponible en www.swebok.org. 2001.

[13] Touriño, M., *¿Qué ventajas puede ofrecer una auditoría de sistemas de información a la dirección de una organización?* Revista práctica para empresarios y directivos - PYMES, 2002. **61**(Julio-Agosto): p. 58-61.