Content Related to Computing Security on Computer Engineering Degree According to International Professional Certificates

D. G. Rosado, L. E. Sanchez, D. Mellado and E. F. Medina

***Abstract*— Companies and professionals are currently demanding increasingly more specialized profiles, and it is therefore desirable for future graduates to have obtained one or more international professional certificates in computing security and auditing, or to at least to have received the preparation required to obtain them. It is therefore of the utmost importance that new studies be focused on professional needs without losing the scientific rigor demanded in engineers. If this objective is to be achieved, it is fundamental that these new study plans be oriented toward facilitating the attainment of these professional certificates. In this paper we establish transversal guidelines for the implementation of content related to computing security in all the subjects, materials and modules of the new degree in Computer Engineering. This will fit perfectly with the material already being taught, will be an enriching element and will allow students to obtain the basic minimum knowledge on security required by any computer engineer from the beginning of their education. The security-related content that is required to be taught during the degree course will additionally be focused on industry and present-day society by means of existing professional security and auditing certificates that will provide future professionals with the knowledge and skills needed as regards security.**

***Keywords*— security and auditing, professional certificates, contents, subjects, implementation.**

I. INTRODUCCION

A LO largo del curso 2009-2010 se empezó a implantar el primer curso del Grado en Ingeniería Informática en la Universidad de Castilla-La Mancha. Los detalles del grado, que ha sido adaptado al Espacio Europeo de Educación Superior (EEES) [1, 2], se recogen en una Memoria de Grado, que entre otras cosas ofrece información sobre su organización en módulos, que a su vez contiene materias, y que éstas están formadas por asignaturas, que son definidas en términos de unos descriptores generales, basándose en las recomendaciones de los principales currículos internacionales [3-9]. Para estas asignaturas, se incluye también información sobre las competencias a las que da cuenta, las prácticas docentes, métodos de evaluación, etc., y en todo caso, queda para el momento de la implantación de las asignaturas, el trabajo de definir detalladamente los contenidos de las mismas. De entre todas las asignaturas definidas en el grado, hay varias dedicadas exclusivamente a seguridad y auditoría, y hay otras asignaturas que definen implícitamente aspectos de seguridad ya sea en las competencias a alcanzar o en los descriptores a desarrollar. De cualquiera de las maneras, hay que detallar el contenido de seguridad y auditoría de todas estas asignaturas que se ajusten a sus competencias y descriptores de forma coordinada, y que se acerquen lo máximo posible a las necesidades que demanda la sociedad a través de las principales certificaciones profesionales de seguridad y auditoría [10-12].

Los contenidos de seguridad y auditoría dentro del grado en Ingeniería Informática deben estar perfectamente acoplados y organizados de forma que sea una progresión de conocimientos conforme se vaya avanzando en el grado, tengan una relación directa entre contenidos, estén ajustados a las competencias y objetivos de las asignaturas y estén orientados a las necesidades más demandadas por la sociedad [13, 14].

Las certificaciones profesionales internacionales son un excelente recurso para medir la demanda existente de profesionales en seguridad y auditoría que el mercado requiere [15-17]. Estas certificaciones definen un contenido especializado en seguridad y auditoría que podemos utilizar para incorporarlos en el grado ajustándolos y adaptándolos a las competencias, descriptores y objetivos de cada asignatura del grado.

Por lo tanto, con este trabajo pretendemos definir los contenidos, competencias, objetivos, prácticas docentes, etc. de cada asignatura donde se definan implícita o explícitamente temas de seguridad y auditoría descritos en el plan de estudios del grado, intentando que ese contenido se acerque lo máximo posible a los contenidos y competencias definidas en las principales certificaciones profesionales en seguridad y auditoría, de forma que haya una relación entre los contenidos de seguridad del grado y los contenidos de seguridad exigidos por las certificaciones profesionales que marcan las necesidades del mercado. Esto se debe hacer sin condicionar excesivamente la implantación del grado, pero de modo que se favorezca un acercamiento a estas certificaciones, tanto para que el alumno tenga una mejor formación, como para que opte a conseguir los certificados.

Además, hemos definido un mapa de conocimientos donde se describen el contenido de seguridad de cada asignatura, la relación con las competencias y objetivos de la asignatura y la

D. G. Rosado, Universidad de Castilla La Mancha, Spain, david.grosado@uclm.es
L. E. Sanchez, Universidad de las Fuerzas Armadas, Ecuador. luisenrique@sanchezcrespo.org
D. Mellado, Agencia Tributaria, Spain, damefe@esdebian.org
E. F. Medina, Universidad de Castilla La Mancha, Spain, eduardo.fdezmedina@uclm.es

relación con el contenido de las certificaciones profesionales.

En este trabajo se presentan los resultados conseguidos y elaborados como consecuencia de la ejecución del proyecto que fue presentado en el Primer Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS 2011 donde se presentó los objetivos que se plantearon, las actividades a desarrollar, las tareas y pasos a seguir para alcanzar los objetivos, el plan de trabajo seguido y se expuso un conjunto de entregables que se perseguían como resultado de todas las actividades y tareas definidas en el proyecto para conseguir los objetivos previstos. Por tanto, en este trabajo, se presentan dichos entregables que encajan perfectamente con los resultados esperados y que ha sido fruto de la ejecución de todas las actividades y tareas que se definieron y siguiendo la metodología de trabajo presentada en el artículo previo. Estos resultados nos servirán como guía de implantación de contenidos de seguridad en el Grado de Informática.

II. RESUMEN DE OBJETIVOS Y TAREAS

A. Objetivos

El objetivo de este proyecto es establecer una guía transversal para la implantación de contenidos relacionados con la seguridad informática en todas las asignaturas, materias y módulos del nuevo grado de Ingeniería Informática, que encajen perfectamente con las materias que se cursan, que sirvan de elemento enriquecedor y que sirva a los alumnos para adquirir los conocimientos básicos de seguridad mínimos que a cualquier ingeniero informático se le exige desde el principio de su formación. Además, esta integración debe asegurar un camino que les lleve a adquirir la base del conocimiento y materias relacionadas y exigidas en las diferentes certificaciones profesionales de seguridad.

Además, estos contenidos deben estar bien definidos y orquestados con las materias que se cursan, con el curso donde se imparta y con el nivel y competencias exigidas a los alumnos. Por tanto, los contenidos deben repartirse por todo el grado de tal forma que no se repitan entre asignaturas afines, que vayan de niveles básicos a más avanzados conforme se vaya progresando en el grado, y que estén relacionados unos con otros dentro de la misma materia e incluso dentro del mismo curso.

Lo que se pretende es que una vez superado los tres primeros cursos del grado, los alumnos hayan adquirido los conocimientos básicos de seguridad necesarios dentro de todos los ámbitos y campos de la informática (sistemas, software, redes, bases de datos, web, programación, arquitecturas, tecnologías, etc.) antes de iniciar la especialización, donde, dependiendo de ésta, se profundice con más detalles sobre seguridad para un ámbito específico de la informática (con alguna asignatura exclusiva de seguridad), como pueden ser los sistemas software, redes, etc. Así, nos aseguramos que aunque sea experto en, por ejemplo, seguridad software, también haya adquirido los conocimientos básicos para el resto de ámbitos de la informática. Tanto las materias de la especialización como las del resto del grado con contenidos de seguridad deben encajar perfectamente con las materias exigidas por las certificaciones profesionales o al menos sentar las bases y principios para conseguirlas.

De esta forma, un futuro graduado en Informática tendrá las nociones y conocimientos básicos sobre Seguridad, con amplios conocimientos sobre un área en concreto y con las bases necesarias para optar a alguna de las acreditaciones profesionales de seguridad que existen y que son demandadas en la industria de las TIC.

B. Tareas

Para conseguir los objetivos establecidos, se divide el proyecto en 4 actividades bien diferenciadas y que son necesarias para la consecución del proyecto. A estas 4 actividades se le añade una actividad más que es la de Coordinación donde se lleva a cabo las tareas de coordinación, integración y seguimiento del proyecto. Las actividades son:

1. Análisis de las certificaciones profesionales: Se debe realizar un estudio profundo y análisis de las diferentes certificaciones profesionales existentes en temas de Seguridad y del contenido establecido para cada una de ellas. Se deberá seleccionar los aspectos claves del contenido de las certificaciones profesionales e identificar los aspectos comunes a ellas.
2. Análisis de las asignaturas del grado: Se debe realizar un estudio y análisis de todas las asignaturas y materias del grado, así cómo conocer los diferentes descriptores y contenido para cada una de ellas con el fin de poder identificar temas y contenidos afines a las certificaciones profesionales para poder incorporar cierto contenido en la siguiente actividad.
3. Establecer guía de implantación en el grado: En esta actividad se hace el trabajo importante del proyecto de innovación dónde detallamos los contenidos más apropiados a ser incorporados en las asignaturas del grado e indicamos en qué asignaturas deben ser incorporados, estableciendo una guía de implantación de los contenidos de seguridad acorde a las certificaciones profesionales dentro de las asignaturas y/o materias del grado, además de actualizar las competencias, tareas, contenidos, objetivos y planificación de cada asignatura modificada. También se define y detallan coherentemente los contenidos, prácticas, actividades docentes, ejercicios, etc. de las asignaturas involucradas. Además, se establece relaciones entre asignaturas con contenidos de seguridad y auditoría con el fin de evitar repetir contenidos y con el propósito de que el aprendizaje de los contenidos sea de forma continua y progresiva conforme se vaya avanzando en el grado.
4. Definir mapas de conocimiento orientados a certificaciones: En esta actividad se hace un análisis y estudio de los contenidos de seguridad y auditoría incorporados, de las asignaturas involucradas y de las competencias que definen aspectos de seguridad dentro del plan de estudios. Con todo esto se hace un mapa indicando qué contenido es cubierto por cuales asignaturas y si cumplen con las competencias

establecidas en el plan de estudios. Así, sabremos el mapa de asignaturas que cubren la mayor parte de los contenidos definidos por qué certificación, de forma que el alumno sepa las asignaturas que debe cursar para estar mejor preparado para una certificación u otra y qué aspectos no son cubiertos y debería reforzar.

III. RESULTADOS ALCANZADOS

Para conseguir los objetivos establecidos, vamos a dividir el plan de trabajo en las 5 actividades bien diferenciadas y que son necesarias para la consecución de los objetivos que han sido mostradas anteriormente. Mostraremos los resultados alcanzados para cada una de estas actividades. Las actividades y los resultados se explican a continuación.

A. Coordinación

Se establece un plan de seguimiento y coordinación entre todos los involucrados en el proyecto, para establecer plazos de entrega y conseguir resultados que alimenten al resto de actividades, de forma ordenada, coherente y a tiempo.

Resultado: Se ha realizado correctamente y se ha llevado un control permanente de todos los trabajos y de los plazos de ejecución. La coordinación se ha llevado de forma correcta y en todo momento cada uno de los participantes sabía que tenía que hacer, qué tenía que entregar y de qué plazo disponía para su entrega. Además, todos los participantes tenían el informe completo de los trabajos que se iban realizando por el resto de participantes para poder integrar y continuar con lo ya realizado.

Entregable: Se han generado varios informes de seguimiento indicando las tareas a realizar, los involucrados en cada tarea, las fechas de inicio y fin de cada actividad, y los resultados y trabajo realizado hasta el momento (en porcentaje de realización). Esto nos ha servido para conocer el estado real del proyecto y si las actividades se iban realizando conforme la planificación inicial (ver sección IV.A).

B. Análisis de las certificaciones profesionales

Se debe realizar un estudio profundo y análisis de las diferentes certificaciones profesionales existentes en temas de Seguridad y del contenido establecido para cada una de ellas. Se deberá seleccionar los aspectos claves del contenido de las certificaciones profesionales e identificar los aspectos comunes a ellas.

Resultado: Aquí han intervenido participantes con un marcado carácter empresarial y certificados profesionalmente que conocen cuáles son las más importantes certificaciones y más demandadas por las empresas, e incluso tienen amplio conocimiento sobre los contenidos de muchas de ellas, lo cual nos ha permitido establecer discusiones sobre el contenido más interesante y que mejor encaja con el plan de estudios y con la situación actual del mercado y de la sociedad.

Entregable: Se ha elaborado una lista de los contenidos más interesantes y adecuados en temas de seguridad y auditoría, extraídos de los contenidos exigidos por las certificaciones profesionales. Este documento ha sido revisado por todos los participantes y ha sido producto de muchos cambios y modificaciones hasta encontrar un consenso entre todos (ver sección IV.B).

C. Análisis de las asignaturas del grado

Se debe realizar un estudio y análisis de todas las asignaturas y materias del grado, así cómo conocer los diferentes descriptores y contenido para cada una de ellas con el fin de poder identificar temas y contenidos afines a las certificaciones profesionales para poder incorporar cierto contenido en la siguiente actividad.

Resultado: En esta actividad contamos con profesores que participaron en la creación y elaboración del actual plan de estudios del grado de informática, por lo que el conocimiento de las competencias, materias y asignaturas es total, lo cual facilitó la labor de analizar en detalle todas las competencias relacionadas con la seguridad, y las asignaturas junto con los descriptores para extraer toda la información necesaria para tomar la decisión de qué asignaturas son más apropiadas, por tener una relación directa o indirecta con aspectos de seguridad, para que pueda incorporarse nuevos contenidos de seguridad y describirlas en detalle.

Entregable: El resultado de esta actividad ha sido una lista de asignaturas del grado junto con sus competencias, orientadas o relacionadas de alguna forma con la seguridad y auditoría, que sirvan como candidatas para poder incorporar los nuevos contenidos de seguridad extraídos de la actividad anterior. Esta lista también ha sido consensuada con el resto de participantes expertos en distintas disciplinas y que imparten asignaturas de diversa índole (ver sección IV.C).

D. Establecer guía de implantación en el grado

En esta actividad se hace el trabajo importante dónde detallamos los contenidos más apropiados a ser incorporados en las asignaturas del grado e indicamos en qué asignaturas deben ser incorporados, estableciendo una guía de implantación de los contenidos de seguridad acorde a las certificaciones profesionales dentro de las asignaturas y/o materias del grado, además de actualizar las competencias, tareas, contenidos, objetivos y planificación de cada asignatura modificada. También se define y detallan coherentemente los contenidos, prácticas, actividades docentes, ejercicios, etc. de las asignaturas involucradas. Además, se establece relaciones entre asignaturas con contenidos de seguridad y auditoría con el fin de evitar repetir contenidos y con el propósito de que el aprendizaje de los contenidos sea de forma continua y progresiva conforme se vaya avanzando en el grado.

Resultado: Sin duda esta actividad ha sido la más complicada de realizar y la que ha supuesto un esfuerzo extraordinario por parte de todos para su consecución. Aunque tenemos, por un lado los contenidos de seguridad a integrar, y por otro lado, las asignaturas candidatas, no es fácil integrar los contenidos en asignaturas, y requiere un análisis profundo y detallado tanto de los contenidos como de los descriptores de las asignaturas, para que dicha integración sea correcta. Además, dicha integración no es directa, sino que hay que estudiar en qué nivel de detalle esos contenidos deben ser

integrados, si se integra como un todo o se divide por partes distribuidos en cierto número de asignaturas de una misma materia, si se integra de forma que sea una evolución sobre algún tema concreto a lo largo de los cursos, si se define una trazabilidad de contenidos relacionados con contenidos afines pero adaptados al nivel de exigencia y competencias exigido, y un largo etcétera que se ha tenido en cuenta para realizar dicha integración.

A pesar de la dificultad de esta actividad, todos los participantes han colaborado activamente en el rol de encargados de sus asignaturas, y otro grupo de participantes más expertos en temas de seguridad (algunos de ellos certificados profesionalmente), han sabido cooperar y trabajar de forma coordinada para que la integración de contenidos de seguridad en asignaturas se haga de la mejor forma posible, de forma no invasiva para que todo encaje a la perfección sin modificar los contenidos de las asignaturas existentes.

Entregable: Este es el entregable más importante y de mayor valor de este proyecto de innovación docente porque es el resultado final al que queríamos llegar. Este entregable, que se describirá en la sección III, resume los entregables de las actividades anteriores, presentado la lista de contenidos de seguridad seleccionados de las certificaciones profesionales, la lista de las asignaturas que han sido seleccionadas como candidatas para incorporar contenidos de seguridad, y también se muestra la relación entre ambas dejando claro qué contenidos en qué asignaturas han sido integradas y de qué forma (ver sección IV.D).

E. Definir mapas de conocimiento orientados a certificaciones

En esta actividad se hace un análisis y estudio de los contenidos de seguridad y auditoría incorporados, de las asignaturas involucradas y de las competencias que definen aspectos de seguridad dentro del plan de estudios. Con todo esto se hace un mapa indicando qué contenido es cubierto por cuales asignaturas y si cumplen con las competencias establecidas en el plan de estudios. Así, sabremos el mapa de asignaturas que cubren la mayor parte de los contenidos definidos por qué certificación, de forma que el alumno sepa las asignaturas que debe cursar para estar mejor preparado para una certificación u otra y qué aspectos no son cubiertos y debería reforzar.

Resultado: El propósito de esta actividad final es la de definir un mapa de conocimientos a partir de los contenidos de seguridad y auditoría que han sido integrados en las distintas materias y asignaturas a lo largo de todo el plan de estudios. El objetivo es indicar qué conjunto de asignaturas tienen ciertos contenidos relacionados de seguridad que juntos establecen un conocimiento completo de algún aspecto o ámbito de seguridad. Además, también se define un camino de asignaturas donde, a partir de los contenidos de seguridad incorporados, facilitan o se acercan más a una certificación profesional u otra, o con el que se consigue un conocimiento más detallado en temas de seguridad para una disciplina determinada dentro de la seguridad y auditoría.

Entregable: Este entregable es una especie de tabla con todo el plan de estudios (cursos, materias y asignaturas) y donde cada casilla indica el contenido de seguridad que ha sido implantado. Así, podemos establecer qué asignaturas tienen relación con respecto a los temas de seguridad que se abordan, para finalmente, poder indicar el camino o conjunto de asignaturas que el alumno puede cursar para adquirir un conocimiento más o menos profundo en aspectos de seguridad que más se ajustan a una u otra certificación profesional (ver sección IV.E).

IV. RESULTADOS DE LOS ENTREGABLES

A. Informes de seguimiento.

Son documentos donde se indica cuál ha sido la evolución del proyecto, quienes son los implicados, qué se debe presentar y qué queda por hacer, aclarando los plazos y la coordinación entre todos, y definiendo los hitos futuros. Además, también sirve para aclarar dudas y ver el estado actual del proyecto.

B. Lista de contenidos a incorporar.

Es un documento donde se definen qué certificaciones profesionales de seguridad y auditoría han sido seleccionadas, junto con los contenidos más adecuados y más interesantes de cada una de las certificaciones seleccionadas. Esta lista de contenidos no debe ser muy amplia ya que de lo contrario, imposibilitaría la incorporación en el plan de estudios.

Existen numerosas entidades y organismos acreditadores en todo el mundo. La lista de certificaciones disponibles en el mercado es también inagotable. Por ello, hemos seleccionado algunas de las más importantes, prestigiosas, avaladas por una larga experiencia y reconocidas por el sector.

- CISA (Certified Information System Auditor) y CISM (Certified Information Security Manager) por ISACA.
- CISSP (Certified Information System Security Manager) por (ISC)[2]
- GIAC (Global Information Security Assurance Certification)
- CIA (Certified Internal Auditor) por el Institute of Internal Auditors.
- CIPP (The Certified Information Privacy Professional) por el the International Association of Privacy Professionals.
- CPP (Certified Protection Professional) por ASIS International.
- CCSP (Cisco Certified Security Professional) por CISCO Systems.

De entre toda esta lista de certificaciones, se han extraído los contenidos que se repiten en todas debido a la importancia que tienen esos aspectos de seguridad, y algún otro contenido que hemos considerado importante. Los contenidos, descripciones y descriptores se describen en la Tabla I.

TABLA I. CONTENIDO, DESCRIPCIÓN Y DESCRIPTORES DE LAS PRINCIPALES CERTIFICACIONES PROFESIONALES.

ID	Contenido	Descripción	Descriptores
AUD	Auditoría de sistemas de información	Para brindar servicios de auditoría de sistemas acorde a las normas, guías, estándares y mejores prácticas para apoyar a la organización a asegurar que sus sistemas y la tecnología de información están protegidos y controlados	Estándares, directrices, y herramientas. Controles. Planificación y gestión de proyectos de auditoría. Leyes y regulaciones aplicables. Recopilación de evidencia. Muestreo, reporte y comunicación. Sistemas y marcos de aseguramiento de la calidad de la auditoría.
GOB	Gobierno y gestión de TI	Para proporcionar aseguramiento de que la organización tiene la estructura, las políticas, los mecanismos de reporte y las prácticas de monitoreo necesarias para cumplir los requisitos del gobierno corporativo y la gestión de las TI	Metas y objetivos del negocio. Relación entre la seguridad de la información y las funciones del negocio. Alcance y los estatutos del gobierno de seguridad de la información. Estrategias de planificación presupuestaria. Desarrollo de casos de negocio. Requerimientos regulatorios y su impacto potencial. Gestión de responsabilidad común y relaciones con terceros y su impacto. Roles, responsabilidades y estructuras organizacionales. Lazos entre políticas y objetivos de negocio de la empresa. Estándares. Métodos centralizados y distribuidos para coordinar actividades de seguridad de la información y para establecer canales de comunicación y notificación en toda la organización.
RIE	Gestión de riesgos de la información	Identificar y gestionar los riesgos de seguridad de la información para lograr los objetivos del negocio.	Riesgos, vulnerabilidades y exposiciones de la información. Metodologías de evaluación y análisis de riesgos. Controles y contramedidas. Estrategias de mitigación de riesgos. Técnicas de análisis costo-beneficio. Principios y prácticas de gestión de riegos basados en el ciclo de vida.
PRO	Desarrollo del programa de seguridad de información	Crear y mantener un programa para implementar la estrategia de seguridad de información	Tipos de actividades. Planificación, diseño, desarrollo, prueba e implementación de los controles de seguridad de la información. Alineación de requisitos de seguridad. Arquitecturas de seguridad. Tecnologías y controles de seguridad. Desarrollo de políticas de seguridad. Cultura y comportamiento. Métodos para desarrollar, implementar, comunicar y mantener políticas, estándares, procedimientos, guías y otros documentos. Diseño, desarrollo e implementación de métricas de seguridad. Certificación y acreditación del cumplimiento. Métodos de seguimiento, medición y sostenimiento.
ARQ	Arquitectura y Modelos de Seguridad	Conceptos, principios, estructuras y estándares empleados para diseñar, monitorizar y asegurar sistemas, equipos, redes, aplicaciones y controles usados para reforzar los diversos niveles de la disponibilidad, integridad y confidencialidad	Conceptos de control y seguridad. Modelos de seguridad. Criterios de evaluación. Seguridad en entornos cliente/servidor y host. Seguridad y arquitectura de redes. Arquitectura de la seguridad IP.
CON	Sistemas y Metodología de Control de Acceso	Conjunto de mecanismos que permiten crear una arquitectura segura para proteger los activos de los SI	Conceptos y tópicos. Identificación y autenticación. Equipo de e-security. Single sign-on. Acceso centralizado / descentralizado / distribuido. Metodologías de control. Monitorización y tecnologías de control de acceso. Modelos de control de acceso (DAC, MAC, RBAC). Mejore prácticas (denegación implícita, menos privilegio, separación de responsabilidades, rotación de trabajo). Fundamentos biométricos. Claves
DAP	Seguridad en el Desarrollo de Aplicaciones y Sistemas	Define el entorno donde se diseña y desarrolla el software y engloba la importancia crítica del software dentro de la seguridad de los SI	Definiciones. Amenazas y metas de seguridad. Ciclo de vida. Arquitecturas seguras. Control de cambios. Medidas de seguridad y desarrollo de aplicaciones. Bases de datos y data warehousing. Knowledge-based systems. herramientas y técnicas de monitoreo
CRI	Criptografía	Los principios, medios y métodos de protección de la información para asegurar su integridad, confidencialidad y autenticidad	Historia y definiciones. Aplicaciones y usos de la criptografía. Protocolos y estándares. Tecnologías básicas. Sistemas de encriptación (AES, DES, PGP, RSA). Criptografía simétrica / asimétrica. Firma digital. Seguridad en el correo electrónico e Internet empleando encriptación. Gestión de claves. Public key infrastructure (PKI). VPN. IPSec. Ataques y criptoanálisis. Cuestiones legales en la exportación de criptografía
FIS	Seguridad Física	Técnicas de protección de instalaciones, incluyendo los recursos de los SI	Gestión de las instalaciones. Seguridad del personal. Defensa en profundidad. Controles físicos

INT	Seguridad en Internet, Redes y Telecomunicaciones	Incluye los dispositivos de la red, los métodos de transmisión, formatos de transporte, medidas de seguridad y autenticación	Gestión de la seguridad en la comunicaciones. Protocolos de red. Identificación y autenticación. Comunicación de datos. Seguridad de Internet y Web. Métodos de ataque. Seguridad en Multimedia. Firewalls. VPN. Seguridad de Perímetros
NEG	Recuperación ante Desastres y Planificación de la Continuidad del Negocio	Planificar, desarrollar y gestionar la capacidad para detectar, responder y recuperarse de incidentes de seguridad de información. Dirige la preservación del negocio en el caso de producirse situaciones de parada para la restauración de las operaciones	Conceptos de recuperación ante desastres y de negocio. Procesos de planificación de la recuperación. Gestión del software. Análisis de Vulnerabilidades. Desarrollo, mantenimiento y testing de planes. Prevención de desastres. Requisitos forenses. Prácticas de revisión e investigación. Cuantificación de daños, costos y otros impactos empresariales
LEY	Leyes, investigaciones y Ética	Engloba las leyes y regulaciones de los crímenes informáticos, las técnicas y medidas de investigación, recuperación de evidencias y códigos éticos	Leyes y regulaciones. Conducción de investigaciones. Ética en la seguridad de la información. Código ético

TABLA II. LISTA DE ASIGNATURAS Y DESCRIPTORES.

Asignaturas	Descriptores
Administración de Bases de Datos	Introducción a la administración de bases de datos. Diccionarios y repositorios de datos. Seguridad de bases de datos. Control de concurrencia y recuperación. Optimización y ajuste.
Análisis Forense Informático	Evidencias digitales. Recolección y manejo de evidencias. Detección de intrusiones informáticas. Redes trampa. Normativa legal y técnica en el tratamiento de evidencias. Herramientas de análisis forense.
Aplicaciones Distribuidas en Internet	Introducción a los modelos arquitecturales de bajo acoplamiento. Desarrollo de sistemas distribuidos. Plataformas de desarrollo basadas en estándares de mensajería y en paso de mensajes. Aspectos de escalabilidad y rendimiento en aplicaciones distribuidas en Internet.
Arquitectura de Computadores	Introducción a los tipos de arquitecturas y modelos de programación. Paralelismo a nivel de instrucción: conceptos y métodos para su explotación. Técnicas de optimización del software.
Aspectos Profesionales de la Informática	Gestión de Proyectos Informáticos. Aspectos jurídicos del uso de las TIC. Legislación y normativa. Propiedad intelectual. Firma electrónica. Ética y responsabilidad profesional. Delitos informáticos. Técnicas de comunicación efectivas para la elaboración del pliego de condiciones.
Auditoria en Sistemas de Información	Control interno y auditoría de sistemas de información. Metodologías de evaluación, control interno y auditoría. Departamento de auditoría. Entorno jurídico de la auditoría. Principales áreas de auditoría de sistemas de información. Herramientas para la auditoría.
Bases de Datos	Ficheros. Conceptos básicos de bases de datos. Sistemas de gestión de bases de datos. Modelos de datos. Modelo relacional. Estándar SQL. Programación y uso de bases de datos. Acceso programático a bases de datos. Introducción a otros modelos de datos.
Bases de Datos Avanzadas	Necesidades de información de las organizaciones. Modelado conceptual y lógico de datos. Bases de datos avanzadas: objeto-relacionales, orientadas a objeto, XML, web, multimedia, distribuidas, librerías digitales. Bases de datos y grid. Bases de datos y computación en nube. Procesamiento y gestión de transacciones.
Cálculo y Métodos Numéricos	Nociones básicas de los distintos conjuntos numéricos. Cálculo diferencial. Desarrollo de Taylor. Optimización. Cálculo integral y sus aplicaciones. Algunos métodos numéricos. Algorítmica numérica.
Comercio electrónico	Modelos de comercio electrónico. Seguridad en el comercio electrónico. Legislación. Transacciones electrónicas. Medios de pago electrónico. Lenguajes para el comercio electrónico Modelos de cliente.
Desarrollo de Bases de Datos	Requisitos de Datos. Diseño conceptual. Diseño lógico. Diseño Físico. Seguridad en BBDD. Diseño avanzado de datos: Objeto-relacional, XML-semiestructurado, multidimensional.
Desarrollo de Sistemas Web	Desarrollo de aplicaciones para la Web. Técnicas de modelado para la Web. Modelado de la interacción y la navegación. Arquitecturas para sistemas basados en web. Servidores web. Sistemas de gestión de contenidos. Dominios de aplicación Web.
Diseño y Gestión de Redes	Conceptos básicos sobre planificación de redes. Cableado estructurado de red. Diseño de LANs. Monitorización de una red. Control de una red. Protocolos de mantenimiento. Protocolos de monitorización. Herramientas de gestión de red.
Gestión de proyectos Software	Planificación estratégica. Planificación de proyectos software. Estimación. Seguimiento y control de proyectos software. Gestión de riesgos. Herramientas de gestión de proyectos.
Gestión de Sistemas de Información	El sistema de información y el negocio, adquisición, despliegue y gestión de soluciones y servicios TIC, técnicas avanzadas de manejo y recuperación de información, bases de datos de propósito especial (documentales, multimedia, espacio-temporales), sistemas de soporte a la decisión, almacenes de datos, minería de datos e inteligencia de negocio
Gestión y Administración de redes	Introducción a los Sistemas de mantenimiento y gestión de Red. Monitorización de una red. Control de una red. Protocolos de mantenimiento. Protocolos de monitorización. Herramientas de gestión de red. Gestión de la calidad de servicio
Ingeniería de Negocio	Requisitos organizacionales. Modelado de empresas. Procesos de negocio. Modelado y gestión de procesos de negocio. Desarrollo de software dirigido por procesos de negocio. Sistemas para toma de decisiones. Procesamiento OLAP. Procesos ETL. Minería de datos. Herramientas de inteligencia de negocio

Ingeniería de Requisitos	Fundamentos de análisis del software. Requisitos software. Tipos de requisitos. Elicitación, análisis, especificación y validación de requisitos software. Análisis orientado a objetos. Notaciones avanzadas. Herramientas de gestión de requisitos. Métodos de gestión de requisitos.
Ingeniería del Software II	Ciclos de vida del software. Procesos de ingeniería del software. Calidad de los productos y procesos del software. Verificación y validación del software. Pruebas del software. Mantenimiento del software. Gestión de configuración del software. Metodologías de desarrollo de software
Multimedia	Contenidos y composición multimedia, estándares para contenidos digitales, técnicas y estándares de compresión multimedia, distribución de contenidos multimedia. Sistemas y aplicaciones multimedia
Redes de Computadores II	Tecnologías de red. Interconexión de dispositivos de red. Protocolos de encaminamiento en Internet. Movilidad y multidifusión. Capa de transporte en TCP/IP. Diseño y programación de aplicaciones en red. Capa de aplicación en TCP/IP: servicios estándares más comunes. Conceptos básicos de la gestión de redes. Conceptos básicos de seguridad en redes.
Redes y Servicios Móviles	Características y diseño de aplicaciones sobre dispositivos móviles. Casos de estudio de plataformas comerciales. Desarrollo de sistemas basados en redes de sensores. Desarrollo de servicios para teléfonos móviles.
Seguridad de los Sistemas Informáticos	Políticas, técnicas y mecanismos de seguridad en los sistemas informáticos. Legislación y estándares de seguridad en las TIC. Vulnerabilidades de seguridad, análisis y clasificación de ataques, planes de seguridad y contingencia.
Seguridad de Sistemas Software	Fundamentos de seguridad. Seguridad organizativa. Requisitos de seguridad. Seguridad en desarrollo de software. Seguridad de sistemas de información. Riesgos de seguridad. Servicios de seguridad. Gestión de seguridad. Certificación, normas y estándares para la seguridad.
Seguridad en redes	Principios de seguridad en redes. Cortafuegos. Redes Privadas Virtuales. Acceso Remoto Seguro. Seguridad en capa de transporte. Seguridad en capa de Aplicación.
Sistemas Distribuidos	Conceptos fundamentales de sistemas distribuidos. Comunicación de procesos y grupos de procesos distribuidos. Objetos distribuidos e invocación remota. Sincronización distribuida. Transacciones y control de concurrencia. Programación de aplicaciones distribuidas.
Sistemas Operativos I	Características, funciones y estructura de los sistemas operativos: procesos, planificación, concurrencia, memoria, entrada y salida, sistemas de ficheros. Entorno de programación del sistema. Nociones de administración de sistemas.
Tecnologías y Sistemas Web	Plataformas web. Arquitecturas de sistemas web. Protocolos y estándares web. Programación de aplicaciones web. Tecnologías de acceso a bases de datos. Tecnologías avanzadas. Seguridad.

C. Lista de asignaturas candidatas.

Este documento define una lista de asignaturas, extraídas del plan de estudios del grado de Ingeniería Informática, que son las más adecuadas, por tener relación con algún aspecto de seguridad, para que se puedan incorporar nuevos contenidos de seguridad en su temario, ya sean como temas, ejercicios, casos prácticos, o prácticas de laboratorio. Para la selección de estas asignaturas se tiene en cuenta tanto los descriptores de cada asignatura, como las competencias con las que están relacionadas, además del visto bueno de la mayoría de tutores de las asignaturas involucradas. Por tanto, la lista de asignaturas candidatas servirá de entrada para el siguiente entregable y se pueden ver en la primera columna de la Tabla III.

~~D.~~A. Guía de Implantación.

Una vez que tenemos identificadas las asignaturas a las que se le puede incorporar ciertos contenidos de seguridad, los cuales son extraídos de las principales certificaciones profesionales, queda asignar o relacionar esos contenidos con esas asignaturas, de forma que se tenga claro dónde encaja esos contenidos en ese conjunto de asignaturas.

En la Tabla III podemos ver una visión general de las asignaturas del grado donde podemos incorporar, definir y planificar contenidos de seguridad y auditoría dentro de la propia guía docente de las asignaturas, ya sean como temas, ejercicios, ejemplos, casos prácticos o material complementario de la asignatura. No se detalla el contenido exacto que debe aparecer en cada asignatura, sólo una visión general del posible contenido, referido a una temática específica extraído de la lista de contenidos de seguridad, que pudiera ser incorporado a dicha asignatura. La definición detallada queda para un trabajo posterior, en el momento de definir la guía docente de la asignatura. Ahora sólo se ofrece unos descriptores a tener en cuenta en temas de seguridad y auditoría. Después del análisis y estudio llevado a cabo en esta actividad, hemos llegado al resultado mostrado en la Tabla III.

Aquí podemos ver cómo hemos relacionado las asignaturas candidatas generadas en la actividad III.C, con los posibles contenidos definidos en las principales certificaciones profesionales en seguridad y auditoría definidas en la actividad III.B.

De esta forma, hemos identificado qué contenido más apropiado de las certificaciones profesionales puede ser integrado y encajado en las diferentes asignaturas del Grado. Queda el siguiente paso que es una vez conocido el contenido que mejor encaja con la asignatura a partir de sus competencias y descriptores, falta definir dicho contenido y la guía docente de la asignatura con los objetivos, competencias, el temario, ejercicios, etc., que se deja para trabajo futuro conforme vayamos avanzamos en la implantación del Grado.

TABLA III. RESUMEN DE LA GUÍA DE IMPLANTACIÓN.

	ARQ	AUD	CON	CRI	DAP	FIS	GOB	INT	LEY	NEG	PRO	RIE
Administración de Bases de Datos					■	■			■	■		
Análisis Forense Informático		■							■	■		
Aplicaciones Distribuidas en Internet	■		■		■			■				
Arquitectura de Computadores	■											
Aspectos Profesionales de la Informática							■		■			■
Auditoria en Sistemas de Información		■							■		■	
Bases de Datos			■		■							
Bases de Datos Avanzadas			■		■	■			■	■		
Cálculo y Métodos Numéricos				■								
Comercio electrónico					■		■	■	■			
Desarrollo de Bases de Datos			■		■							
Desarrollo de Sistemas Web	■		■		■			■				
Diseño y Gestión de Redes	■			■				■				
Gestión de proyectos Software		■					■			■	■	■
Gestión de Sistemas de Información					■		■			■	■	■
Gestión y Administración de redes	■							■				
Ingeniería de Negocio							■			■	■	
Ingeniería de Requisitos					■						■	■
Ingeniería del Software II					■					■		■
Multimedia				■								
Redes de Computadores II	■		■					■				
Redes y Servicios Móviles	■		■	■				■				
Seguridad de los Sistemas Informáticos							■		■	■		■
Seguridad de Sistemas Software		■			■		■		■	■	■	■
Seguridad en redes	■		■	■				■				
Sistemas Distribuidos	■				■			■				
Sistemas Operativos I			■								■	
Tecnologías y Sistemas Web	■		■	■	■			■				

ARQ: Arquitectura y Modelos de Seguridad
AUD: Auditoría de sistemas de información
CON: Sistemas y Metodología de Control de Acceso
CRI: Criptografía
DAP: Seguridad en el Desarrollo de Aplicaciones y Sistemas
FIS: Seguridad Física
GOB: Gobierno y gestión de TI
INT: Seguridad en Internet, Redes y Telecomunicaciones
LEY: Leyes, investigaciones y Ética
NEG: Recuperación ante Desastres y Planificación de la Continuidad del Negocio
PRO: Desarrollo del programa de seguridad de información
RIE: Gestión de riesgos de la información

A. Mapa de certificaciones.

Este último material generado es un esquema o mapa de todo el plan de estudios del grado en Ingeniería Informática, y las relaciones en cuanto a contenidos de seguridad que se imparten en esas asignaturas con respecto a las certificaciones profesionales más destacadas. Aquí se muestran las asignaturas del grado y los posibles caminos hacia posibles certificaciones profesionales indicando qué conjunto de asignaturas pueden ser cursadas durante el grado para aproximarse al contenido exigido por las principales certificaciones profesionales.

La Tabla IV muestra las asignaturas de dos de las 4 intensificaciones para el Grado en Informática de la UCLM, junto con las optativas, y la relación existente con el contenido de las certificaciones profesionales seleccionadas. Debido a restricciones de espacio, la Tabla IV sólo muestra las dos intensificaciones (Ingeniería el Software (IS) y Tecnologías de Información (TI)) que tienen más relación con temas de seguridad, aunque el trabajo completo ha considerado todas las asignaturas de las 4 intensificaciones que no han sido mostradas aquí. Para el resto de intensificaciones (Ingeniería de Computadores y Computación) hay muy poco contenido en las asignaturas que forman esas intensificaciones que tengan relación con temas de seguridad identificados en las certificaciones profesionales.

De esta forma, podemos crear los diferentes mapas para las diferentes certificaciones profesionales, dando a conocer el conjunto de asignaturas y optativas que mejor encajan y que te dan una aproximación más completa a una determinada certificación profesional. Así, por ejemplo, quien esté interesado en tener mayor conocimiento sobre los contenidos de la certificación CISA, debe saber que tiene que cursar preferentemente la intensificación de Ingeniería de Software (IS) y elegir un conjunto concreto de optativas. Si lo que está interesado es en obtener conocimientos más relacionados con la certificación CISSP, deberá cursar la intensificación de Tecnologías de la Información (TI) y las cuatro asignaturas optativas que se indican en la Tabla IV.

TABLA IV. MAPA DE CERTIFICACIONES.

	Asignaturas	CISA	CISM	CISSP	GIAC
IS	Ingeniería de Requisitos	X	X		X
	Diseño de Software	X			
	Procesos de Ingeniería del Software				
	Calidad de Sistemas Software				
	Gestión de Proyectos Software	X	X		X
	Desarrollo de Bases de Datos	X		X	X
	Sistemas de Información Empresariales	X			
	Seguridad de Sistemas Software	X	X		X
TI	Integración de Sistemas Informáticos				
	Interacción Persona-Ordenador II				
	Diseño y Gestión de Redes			X	X
	Gestión de Sistemas de Información	X	X		X
	Tecnologías y Sistemas Web	X		X	X
	Comercio Electrónico	X	X	X	X
	Multimedia				X
	Seguridad en Sistemas Informáticos	X	X		X
Opt.	Ingeniería de Negocio	X	X		
	Bases de Datos Avanzadas	X	X	X	X
	Auditoría de Sistemas de Información	X	X		
	Administración de Bases de Datos	X	X		
	Desarrollo de Sistemas Web	X		X	
	Análisis Forense Informático	X	X		
	Redes y Servicios Móviles			X	
	Aplicaciones Distribuidas en Internet	X		X	X

V. CONCLUSIONES.

Este trabajo es el resultado de la ejecución de un proyecto de innovación docente donde se pretende plasmar la relación de temas de seguridad y auditoría entre los contenidos de las asignaturas del grado y los contenidos de las principales certificaciones profesionales de seguridad y auditoría que miden la demanda existente de profesionales en seguridad y auditoría que el mercado requiere, lo cual le da un aspecto más profesional, más orientado a las necesidades y más especializado en un ámbito concreto e importante de la Informática como es el de la Seguridad.

Con los resultados conseguidos, podemos tener la certeza de comprobar si el contenido más apropiado, que se ajustan a las necesidades reales de las empresas, ha sido debidamente incorporado e implementado en el grado, y si con dicha incorporación se cubre con alto porcentaje de competencias especificadas en el plan de estudios para las asignaturas. Además, con esta asociación, se puede extraer información de los puntos débiles en cuanto a contenidos y lo que el alumno tendría que reforzar para optar a alguna de las acreditaciones profesionales en seguridad y auditoría.

Para concluir, tan sólo me gustaría mencionar que todos los resultados obtenidos en este proyecto se comenzarán a aplicar en los cursos futuros, en el momento de empezar a definir las guías docentes de las asignaturas implicadas, principalmente en las asignaturas de las distintas intensificaciones y optativas, que son las más específicas y dónde tienen más cabida aspectos específicos de seguridad.

AGRADECIMIENTOS

Esta trabajo es el resultado de un proyecto de innovación docente titulado “Implantación y Orquestación de los Contenidos de Seguridad en el Grado en Ingeniería Informática que Favorezca en Acercamiento a las Principales Certificaciones Profesionales de Seguridad y Auditoría”, concedido dentro de la 6ª Convocatoria de Ayudas para Proyectos de Innovación Docentes promovidos por el Vicerrectorado de Ordenación Académica y Formación Permanente de la Universidad de Castilla-la Mancha. También es parte de los siguientes proyectos: SIGMA-CC (TIN2012-36904) and GEODAS (TIN2012-37493-C03-01) financiados por el “Ministerio de Economía y Competitividad” (España). Y por el proyecto PROMETEO financiado por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) del Gobierno de Ecuador.

REFERENCIAS

[1] EEES. Espacio Europeo de Educación Superior. Available from: http://www.eees.es/.
[2] ECTS. European Credit Transfer System. Available from: http://www.ects.es/.
[3] ACM/AIS, MSIS 2006: Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems. 2006.
[4] ACM/IEEE, Computer Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering. 2004.
[5] ACM/IEEE, Software Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. 2004.
[6] ACM/IEEE, Computing Curricula 2005. The Overview Report. 2005.
[7] ACM/IEEE, Computer Science Curriculum 2008. 2008.
[8] ACM/IEEE, Information Technology 2008. Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. 2008.
[9] ISACA, ISACA Model Curriculum for Information Security Management. 2008.
[10] Seidman, S., The Emergence of Software Engineering Professionalism, in IFIP International Federation for Information Processing. 2008, Springer.
[11] Crowley, E., Information system security curricula development, in 4th conference on Information technology curriculum. 2003. p. 249-255.
[12] Suarez, B. and E. Tovar, Accreditation in engineering, in Plenary Sessions of Int. Conf. Engineering Computer Education 2005 (ICECE05). 2006.

[13] Seidman, S.B., Software Engineering Certification Schemes in Computer. 2008.
[14] Batchman, T. and E. Tovar, Advantages and challenges which the accreditation process with ABET offers to engineering and computer science programs. Perspective of the engineering college, in Plenary Sessions of Int. Conf. Engineering Computer Education 2005 (ICECE05). 2005.
[15] (ISC)2. The International Information Systems Security Certification Consortium, Inc., (ISC). Available from: http://www.isc2.org/.
[16] GIAC. GIAC –Global Information Security Assurance Certification. Available from: www.giac.org.
[17] ISACA. Information Systems Audit and Control Association. Available from: www.isaca.org.

David G. Rosado has an MSc and PhD. in Computer Science from the University of Málaga (Spain) and from the University of Castilla-La Mancha (Spain), respectively. His research activities are focused on security for Information Systems and Cloud Computing. He has published several papers in national and international conferences on these subjects, and he is co-editor of a book and chapter books. Author of several manuscripts in national and international journals (Information Software Technology, System Architecture, Network and Computer Applications, etc.). He is member of Program Committee of several conferences and workshops nationals and internationals such as ICEIS, ICCGI, CISIS, SBP, IAS, SDM, SECRYPT, COSE and international journals such as Internet Research, JNCA, KNOSYS, JKSU, and so on. He is a member of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.

Luis Enrique Sánchez is PhD and MsC in Computer Science and is an Professor at the Universidad de las Fuerzas Armadas (ESPE) of Latacunga (Ecuador), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla-LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc)

Daniel Mellado holds a PhD and MSc in Computer Science from the Castilla- La Mancha University (Spain) and holds a degree in Computer Science from the Autonomous University of Madrid (Spain), and he is Certified Information System Auditor by ISACA (Information System Audit and Control Association). He is Assistant Professor of the Department of Information Technologies and Systems at the Rey Juan Carlos University (Spain). He participates at the GSyA research group of the Department of Information Technologies and Systems at the Castilla- La Mancha University. He is civil servant at the Spanish Tax Agency (in Madrid, Spain), where he works as IT Auditor Manager. His research activities are security governance, security requirements engineering, security in cloud computing, security in information systems, secure software process improvement and auditory, quality and product lines. He has several dozens of papers in national and international conferences, journals and magazines on these subjects and co-author of several chapter books. He belongs to various professional and research associations (ASIA, ISACA, ASTIC, ACTICA, etc).

Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in databases, datawarehouses, web services and information systems, and also in security metrics. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences (DEXA, CAISE, UML, ER, etc.). Author of several manuscripts in national and international journals (Information Software Technology, Computers And Security, Information Systems Security, etc.), he is director of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain. He belongs to various professional and research associations (ATI, AEC, ISO, IFIP WG11.3 etc.).