La Seguridad como una asignatura indispensable para un Ingeniero del Software

David G. Rosado, Carlos Blanco, Luis Enrique Sánchez, Eduardo Fernández-Medina y Mario Piattini
Grupo de Investigación ALARCOS – Instituto de Tecnologías y Sistemas de Información
Dep. de Tecnologías y Sistemas de Información – Escuela Superior de Informática
Universidad de Castilla-La Mancha. Ciudad Real.
{David.GRosado, Carlos.Blanco, Luise.Sanchez, Eduardo.Fdezmedina, Mario.Piattini}@uclm.es

Resumen

La seguridad informática ha venido cobrando mayor importancia para las organizaciones dado el marcado crecimiento de las nuevas tecnologías de la información, servicios Web, comercio electrónico, etc. Es por ello que existe la necesidad de contar con nuevos profesionales en este entorno. Para ello, es necesario contar con asignaturas de Seguridad en las escuelas universitarias, que doten al futuro profesional de los conocimientos necesarios para afrontar con éxito las necesidades que el mundo empresarial actual demanda. Así, aprovechando el estado actual de implantación del sistema europeo de créditos, en este artículo se resume una propuesta de grado de informática, y se presenta la asignatura de Seguridad de Sistemas Software, ubicada en el perfil de Ingeniería del Software, definiendo el contenido de dicha asignatura de acuerdo a las directrices del sistema ECTS, y a las necesidades reales que cualquier ingeniero del software puede encontrarse en el mundo empresarial actual.

1. Motivación

Los Ingenieros del Software consideran la seguridad como un requisito no funcional, pero a diferencia de otros requisitos no funcionales como la fiabilidad y rendimiento, la seguridad no ha sido completamente integrada dentro del ciclo de vida de desarrollo y todavía es considerada después que el sistema ha sido diseñado. Sin embargo, la seguridad introduce no sólo características de calidad, sino también restricciones bajo las cuales el sistema debe operar. Ignorar tales restricciones durante el proceso de desarrollo podría llevar a serios problemas [8], tales como que los mecanismos de seguridad deberían ser encajados dentro de un diseño ya existente, por lo que provoca cambios de diseño que generalmente se traducen en vulnerabilidades software [9, 22], además de requerir una gran cantidad de dinero y tiempo para solventarlos una vez que han sido identificados (generalmente es necesaria una reconstrucción del sistema).

Lo más probable es que al considerar la seguridad solo en ciertas etapas del proceso de desarrollo, las necesidades de seguridad entren en conflicto con los requisitos funcionales del sistema. Si tenemos en cuenta la seguridad junto con los requisitos funcionales del sistema a través de las etapas de desarrollo, nos ayudaría a limitar los casos de conflicto, identificándolos pronto en el desarrollo del sistema, y encontrando formas de superarlos. Una de las formas de superarlas es que la seguridad forme parte del entrenamiento de los desarrolladores software. Concretamente, los ingenieros del software deberían considerar la seguridad de sus productos software desde las etapas más tempranas de la arquitectura y diseño.

Con el auge de las nuevas tecnologías de la información, servicios Web, comercio electrónico, etc., las organizaciones no se sienten seguras, sólo se generará confianza cuando podamos demostrar que el sistema global es seguro. Por ello, existe la necesidad de contar con nuevos profesionales en este entorno (administradores de redes, instaladores y supervisores de servidores Web seguros, protección de datos, auditoría, contingencias, recuperación, etc.).

Dado lo importante que es para las organizaciones contar con ese tipo de profesionales, 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.), queda justificada la gran importancia que tiene la implantación de la Seguridad en nuestra sociedad moderna y conectada. A pesar de su gran importancia, en los actuales planes de estudios (planes a extinguir) no se considera como una asignatura importante y se definen como asignaturas optativas o de libre configuración especificas sobre seguridad, dedicando una cantidad de créditos muy reducida, o hablando sobre seguridad en algún apartado dentro de las asignaturas obligatorias de la titulación, como por ejemplo en sistemas operativos o redes.

Aprovechando el establecimiento de los nuevos planes de estudios, se pretende dar a la asignatura de Seguridad la importancia que tiene para los futuros ingenieros del software, definiéndola como una asignatura obligatoria dentro de la intensificación de Ingeniería del Software del nuevo plan de estudios que se pretende implantar en el grado de informática de la Universidad de Castilla-La Mancha (UCLM). Este artículo se centra en definir de forma detallada los contenidos y actividades de la asignatura de Seguridad de Sistemas Software basándonos en los currículos internacionales, estándares de seguridad, y normas y especificaciones sobre seguridad.

Este artículo se estructura de la siguiente forma: en la sección 2 se define el objetivo del nuevo sistema europeo de educación y la propuesta de un nuevo plan de estudios adaptado a este sistema europeo para el grado de Informática de la UCLM. La sección 3 presenta el contenido de la asignatura de Seguridad Software que es una asignatura obligatoria de 6 ECTS dentro de la materia de Tecnología Específica de Ingeniería del Software. Finalmente, en la sección 4 proponemos las conclusiones a este trabajo.

2. Tiempos de cambio

La construcción de una Europa del conocimiento ha dado lugar a un movimiento importante, el cual tiene como objetivo el desarrollo de un Espacio Europeo de Educación Superior (EEES). Esto permitirá un reconocimiento más fácil de las titulaciones y asegurará una formación óptima de los estudiantes y su integración en un mercado laboral unificado y sin fronteras [12].

El EEES pretende establecer un sistema de carreras y créditos [11] común a todos los países de la UE (los créditos ECTS, European Credit Transfer System), el cual sólo establece una serie de directrices, y no especifica el contenido exacto que debe tener cada carrera, reservándose esa labor a las comisiones de expertos de cada país.

La llamada Declaración de Bolonia marca los objetivos para adoptar un sistema fácilmente legible y comparable de titulaciones basado en dos ciclos principales, establecer un sistema internacional de créditos compatibles (ECTS), promover la movilidad de estudiantes, profesores e investigadores y suscitar la cooperación europea para garantizar la calidad de la educación superior con la finalidad, en definitiva, de facilitar una dimensión europea de la educación superior.

Este nuevo sistema de educación europea está haciendo que las diferentes universidades tanto nacionales como internacionales estén definiendo, actualizando y estableciendo sus nuevos planes de estudios para adaptarlos hacia el sistema europeo de créditos (ECTS). Este es el caso que nosotros presentamos a continuación en este artículo, una propuesta de un nuevo plan de estudios que, la Universidad de Castilla-La Mancha (UCLM) para el grado en ingeniería informática, ha elaborado para adaptarlo al sistema europeo de educación y que se encuentra sometido al proceso de verificación de la ANECA.

2.1. Plan de Estudios propuesto

El Plan de Estudios propuesto se estructura en base a la resolución de 8 de Junio de 2009 de la Secretaría General de Universidades (BOE Num. 187 del 4/8/2009). En ella se explicita que los Planes de Estudios tendrán una duración de 240 créditos europeos, que deberán cursarse un conjunto de bloques de formación, e indica el conjunto mínimo de módulos a cursar, que son: Formación básica; Formación común a la rama de la Informática; De Tecnología Específica (al menos uno de ellos): Ingeniería del Software, Ingeniería de computadores, Computación, y Tecnologías de la Información.

De acuerdo con lo anterior, el título de Grado en Ingeniería Informática se ha diseñado usando el modelo de un único grado con cuatro intensificaciones y un catálogo de optativas. Cada

intensificación contiene un bloque completo de 48 ECTS de tecnología específica. Las cuatro intensificaciones ofertadas son: Computación, Ingeniería de Computadores, Ingeniería del Software y Tecnologías de la Información.

En la Figura 1 podemos ver la estructura completa del proyecto de innovación docente propuesto.

Figura 1. Estructura del proyecto de innovación docente propuesto

En relación con los métodos docentes, las actividades formativas contempladas según el tipo de materia serán:

- Actividades dirigidas: Clases Magistrales, Seminarios de problemas y casos y Prácticas de Laboratorio;
- Actividades supervisadas: Tutorías;
- Actividades autónomas: Estudio individual, Resolución de problemas y preparación de casos, y Preparación de prácticas de laboratorio;
- Actividades de evaluación: Pruebas escritas y/u orales.

También en relación con los métodos docentes, los posibles sistemas de evaluación dependen de las materias y son los siguientes:

- Pruebas escritas y/u orales;
- Entrega de informes, problemas, etc.;
- Trabajo de laboratorio y/o casos;
- Presentaciones y participación en seminarios.

Una vez presentado el nuevo plan de estudios a ser evaluado e implantado en el curso 2010/2011, el foco de nuestro estudio está en describir de forma detallada los contenidos de una de las asignaturas que creemos importante y que forma parte de la intensificación de Ingeniería del software como es la Seguridad de Sistemas Software, que veremos a continuación.

3. Seguridad Software

El objetivo de este artículo es presentar de forma detallada el contenido y las actividades que se compone la asignatura de Seguridad de Sistemas Software, la cual se encuentra enmarcada dentro del módulo III referente a tecnología específica, y donde podemos ver (Tabla 1) que la seguridad software ha sido incluida en la materia de tecnología específica de Ingeniería del Software como asignatura obligatoria de 6 ECTS en el nuevo plan de estudios propuesto.

Asignatura	ECTS
Ingeniería de Requisitos	6
Diseño de Software	6
Procesos de Ingeniería del Software	6
Calidad de Sistemas Software	6
Gestión de Proyectos Software	6
Desarrollo de Bases de Datos	6
Sistemas de Información Empresariales	6
Seguridad de Sistemas Software	6
Total	**48**

Asignaturas de tecnología específica de Ingeniería del Software

La asignatura de Seguridad pretende englobar todos los aspectos más importantes de seguridad que son requeridos por la sociedad para los futuros ingenieros del software. El contenido propuesto está basado en diferentes estándares, currículos internacionales y especificaciones de seguridad que consideramos más importantes y más demandados y utilizados por las empresas e instituciones tanto nacionales como internacionales donde la figura del ingeniero del software es requerida.

Una descripción a alto nivel ha sido definida en el nuevo plan de estudios (descriptores) para esta asignatura, donde su contenido consta de:

- 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.

Lo que se pretende con esta asignatura es que el alumno sea capaz de identificar, modelar e integrar los requisitos de seguridad del software en el proceso de su desarrollo, conocer las principales técnicas, mecanismos, servicios y los aspectos más importantes de seguridad del software, y conocer las normas, estándares y legislación más relevante sobre seguridad.

A continuación vamos a detallar cada uno de estos descriptores, indicando el contenido más adecuado y que encaja con lo dictado por las normas y estándares de seguridad [10, 14, 15, 18-20], y por los currículos internacionales más importantes [1-7].

3.1. Fundamentos de Seguridad

En este primer descriptor se intenta dotar al alumno de los aspectos básicos de seguridad en los sistemas de información, de mostrar la importancia que tiene la seguridad en la sociedad abierta y conectada en la que nos encontramos y de los conocimientos esenciales a tener en cuenta que servirán de introducción al resto de la asignatura.

Haciendo un recorrido por los principales currículos internacionales, nos encontramos un área de Fundamentos de Seguridad de Información dentro del currículo CS2008 [6], y el área de Garantía y Seguridad de Información dentro del currículo IT2008 [7], donde se establecen como aspectos a tratar el propósito y papel de la seguridad, sus objetivos, los principios básicos de seguridad, los estándares, mecanismos y políticas, y ataques o amenazas. Estos aspectos son interesantes y dotan al alumno de una primera aproximación al campo de la seguridad de los sistemas de información.

Por tanto, siguiendo las recomendaciones dictadas por los currículos internacionales (Computer Science and Information Technology), el contenido de este descriptor se podría organizar como sigue:

- Conceptos de Seguridad Informática;
- Principios de Seguridad Informática: Confidencialidad, Integridad y Disponibilidad;
- Factores de riesgo: Ambientales, tecnológicos y humanos;
- Mecanismos de seguridad: preventivos, detectivos y correctivos;
- Tipos de amenazas y atacantes.

3.2. Seguridad Organizativa

El objetivo de este segundo descriptor es dar a conocer la importancia de la seguridad dentro de las organizaciones. La implantación de la seguridad debe empezar desde las propias organizaciones, gestionando y manteniendo sus recursos, activos e información protegidos utilizando los mecanismos y políticas de seguridad más apropiadas para cada organización, ya que los problemas de seguridad no son exclusivamente técnicos.

La ISO/IEC 17799:2005 [16] tiene una parte dedicada a los aspectos organizativos y en ella se pretende aportar las bases para tener en consideración todos y cada uno de los aspectos que puede suponer un incidente en las actividades de negocio de la organización. Esta norma define cuestiones como aspectos organizativos para la seguridad, políticas de seguridad, clasificación y control de activos y seguridad ligada al personal.

Por tanto, siguiendo los aspectos definidos en ISO/IEC 17799:2005, el contenido para este descriptor lo hemos divido en:

- Introducción a la seguridad organizativa;
- Políticas y procedimientos de Seguridad en la organización;
- Clasificación y control de activos;
- Seguridad personal.

3.3. Requisitos de Seguridad

Una parte muy importante en el proceso de desarrollo software para conseguir sistemas software seguros es la denominada Ingeniería de Requisitos de Seguridad, la cual proporciona técnicas, métodos y normas para abordar esta tarea en el ciclo de desarrollo de los Sistemas de Información.

Lo que se pretende con este descriptor es mostrar la importancia de una de las principales partes en un proceso de desarrollo software seguro, como son los requisitos de seguridad. Para ello, nos servirá de guía uno de los estándares más conocidos relativos a requisitos de seguridad como es el denominado Common Criteria (CC) [15] que es un estándar internacional (ISO/IEC 15408) para la seguridad de computadores. Su propósito es permitir que los usuarios especifiquen los requisitos de seguridad, que los desarrolladores especifiquen los atributos de seguridad de sus productos, y que los evaluadores

determinen si los productos conocen sus demandas.

Además, buscando en los distintos currículos internacionales aspectos relativos a los requisitos de seguridad, lo único que hemos encontrado es una categoría de requisitos funcionales y no funcionales dentro del currículo de Computer Science (CS2008). Por tanto, para este descriptor seguiremos las recomendaciones y contenidos del common criteria referentes a los requisitos de seguridad, quedando el contenido como:

- Concepto de Requisito no funcional;
- Ingeniería de Requisitos;
- Definición y clasificación de Requisitos de seguridad;
- Técnicas y modelos de Ingeniería de Requisitos de Seguridad: Casos de mal uso y abuso, Common Criteria y SQUARE.

3.4. Seguridad en el desarrollo software

La creciente necesidad de construir sistemas seguros, debido principalmente a las nuevas vulnerabilidades derivadas del uso de Internet y de las aplicaciones distribuidas en entornos heterogéneos, motiva a la comunidad científica a demandar una clara integración de la seguridad dentro de los procesos de desarrollo.

Este descriptor intenta capturar los principales conceptos y aspectos más relevantes en cuanto a la incorporación de la seguridad en los procesos de desarrollo software. Haciendo una revisión a los principales currículos internacionales, encontramos diversas áreas y campos dedicados al desarrollo de sistemas, al análisis, al diseño, a las pruebas, etc., pero sin estar enfocado a la seguridad, sólo tenido en cuenta muy por encima y al mismo nivel que cualquier otro requisito no funcional como el rendimiento, fiabilidad, etc. Por ejemplo, en el currículo SE2004 [4], se define un área de desarrollo de sistemas considerando aspectos como la seguridad, el rendimiento, escalabilidad, etc.; un área de análisis de la calidad de los requisitos no funcionales, y de diseño de atributos de calidad, donde encontramos la seguridad entre ellos. Donde podemos encontrar un tema más enfocado a la seguridad es en el currículo CS2008 [6], pero la seguridad está centrada en la programación en sí (codificación y programas).

Por tanto, viendo la escasa información aportada en los distintos currículos internacionales referentes a este descriptor, y teniendo en cuenta la importancia que está cobrando en los últimos años la incorporación de la seguridad en los procesos software, nos vemos en la necesidad de definir en detalle los aspectos más importantes a tener en cuenta y de de dar a conocer las aportaciones más interesantes referentes a este tema.

Así, este descriptor es definido, siguiendo las recomendaciones de diferentes expertos de seguridad en procesos de desarrollo, con el siguiente contenido:

- Introducción al desarrollo software;
- Importancia de la seguridad en el desarrollo software;
- Propuestas de Seguridad en procesos de desarrollo: UMLSec, Model Driven Security.

3.5. Seguridad en Sistemas de Información

En la actual Sociedad de la Información, que depende de multitud de sistemas software cuya misión es crítica, la seguridad se ha convertido en un aspecto crucial para el desempeño de las organizaciones y avance de la sociedad.

Este descriptor intenta dar al alumno una visión general de la problemática de la seguridad en los sistemas de información, dando a conocer cuales son las técnicas, mecanismos, políticas, protocolos, amenazas, etc. más utilizadas y aparecidos en los diferentes sistemas de información.

Muchos aspectos relacionadas con este descriptor aparecen en distintos currículos internacionales, así tenemos que en el currículo CS2008 [6] se habla de criptografía, protocolos de seguridad, firma digital, políticas, control de acceso, etc., de forma genérica y también de forma específica centrándose en sistemas operativos y redes. El currículo SE2004 [4] también hace referencia a la criptografía, a la seguridad en el comercio electrónico y bases de datos. Y finalmente, hemos encontrado en el currículo IT2008 [7] un área dedicada a la seguridad de la información donde se definen temas como la criptografía y la seguridad y protección en sistemas operativos.

Por tanto, vemos como existen muchos aspectos que coinciden en distintos currículos, mostrando la gran importancia que tiene para un ingeniero informático. Así que, basándonos en los aspectos encontrados en estos currículos, este

descriptor puede ser organizado de la siguiente forma:

- Introducción a la seguridad en los sistemas de Información;
- Seguridad física y seguridad lógica;
- Criptografía: Criptografía simétrica y asimétrica, Infraestructura de clave pública (PKI), Certificados digitales, Autoridades de certificación, Firma digital;
- Seguridad en Internet: Correo electrónico seguro, WWW, Redes Virtuales Privadas;
- Seguridad en Sistemas Operativos;
- Seguridad en Bases de Datos.

3.6. Riesgos de Seguridad

La fase de análisis y la gestión de riesgos nos ayudan a identificar todos los activos importantes para la seguridad de los sistemas de información, las amenazas que pueden afectarles, identificar la vulnerabilidad de cada uno de ellos frente a estas amenazas y calcular el riesgo existente de un posible impacto sobre el activo. Con toda esta información, el responsable de seguridad puede tomar las decisiones pertinentes para implantar medidas de seguridad optimizando el factor riesgo-inversión. Este descriptor intenta dar a conocer en profundidad los posibles riesgos de seguridad que pueden aparecer, los elementos que tiene relación y del impacto y consecuencias negativas existentes.

Para definir el contenido de este descriptor, nos basamos en las diferentes disciplina, áreas y temas más interesantes propuestos por los currículos internacionales, como es el currículo CS2008 [6] donde dedica áreas exclusivas para la evaluación, la gestión y el análisis de riesgos, además del análisis de coste-beneficio. También, en los currículos MSIS2006 [1] y SE2004 [4] definen unidades y cursos de gestión de riesgos. Finalmente, hay un importante currículo para la gestión de seguridad de la información definido por ISACA [13] donde dejan claro la importancia de la evaluación y gestión de riesgos.

Por tanto, considerando los aspectos relacionados con los riesgos de seguridad aparecidos en los currículos más importantes, podemos descomponer este descriptor en temas que aporten al alumno profundos conocimientos en este tema. Así, el descriptor se compondría de la siguiente forma:

- Introducción a los riesgos de seguridad;
- Análisis de riesgos;
- Gestión de riesgos: MAGERIT, ISO/IEC 27005:2008;
- Evaluación del riesgo y análisis de coste-beneficio.

3.7. Servicios de Seguridad

El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para hacer frente a las amenazas a la seguridad del sistema y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.

Dentro de los currículos internacionales de ACM, sólo hemos encontrado en el currículo IT2008 [7] un área denominada Servicios de Seguridad donde los servicios de Disponibilidad, Integridad, Confidencialidad, Autenticación y No repudio son indicados, y otros temas sobre cifrado de datos entre sistemas y servicios, autenticación entre recursos y servicios, etc. No hay que olvidar los estándares más importantes en cuanto a servicios y dimensiones de seguridad como son el ITU_T X.800 [20] y X.805 [21] donde definen un conjunto de servicios de seguridad.

Por tanto, este descriptor, siguiendo el contenido de estos estándares y currículos donde los servicios de seguridad son mencionados, se podría descomponer en los siguientes temas:

- Seguridad como un Servicio: SaaS;
- Servicios básicos de Seguridad: Integridad, Confidencialidad, Autenticación, Autorización y No repudio;
- Servicios avanzados de Seguridad: Privacidad, Confianza, Delegación, Credenciales, Identidad, etc.

3.8. Gestión de Seguridad

Este descriptor define todos los aspectos relacionados con la gestión y administración de la seguridad en los sistemas de información, y pretende dotar al alumno de los conocimientos más relevantes y más destacados que es necesario conocer. Este descriptor se divide en dos únicos temas, que son:

- Gestión y planificación de la seguridad TI;
- Técnicas para la gestión de la seguridad TI.

Este contenido ha sido extraído de la revisión realizada por un lado, de los currículos internacionales como IT2008 [7], donde se definen temas como la gestión de la seguridad, y por otro lado, del currículo ISACA para la gestión de la Seguridad de la Información [13] donde establece como conceptos y temas a tratar la gestión de la seguridad y la medición e implementación de la gestión de la seguridad. Por último, los estándares ISO/IEC 13335-1:2004 [14] y ISO/IEC 27001:2005 [18] describen en profundidad los sistemas de gestión, y han sido tenidos en cuenta.

3.9. Certificación, normas y estándares para la seguridad

Las organizaciones gestionan una serie de datos y recursos los cuales su seguridad debe ser gestionada de forma competente y efectiva, identificando y detectando los riesgos a los que se someten y adoptando medidas adecuadas y proporcionadas. Para ello, es necesario un conjunto completo y coherente de certificados y normas a seguir.

Para describir el contenido de este descriptor nos hemos basado en el conjunto de estándares y especificaciones más relevantes de seguridad, como es la familia ISO/IEC 27000 que proporciona recomendaciones de mejores prácticas en la gestión de los sistemas de información, riesgos y controles dentro del contexto de un completo sistema de gestión de seguridad de información (SGSI). Hay diferentes criterios de evaluación tales como: Common Criteria [15], ISO/IEC 15408, y Information Technology Security Evaluation Criteria (ITSEC). Además, hay numerosas metodologías de evaluación, tales como: a) Common Methodology for Information Technology Security Evaluation (CEM); b) ISO/IEC 18045 [17]; c) Information Technology Security Evaluation Manual (ITSEM). Por ultimo, existen otros muchos estándardes y especificaciones relacionadas con la seguridad como pueden ser la familia X.800 ITU_T [20], ISO/IEC 13335 [14], y muchas otras.

Por tanto, para resumir todo el contenido referente a certificaciones, estándares y especificaciones de seguridad que podemos encontrar, y que sirva al futuro ingeniero para obtener un conocimiento amplio de todos ello, este descriptor se ha estructurado de la siguiente forma:

- Certificaciones de Seguridad;
- Especificaciones y estándares de Seguridad: X800 ITU_T family, ISO/IEC 13335, ISO/IEC 27000 series.

4. Conclusiones

Con la adaptación de los nuevos planes de estudios es el momento perfecto para incorporar y adaptar un conjunto de asignaturas en el grado de informática que a lo largo de estos últimos años ha ido evolucionando e incrementando su importancia, y que no han sido suficientemente consideradas en los actuales planes de estudios, y que los futuros ingenieros informáticos deberían conocer para tener garantías de éxito en el mundo profesional. Este es el caso de la asignatura de seguridad, donde se intenta dotar al alumno y futuro profesional de los conocimientos, técnicas y guías más importantes y más demandadas relativas a aspectos de seguridad de los sistemas software y que la mayoría de organizaciones y empresas demandan en la actual sociedad.

Creemos por lo tanto, que es fundamental que en una Ingeniería Informática se incluya la Seguridad como una asignatura obligatoria, con un gran peso en créditos 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. Las universidades, cada vez más, se están dando cuenta de la gran demanda existente, y están ampliando su oferta de asignaturas relacionadas con la Seguridad para implantarlas en los nuevos planes de estudios.

Este es el caso de la UCLM, donde en el nuevo plan de estudios adaptado al espacio europeo para el grado de Informática, se ha definido y se pretende establecer una asignatura obligatoria de 6 ECTS relacionada con la Seguridad de sistemas software donde se impartan los aspectos más importantes y relevantes de seguridad y se obtenga un amplio conocimiento sobre este campo para los futuros ingenieros del software.

Agradecimientos

Esta investigación es parte de los siguientes proyectos: QUASIMODO (PAC08-0157-0668), SISTEMAS (PII2I09-0150-3135) y SEGMENT (HITO-09-138) financiados por la “Junta de Comunidades de Castilla-La Mancha” y FEDER, MEDUSAS (IDI-20090557) y BUSINESS (PET2008_0136) financiados por el "Ministerio de Ciencia e Innovación (CDTI)”.

Referencias

[1] ACM/AIS, MSIS 2006: Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems. 2006.
[2] ACM/AIS/AITP, IS 2002. Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems. 2002.
[3] ACM/IEEE, Computer Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering. 2004.
[4] ACM/IEEE, Software Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. 2004.
[5] ACM/IEEE, Computing Curricula 2005. The Overview Report. 2005.
[6] ACM/IEEE, Computer Science Curriculum 2008. 2008.
[7] ACM/IEEE, Information Technology 2008. Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. 2008.
[8] Anderson, R., Security Engineering: A Guide to Building Dependable Distributed Systems. 2001: Jonh Wiley & Sons, Inc.
[9] Artelsmair, C. and R. Wagner. Towards a Security Engineering Process. in The 7th World Multiconference on Systemics, Cybernetics and Informatics. 2003. Orlando, Florida, USA.
[10] COBIT 4.1. Control Objectives for Information and related Technology. 2007; www.isaca.org.
[11] ECTS. European Credit Transfer System. http://www.ects.es/.
[12] EEES. Espacio Europeo de Educación Superior. http://www.eees.es/.
[13] ISACA, ISACA Model Curriculum for Information Security Management. 2008.
[14] ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security. 2004.
[15] ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation. 2009.
[16] ISO/IEC 17799:2005, Information technology -- Security techniques -- Code of practice for information security management.
[17] ISO/IEC 18045:2005, Information technology -- Security techniques -- Methodology for IT security evaluation.
[18] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements.
[19] ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management.
[20] ITU, ITU_T Recommendation X.800. Security Architecture for Open Systems Interconnection for CCITT Applications. 1991.
[21] ITU, ITU-T Recommendation X.805. Security architecture for systems providing end-to-end communications. 2003.
[22] Mouratidis, H. and P. Giorgini, Integrating Security and Software Engineering: Advances and Future Vision. 2006: Idea Group Publishing.