ALI®
Asociación de Titulados
en Ingeniería en Informática

UAH
Universidad de Alcalá
de Henares

Curso de postgrado en Seguridad Informática

Mayo 2014

C/ Mayor, 4 6ª planta – 28013 Madrid ◆ Teléfono: 91.523.86.20 ◆ Fax: 91.523.86.21
Correo-e: secretec@ali.es ◆ Web: www.ali.es

ALI®
Asociación de Titulados
en Ingeniería en Informática

UAH
Universidad de Alcalá
de Henares

Índice

1. Presentación

El curso da respuesta a las necesidades de formación en los conocimientos teóricos y prácticos que se precisan para acometer con éxito los procesos, actividades, estudios y proyectos en el ámbito de la seguridad informática.

Para los profesionales de la informática estos conocimientos son fundamentales y una exigencia en los proyectos que llevan a cabo y un imperativo legal al más alto nivel recogido como ***"Razón imperiosa de interés general"*** [1], según detalle:

> *"**Razón definida e interpretada la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, limitadas las siguientes:** el orden público, la seguridad pública, la protección civil, la salud pública, la preservación del equilibrio financiero del régimen de seguridad social, la protección de los derechos, la seguridad y la salud de los consumidores, de los destinatarios de servicios y de los trabajadores, las exigencias de la buena fe en las transacciones comerciales, la lucha contra el fraude, la protección del medio ambiente y del entorno urbano, la sanidad animal, la propiedad intelectual e industrial, la conservación del patrimonio histórico y artístico nacional y los objetivos de la política social y cultural."*

Son muchas de estas razones las que, en la sociedad de la información que estamos desarrollando, pueden verse directamente afectadas por la informática. Por citar solo algunas:

> ***"Los derechos fundamentales a la intimidad, a los datos de carácter personal, a la libertad de expresión; la seguridad pública (en sus infraestructuras críticas); la lucha contra el fraude (que utilizan la informática para llevarlos a cabo); la protección civil (sistema de control de transporte, de emergencias nucleares, contaminación, etc.), la propiedad intelectual, etc."***

Las exigencias de seguridad informática es exigida en leyes como: LOPD[2] y Real Decreto que la desarrolla[3], ENS[4], EJIS[5], etc.

En este curso se analizan todas las áreas de conocimiento que inciden en la seguridad informática: física, lógica, de comunicaciones, legal, etc.

---

[1] Art. 3 de la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.
[2] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter persona
[3] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
[4] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
[5] Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Este proyecto educativo ha sido **Galardonado por la Revista SIC**[6]**,** en el marco del Congreso "SECURMATICA" en la VIII edición de sus premios de Seguridad de la Información, categoría de Innovación, excelencia, formación, divulgación y profesionalización del Sector.

El planteamiento se basa en tres premisas adaptadas a las necesidades actuales de formación:

- **Concretar las necesidades formativas en Seguridad en los núcleos fundamentales de los conocimientos teóricos y prácticos que se precisan**.

- **Incluir las exigencias, cada vez más frecuentes, del mercado de las TI.** Incluyendo la formación para la obtención de certificaciones internacionales.

- **Ampliar los conocimientos teóricos y prácticos con una estructura modular** que incluyen nuevas áreas de conocimientos: tanto en el ámbito de la dirección y gestión de las áreas de Seguridad y Auditoría Informática, como en la dirección de los proyectos a llevar a cabo.

2. Objetivos

Se basan en la necesidad de las organizaciones públicas y privadas de proteger sus sistemas informáticos ante las innumerables amenazas a las que se exponen y en la necesidad que siente la sociedad de saber que los sistemas con los que opera son seguros, que hace necesario contar con profesionales verdaderamente formados, capaces de implementar los mecanismos de seguridad acordes con lo que se pretende proteger, generando la confianza suficiente para progresar en la sociedad de la información:

- Formación de alto nivel con los conocimientos y destrezas que se requieren para ejercer como Ingenieros de Seguridad, en un contexto internacional y para dirigir y gestionar los departamentos de Seguridad en administraciones públicas y organizaciones privadas.

- Ofrecer un instrumento práctico para la seguridad y control de los activos relacionados con la Información en general y de su soporte informático en particular para aquellos que pretendan desarrollar su carrera en este ámbito, así como si ya lo están desarrollando quieren profundizar en su conocimiento.

[6] SIC Seguridad en Informática y Comunicaciones

3. Dirigido para

- Desempeñar puestos de responsabilidad en seguridad informática en organizaciones privadas y públicas.
- Consultoría en seguridad TIC, sobre todo en responsabilidades del seguimiento o control de los proyectos de seguridad.
- Responsabilidad de proyectos en el ámbito de la seguridad TIC que desean ampliar sus conocimientos teóricos y prácticos en los estándares actuales de seguridad.
- Orientar su desarrollo profesional, en las tareas propias y exigibles en seguridad informática y optar a puestos de trabajo bien retribuidos a nivel nacional e internacional.

4. Contenidos

El curso se desarrolla en tres temas:

Tema 1 - Fundamentos de seguridad y riesgos de la información en las organizaciones

Este tema presenta los estándares internacionales y buenas prácticas de seguridad de la información en las organizaciones, en particular los previstos en la serie de normas ISO/IEC 27000, el Esquema Nacional de Seguridad, ENISA, etc. Así mismo aborda el análisis y gestión de riesgos (AGR) a nivel teórico y práctico y las metodologías AGR más utilizadas. Y en las habilidades directivas que han de desarrollar los responsables de la seguridad: Directores, Jefes e Ingenieros de seguridad.

Tema 2 - Fundamentos científicos de la seguridad

La protección de la información ***en la sociedad de la información y para la que hemos admitido que la red que la da soporte, Internet, haya sido diseñada y creada como una red insegura en si misma, se ha convertido en su gran talón de Aquiles.***

Los hechos que están acaeciendo así lo están demostrando: sustracción de datos personales, suplantaciones de identidad, estafas, evasión de capitales, sustracción de documentos, violación de la propiedad intelectual, espionaje internacional, etc.

Este tema presenta los principales fundamentos científicos que podemos aplicar para que partiendo de esta realidad, podamos aminorar los riesgos de seguridad de la información. En particular riesgos relacionados con la confidencialidad, integridad y no repudio.

El modulo presenta y trata a nivel teórico y práctico: Las técnicas criptográficas clásicas y modernas; los protocolos criptográficos; el criptoanálisis; la Firma Digital; las técnicas biométricas basadas en características físicas y en el comportamiento.

Tema 3 - Diseño e implantación de Sistemas de Gestión de Seguridad de la Información SGSI

Para aminorar los riesgos de seguridad de la información y garantizar la confianza las organizaciones privadas y públicas están creando sus propios procesos de seguridad que han de estar adecuadamente gestionados mediante un SGSI cuyo alcance, diseño e implantación es propio de cada organización, si bien los criterios en los que han de basarse están recogidos tanto en normas internacionales (serie de normas ISO 27000), como en el cumplimiento legal en España: LOPD, RDLOPD, ENS, etc. Este cumplimento adquiere mayor alcance en multinacionales, que también deberán cumplir con la legislación de los países en los que están implantadas.

Este tema aborda en profundidad todos los aspectos teóricos y prácticos del análisis, diseño e implantación de los sistemas de gestión de seguridad y en su presentación se siguen los criterios recogidos en las normas ISO 27000: La seguridad física y del entorno; Control de accesos al sistema; La seguridad en las comunicaciones; Seguridad en la operación de ordenadores y redes; La seguridad en SS.OO. Entornos virtuales, arquitecturas Cloud y SGBD; Seguridad en las aplicaciones y modelo de madurez de seguridad de software – SAMM[7]; La Seguridad y las personas; El Plan de Continuidad de Negocio según la norma ISO 22301[8]; Seguridad en el cumplimiento legal.

La última parte del tema está dedicada a presentar y preparar al alumno para que, si lo desea, se presente a la obtención de la certificación CISM®[9], muy valorada a nivel mundial y con frecuencia exigida por grandes y medianas empresas en la contratación de profesionales que han de llevar a cabo los proyectos de seguridad informática.

[7] Modelo de madurez de seguridad de software – SAMM
[8] UNE-ISO 22301:2013 "Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio (SGCN). Especificaciones".
[9] Certified Information Security Manager (CISM)

5. Programa

El curso se desarrolla en tres temas:

Tema 1 - Fundamentos de seguridad y riesgos de la información en las organizaciones

Incluye 3 unidades didácticas que requieren una dedicación total de 100 horas: 28 horas de clase, 38 horas de actividades prácticas y 34 horas de estudio.

U.D.	Descripción de las Unidades Didácticas	Horas
UD1	**Estándares internacionales de buenas prácticas de seguridad de la información en las organizaciones:** Las normas ISO 27002, ISO 27001, Esquema Nacional de Seguridad (ENS). INTECO. ENISA. NIST	30
UD2	**Los riesgos de seguridad de la información:** Normas internacionales y metodologías utilizadas en el análisis y gestión de riesgos de la información (AGR).	42
UD3	**Gestión y liderazgo en seguridad y auditoría:** Liderazgo en el ejercicio profesional. Habilidades de comunicación y negociación. La gestión del tiempo. Orientación al cliente. Desarrollo personal.	28

Tema 2 - Fundamentos científicos de la seguridad

Incluye 2 unidades didácticas que requieren una dedicación total de 100 horas: 20 horas de clase, 36 horas de actividades prácticas y 44 horas de estudio.

U.D.	Descripción de las Unidades Didácticas	Horas
UD4	**Criptología: Criptografía y Criptoanálisis.** Técnicas criptográficas clásicas y modernas. Protocolos criptográficos. Criptoanálisis. Firma Digital	56
UD5	**Biometría.** Técnicas biométricas basadas en características físicas Técnicas basadas en el comportamiento.	44

Tema 3 - Diseño e implantación de Sistemas de Gestión de Seguridad de la Información SGSI

Incluye 10 unidades didácticas que requieren una dedicación total de 400 horas: 104 horas de clase**, 144** horas de actividades prácticas y **152** horas de estudio.

U.D.	Descripción de las Unidades Didácticas	Horas
UD6	**La seguridad física y del entorno.** Caso Práctico: Proyecto de implantación.	29
UD7	**Control de accesos al sistema.** Gestión de identidades. Control de acceso a la red, sistemas y aplicaciones. Detección de accesos no autorizados. Registro de eventos. Aplicación de La Firma Electrónica y Certificación por Terceras Partes (PKI)	36
UD8	**La seguridad en las comunicaciones** Mecanismos de protección. Construcción de perímetros de seguridad. Ataques a las redes. Supuestos prácticos.	36
UD9	**Seguridad en la operación de ordenadores y redes.** La preparación de los datos. La gestión de librerías. Planificación de la capacidad y evaluación del rendimiento. Niveles de servicio. Controles de acceso al sistema.	32
UD10	**La seguridad en SS.OO. Entornos virtuales, Arquitecturas Cloud y SGBD:** Supuestos prácticos y controles	34
UD11	**Seguridad en las aplicaciones:** Modelo de madurez de seguridad de software (Software Assurance Maturity Model - SAMM). Seguridad en ERP´s y Comercio electrónico	42
UD12	**La Seguridad y las personas:** Controles de seguridad e identificación de las personas, Planes de formación en seguridad de las personas. Ejemplos prácticos	36
UD13	**Plan de Continuidad de Negocio (PCN):** Conceptos fundamentales, principios y metodología de diseño e implantación del PCN según ISO 22301. Resolución de casos prácticos.	54
UD14	**Seguridad en el cumplimiento legal:** Derechos Fundamentales a la Intimidad y a la protección de datos de carácter personal. El Documento de Seguridad de la LOPD y RD1720	36
UD15	**Preparación para la certificación CISM de ISACA** - (Certified Information Security Manager).	65

6. Desarrollo del curso

A) Impartición de las clases: El curso es impartido en modalidad presencial y online, con horarios de clase compatibles con las actividades laborales:

- Viernes de 17,00 a 22,00 horas
- Sábados de 9,00 a 14,00 horas

B) Material didáctico: Para realizar el curso se facilita documentación completa para el estudio y actividades prácticas.

C) Actividades a realizar: Las actividades a realizar en el curso están organizadas en Test, Cuestiones y Ejercicios. Cada profesor decide las actividades a realizar con la unidad didáctica impartida:

- Los test tienen como finalidad permitir verificar la comprensión de los conceptos fundamentales sobre los que versa la unidad didáctica.
- Las cuestiones son preguntas breves a las que el alumno ha de responder relacionadas con la unidad didáctica que está estudiando. La finalidad de las mismas es que el alumno pueda sintetizar los conceptos solicitados.
- Los ejercicios propuestos permiten la aplicación práctica de los temas estudiados en las unidades didácticas y/o tratados en las clases.

D) Foro de alumnos: Mientras se desarrolla el curso está disponible un Foro en el que alumnos y profesores compartirán opiniones sobre temas de actualidad relacionados con el curso y también para aclarar las dudas que puedan presentarse en el estudio y realización de las prácticas.

7. Prerrequisitos, Certificaciones y Titulación

a) Requisitos de admisión

Para realizar el curso es necesario poseer un título universitario oficial de cualquier universidad española o universidad extranjera homologada por la UAH.

Dada la naturaleza de los temas tratados en el curso, en el proceso de admisión se tendrán en cuenta los conocimientos fundamentales de informática de los alumnos interesados en realizar el curso.

b) Medios imprescindibles disponibles por los alumnos

Así mismo para participar en el curso, los asistentes deben:

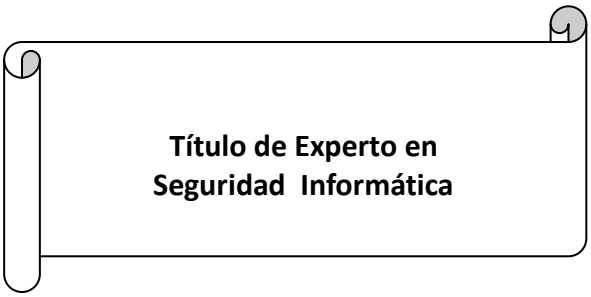
- Disponer de un PC equipado para conectarse a Internet, con cualquiera de los navegadores más utilizados y un procesador de textos (Word o similar) y cuenta de correo electrónico.

c) Observaciones sobre la preparación para la Certificación CISM

Es decisión del alumno presentarse a los exámenes de certificación realizados por las organizaciones, debidamente autorizadas y acreditadas en España. En el curso se imparte la preparación encaminada a su obtención.

d) Titulación

A los alumnos que asistan con normalidad a las clases y realicen las actividades prácticas incluidas en el curso con la evaluación de los profesores, obtendrán el titulo de postgrado emitido por la UAH.



8. Los puestos de Responsables de Seguridad y Jefe de Seguridad Informática

8.1 Responsables de seguridad informática

- Analizar y Gestionar los riesgos del sistema informático, determinar sus vulnerabilidades y establecer las medidas de salvaguarda que garanticen la confidencialidad, integridad y disponibilidad de la información de acuerdo a un riesgo residual asumido por la organización.
- Definir, de acuerdo a los objetivos de seguridad establecidos en la organización, la seguridad de los sistemas informáticos.
- Colaborar en la definición de las Políticas de seguridad.
- Organización de la seguridad y clasificación de los recursos.
- Seguridad física y del entorno.
- Protección y control de acceso al sistema.

- Seguridad en las Comunicaciones.
- Seguridad en la operación y producción.
- Seguridad en el software tanto de los sistemas operativos, bases de datos y aplicaciones.
- Seguridad en las personas que le utilizan.
- Definir las especificaciones de seguridad para que los sistemas informáticos cumplan la legislación y normas estándar de seguridad nacionales e internacionales.
- Diseñar la seguridad del sistema informático según las especificaciones establecidas.
- Dirigir los proyectos de seguridad basados en las leyes y normas estándar que permiten a la organizaciones públicas y privadas validar (ó certificar) su cumplimiento y obtener las acreditaciones de seguridad exigidas por ley y normas adoptadas.
- Gestionar el plan de seguridad informática y mantenerle actualizado, muy especialmente el plan de continuidad del negocio.
- Velar por el cumplimiento legal de los sistemas informáticos utilizados en la organización: datos personales, propiedad intelectual, software legal, etc.
- Colaborar con la Dirección en la resolución de incidentes de seguridad y especialmente en aquellos que puedan dar origen a delitos y faltas tipificados en el derecho Penal, Civil, Convenios internacionales, etc.

8.2 Jefe de seguridad informática

- Definición de las políticas y procedimientos de seguridad.
- Implantación práctica de la seguridad en la organización.
- Mecanismos de registro de actividad y recuperación de errores.
- Velar por mantener un adecuado nivel de riesgo en la organización y establecer el riesgo residual latente.
- Velar por la adecuación de los planes de continuidad del negocio.
- Verificar los incidentes de seguridad y proponer medidas correctoras.

9. Patrocinadores