CPITICM
Colegio Profesional de
Ingenieros Técnicos en Informática
de la Comunidad de Madrid

Universidad de Alcalá

Curso de postgrado en Auditoría Informática

Mayo 2014

Secretaría Técnica
C/ Mayor, 4 6ª planta – 28013 Madrid • Tel: 91.523.86.20 • Fax: 91.521.48.25 • secretaria@cpiticm.es • www.cpiticm.es

CPITICM
Colegio Profesional de
Ingenieros Técnicos en Informática
de la Comunidad de Madrid

Universidad de Alcalá

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, informes y proyectos en el ámbito de la auditoría informática.

Estos conocimientos son fundamentales y una exigencia para los profesionales de la auditoría, de forma análoga a como se lleva a cabo la auditoría en otros ámbitos como: Medio ambiente, Industria, Sanidad, Financiero, Calidad, etc.

La auditoría informática también es un instrumento clave para realizar las "certificaciones" basadas en normas UNE, ISO, etc. de sistemas, productos y servicios basados en la informática.

Cada vez son más las leyes que exigen la auditoría de los sistemas de información como instrumento de control y garantía de cumplimiento. Entre las más conocidas se pueden citar: LOPD[1] y Real Decreto que la desarrolla[2], ENS[3], EJIS[4], etc.

La auditoría informática definida por Ron Weber en 1988 como:

> ***"El proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informático salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización y utiliza eficientemente los recursos"***

Es actualmente una gran necesidad en organizaciones públicas y privadas. El propio desarrollo de la sociedad de la información ha aumentado tanto los riesgos como la cantidad y complejidad de los sistemas y servicios informáticos que utilizamos basados en arquitecturas web interconectados en redes abiertas e inseguras de las que Internet es el mayor exponente.

Las organizaciones públicas y privadas precisan controlar, medir y sopesar los riesgos a los que pueden estar sometidos sus sistemas, adaptarlos a las leyes y normas vigentes, conocer en todo momento el estado en el que se encuentran y tener capacidad de maniobra para poder responder ante cualquier eventualidad y generar confianza.

El objetivo del curso es formar para capacitar a los profesionales para la realización de AUDITORÍAS INFORMÁTICAS.

---

[1] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter persona

[2] 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.

[3] 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.

[4] 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 curso es un gran proyecto educativo que ha sido **Galardonado por la Revista SIC[5], ** 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 profesional:

- **Concretar las necesidades formativas en Auditoría en los núcleos fundamentales de los conocimientos teóricos y prácticos que se precisan.**
- **Formación para la obtención de certificaciones internacionales, necesarias en el mercado de las TI**
- **Ampliar los conocimientos teóricos y prácticos dando a sus programas una estructura modular:** Con cursos que incluyen nuevas áreas de conocimientos: tanto en el ámbito de la dirección y gestión de las áreas de la Auditoría y de Seguridad Informática, como en la dirección de los proyectos a llevar a cabo.

2. Objetivos

- Formación de alto nivel con los conocimientos y destrezas que se requieren para el ejercicio profesional como Auditores de TI en administraciones públicas y organizaciones privadas, en un contexto internacional.

- 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 desarrollar la carrera en este ámbito, así como si ya se está desarrollando, profundizar en su conocimiento.

3. Dirigido para

- Desempeñar los puestos de Auditor en Informática en organizaciones privadas y públicas.

- Orientar el desarrollo profesional en las tareas exigibles a los Auditores en Informática y optar a puestos de trabajo bien retribuidos a nivel nacional e internacional.

4. Contenidos

[5] SIC Seguridad en Informática y Comunicaciones

El curso se desarrolla en tres temas:

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

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 ha de desarrollar el auditor.

Tema 2 - Marcos de referencia y metodologías utilizadas en auditoría.

Dedicado tanto a conocer los conceptos básicos de auditoría, como los marcos de referencia para llevarlas a cabo, en particular el marco creado por ISO según el estándar ISO 19011 y el marco desarrollado por ISACA a través de CobiT. Ambos marcos son tratados con múltiples prácticas en las distintas situaciones reales a las que el auditor tiene que enfrentarse. También se presentan las metodologías y técnicas utilizadas por el auditor y las aplicaciones informáticas de ayuda a la auditoría (Computer Assisted Audit Tools – CAATs)

Tema 3 - Supuestos de Auditoría, Acreditaciones y Certificaciones.

La formación del auditor requiere del conocimiento de múltiples supuestos prácticos que se presentan en la auditoría informática. En la primera parte se tratan los principales supuestos de auditoría y la forma de llevarlos a cabo: *Controles Generales; Acceso a los Sistemas; Los Datos y Bases de Datos, Los sistemas, Las comunicaciones; Entornos Web; Servicios TI, Auditoría de ERP, etc.*; Auditoria del Plan de Continuidad de Negocio; Auditoría exigida por la LOPD y RDLOPD.

La segunda parte de este tema está dedicada a dar a conocer las acreditaciones procedimientos y entidades de acreditación y a preparar al alumno para que, si lo desea, se presente a la obtención de la certificación CISA®[6], muy valorada a nivel mundial y con gran frecuencia exigida por grandes y medianas empresas en la contratación de auditores internos y externos.

[6] Certified Information Systems Auditor (CISA)

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 auditoría y seguridad:** Liderazgo en el ejercicio profesional. Habilidades de comunicación y negociación. La gestión del tiempo. Orientación al cliente. Desarrollo personal.	28

Tema 2 - Marcos de referencia y metodologías utilizadas en auditoría

Incluye 5 unidades didácticas que requieren una dedicación total de 225 horas: 48 horas de clase, 81 horas de actividades prácticas y 96 horas de estudio.

U.D.	Descripción de las Unidades Didácticas	Horas
UD4	**Conceptos básicos de Auditoria:** Naturaleza, tipos de auditoría, responsabilidades del auditor. Evidencias; la independencia del auditor. El concepto de cumplimiento. Legislación sobre auditoría. Ética y Código Profesional.	36
UD5	**Marco de referencia ISO:** Auditoría de los sistemas de gestión según el estándar ISO 19011: - Auditoría del SGSI según ISO 27001 - Auditoria del SGSI según el ENS	42

U.D.	Descripción de las Unidades Didácticas	Horas
UD6	**Marco de referencia CobiT:** Objetivos de Control. Su implantación. Guías de Auditoría: Casos Prácticos. Gobierno de TI, Val IT.	61
UD7	**Metodologías y técnicas del Auditor:** Desarrollo de procesos y Aseguramiento de TI. Técnicas estadísticas El Informe de Auditoría. Certificaciones de Control.	50
UD8	**Aplicaciones Informáticas de ayuda a la Auditoría:** Computer Assisted Audit Tools - CAATs	36

Tema 3 - Supuestos de Auditoría, Acreditaciones y Certificaciones

Incluye 5 unidades didácticas que requieren una dedicación total de 275 horas: 76 horas de clase, 99 horas de actividades prácticas y 100 horas de estudio.

U.D.	Descripción de las Unidades Didácticas	Horas
UD9	**Prácticas de Auditoría en Informática.** - Controles Generales. - El Acceso a los Sistemas. - Los Datos/ Bases de Datos. - Auditoría de ERP - Las Comunicaciones. - Los entornos Web. - Auditoría de Sistemas. - Auditoría de Servicios de TI. - Auditoria de Proyectos T.I. - Auditoría de Código	90
UD10	**Auditoría del Plan de Continuidad de Negocio (PCN):** Conceptos fundamentales y principios del PCN según la norma ISO 22301. Auditoría del PCN casos prácticos y certificaciones	54
UD11	**Auditorías de cumplimiento legal:** Derechos Fundamentales a la Intimidad y a la protección de datos de carácter personal. - Auditoría basada en la LOPD y RD1720.	48
UD12	**Acreditación de organizaciones y profesionales:** Organizaciones de acreditación. Normas de acreditación de organizaciones y personas. Acreditación de Auditores.	18
UD13	**Preparación para la certificación CISA de ISACA** - (Certified Information Systems Auditor®).	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 17,30 a 21,30 horas
- Sábados de 9,30 a 13,30 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:

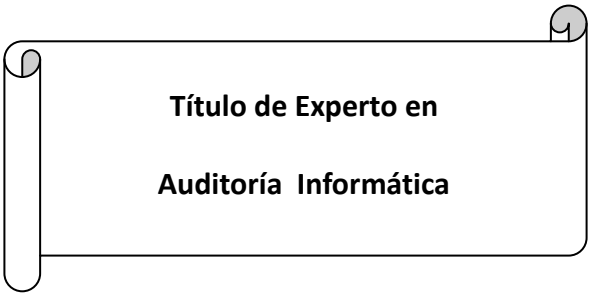
- Disponer de un PC equipado para conectarse a Internet, con cualquiera de los navegadores más utilizados y un procesador de textos (Word o similar) y cuenta de correo electrónico.

c) Observaciones sobre la preparación para la Certificación CISA

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. El puesto de Auditor en Informática

Este apartado describe las principales actividades en el desempeño del puesto de **Auditor en Informática**

- Recoger, agrupar y evaluar evidencias para efectuar diagnóstico de los sistemas informáticos desde diferentes ángulos: técnico, organizativo, funcional, económico, legal, normativo y humano.

- Determinar si en el análisis, diseño, construcción y explotación (producción) de un sistema informático se han considerado y evaluado los riesgos y si se han establecido las salvaguardas adecuadas para mantener la confidencialidad, integridad, disponibilidad y no repudio de la información tratada por dicho sistema.

- Determinar si un sistema informático salvaguarda los activos y lleva a cabo los fines encomendados para la organización a la que da servicio.

- Determinar la eficiencia y eficacia del sistema informático teniendo en cuenta los objetivos de la organización con los que debe de estar alineado y los recursos utilizados.

- Verificar la conformidad del sistema informático con la legislación aplicable, o con normas estándar nacionales e internacionales exigidas por las organizaciones públicas ó privadas tanto en su construcción, como en su explotación (producción) posterior.

- Emitir informes de Auditoría Informática para las Administraciones Públicas y para las Organizaciones privadas y especialmente las establecidas por las leyes y reglamentos vigentes.

- Realizar Informes de Auditoría sobre aspectos concretos de los sistemas informáticos: Planificación y Gestión; Acceso a los sistemas; Datos y Bases de Datos; Desarrollo y Calidad del Software; Canales de Distribución, Eficacia; Eficiencia de su gestión, etc.

- Proponer las soluciones de mejora, en base a los informes emitidos y controlar su implantación.

9. Patrocinadores

exevi
efficiency through technology