(Auditoría y Certificación de Sistemas Informáticos)

Guía de Aprendizaje – Información al estudiante

1. Datos Descriptivos

Titulación	Master Oficial Universitario en Ingeniería Informática
Módulo	Modulo Tecnologías informáticas
Materia	Auditoria y Calidad del Software y Sistemas
Asignatura	Auditoria y Certificación de Sistemas Informáticos
Carácter	Obligatoria
Créditos ECTS	6
Departamento responsable	Lenguajes y Sistemas Informáticos e Ingeniería Software
Especialidad	

Curso académico	2013-2014
Semestre en que se imparte	2º semestre del curso
Idioma en él que se imparte	Español
Página Web	

2. Profesorado

NOMBRE Y APELLIDO	DESPACHO	Correo electrónico
Edmundo Tovar (Coord.)	5111	etovar@fi.upm.es
Jose Domingo Carrillo	5107	jcarrillo@fi.upm.es

3. Conocimientos previos requeridos para poder seguir con normalidad la asignatura

Asignaturas superadas	• Gobernanza y Gestión de TI
Otros resultados de aprendizaje necesarios	• Conocimientos previos equivalentes al grado de Ingeniería Informática

4. Objetivos de Aprendizaje

COMPETENCIAS ESPECÍFICAS ASIGNADAS A LA ASIGNATURA Y SU NIVEL DE ADQUISICIÓN		
Código	**Competencia**	**Nivel**
CE6	Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas y productos informáticos	S
CE7	Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido	P
CE16	Habilidad para hacer conexiones entre los deseos y necesidades del consumidor o cliente y lo que la tecnología puede ofrecer.	S
CE18	Capacidad para comprender el mercado, sus hábitos y necesidades de productos o servicios tecnológicos	P

Nivel de competencia: conocimiento (C), comprensión (P), aplicación (A) y análisis y síntesis (S),

RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA			
Código	**Resultado de aprendizaje**	**Competencias asociadas**	**Nivel de adquisición**
RA1	Maneja con soltura los conceptos relacionados con riesgos de las TI	CE6	S
RA2	Define y evalúa controles a implantar en Sistemas de Información utilizando un marco de mejores prácticas	CE6	S
RA3	Aplica técnicas para realizar auditorías de Sistemas de Información	CE6, CE16	S,P
RA4	Organiza el plan de trabajo de un equipo de auditoría	CE6	S
RA5	Diseña e implanta controles de seguridad establecidos en un Sistema Informático	CE7	P
RA6	Certifica el Sistema de Gestión de la Seguridad	CE7, CE18	P, P
RA7	Conoce el concepto de certificación y mecanismos de funcionamiento	CE6, CE7	C

5. Sistema de evaluación de la asignatura

INDICADORES DE LOGRO		
Ref	**Indicador**	**Relacionado con RA**
I1	Ha aplicado correctamente de la metodología de análisis de riesgos	RA1
I2	La presentación del caso de análisis de riesgos ha sido comprendida por el resto de compañeros	RA1
I3	Han identificado y definido correctamente los controles de TI que hay que implantar en el caso de negocio utilizando COBIT	RA2
I4	Han identificado y definido correctamente los controles de seguridad que hay que implantar en el caso de negocio utilizando la ISO 27002	RA5
I5	Puntuación obtenida en el examen de certificación de la ISO 27000	RA6
I6	Sabe resolver un ejercicio utilizando alguna de las técnicas de auditoría estudiadas	RA3
I7	El informe de auditoría elaborado está bien organizado y presenta resultados adecuados en cada apartado	RA2, RA4
I8	Contesta a un cuestionario de nivel de conocimiento sobre la materia	RA(1-7)

EVALUACION SUMATIVA			
Breve descripción de las actividades evaluables	**Momento**	**Lugar**	**Peso en la calif.**
Realización de un análisis de riesgo (Caso de Magerit) por grupos y presentación en clase	Semana 3	Aula, Sala de trabajo	10
Desarrollo de controles en un caso de negocio	Semana 4	Sala de trabajo	5%

EVALUACION SUMATIVA			
Breve descripción de las actividades evaluables	**Momento**	**Lugar**	**Peso en la calif.**
Desarrollo de un caso práctico de auditoría. Elaboración de un informe	Semana 6	Sala de trabajo	20%
Desarrollo de controles de seguridad en un caso de negocio	Semana 8	Sala de trabajo	5%
Examen de certificación	Semana 16	Aula	20%
Examen parcial 1	Semana 8	Aula	35%
Examen final	Semana 16	Aula	40%
			Total: 100%

En virtud de lo establecido en la normativa de exámenes de la UPM, en la convocatoria ordinaria, la elección entre el sistema de evaluación continua o el sistema de evaluación mediante sólo prueba final corresponde al estudiante. En el caso de la Facultad de Informática, esto sólo es aplicable a los títulos de Grado en Ingeniería Informática, Grado en Matemáticas e Informática y Máster Universitario en Ingeniería Informática.

El plazo, conforme a los plazos indicados en dicha normativa (artículo 20), que se fija para realizar esta opción es de una semana a contar desde el inicio de la actividad docente de la asignatura, por comunicación directa por escrito al coordinador de la asignatura.

CRITERIOS DE CALIFICACIÓN

Exámenes.

Se realizarán dos exámenes parciales. La realización de los trabajos prácticos y el aprobado en ambos exámenes, permitirán aprobar la asignatura.

Asistencia a Clase.

Será necesario haber asistido al 80% de las clases.

Prácticas.

Se realizarán prácticas por grupo e individualmente lo largo del curso.

Evaluación

La ponderación de los distintos trabajos y exámenes en la nota final de la asignatura aparecen en el cuadro de “Evaluación Sumativa” de esta guía, para el caso de evaluación continua.

6. Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS		
Bloque / Tema / Capítulo	**Apartado**	**Indicadores Relaciona-dos**
Tema 1: Análisis y Gestión de Riesgos	1.1 Relación entre gobernanza de TI, riesgos y cumplimiento	I8
	1.2 Organización de la función de Riesgos en la empresa (ISO31000 y COSO)	I8
	1.3 Análisis de Riesgos de la Información (ISO27006)	I1, I2
	1.4 Gestión de Riesgos de la Información (ISO 27006)	I1, I2
	1.5 Métodos, Técnicas y Herramientas para el Análisis la Gestión de Riesgos	I8
Tema 2: Definición e Implantación de controles	2.1 Marco de control interno	I8
	2.2 Definición, desarrollo, implantación y prueba de controles	I3
	2.3 Estudio y aplicación de marcos objetivos de control (COBIT, ValueIT)	I3
Tema 3: Organización y desarrollo de una auditoría de SI	3.1 Organización de la función de Auditoría	I7
	3.2 El proceso de auditoría. Conceptos generales e Informe de auditoría	I3, I7
	3.3 Conceptos financieros para un auditor	I8
	3.4 Certificación del auditor (CISA)	I8
Tema 4. Técnicas y Herramientas para el desarrollo de una auditoría de SI	4.1 Principales técnicas a utilizar en auditoría. Concepto de CAATS	I6
	4.2 Taxonomía de herramientas	I6
	4.3 Metodología para seleccionar la herramienta CAATS	I6
Tema 5. Gobernanza y Gestión de la Seguridad de la Información. Controles de Seguridad (ISO	5.1 Gobernanza de la Seguridad de la Información. Organización de la seguridad de la información en la empresa	I8
	5.2 Sistema de Gestión de la Seguridad de la Información (ISO 27001)	I4

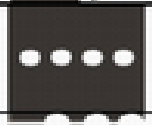
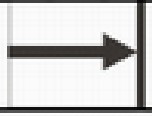
POLITÉCNICA

7. Breve descripción de las modalidades organizativas utilizadas y de los métodos de enseñanza empleados

Tabla 7. Modalidades organizativas de la enseñanza

MODALIDADES ORGANIZATIVAS DE LA ENSEÑANZA		
Escenario	**Modalidad**	**Finalidad**
	Clases Teóricas	*Hablar a los estudiantes*
	Seminarios-Talleres	*Construir conocimiento a través de la interacción y la actividad de los estudiantes*
	Clases Prácticas	*Mostrar a los estudiantes cómo deben actuar*
	Prácticas Externas	*Completar la formación de los alumnos en un contexto profesional*
	Tutorías	*Atención personalizada a los estudiantes*
	Trabajo en grupo	*Hacer que los estudiantes aprendan entre ellos*
	Trabajo autónomo	*Desarrollar la capacidad de autoaprendizaje*

Table 8. Métodos de enseñanza

MÉTODOS DE ENSEÑANZA		
	Método	**Finalidad**
	**Método Expositivo/Lección Magistral**	***Transmitir conocimientos y activar procesos cognitivos en el estudiante***
	**Estudio de Casos**	***Adquisición de aprendizajes mediante el análisis de casos reales o simulados***
	**Resolución de Ejercicios y Problemas**	***Ejercitar, ensayar y poner en práctica los conocimientos previos***
	**Aprendizaje Basado en Problemas (ABP)**	***Desarrollar aprendizajes activos a través de la resolución de problemas***
	**Aprendizaje orientado a Proyectos**	***Realización de un proyecto para la resolución de un problema, aplicando habilidades y conocimientos adquiridos***
	**Aprendizaje Cooperativo**	***Desarrollar aprendizajes activos y significativos de forma cooperativa***
	**Contrato de Aprendizaje**	***Desarrollar el aprendizaje autónomo***

Se conoce como método expositivo *"la presentación de un tema lógicamente estructurado con la finalidad de facilitar información organizada siguiendo criterios adecuados a la finalidad pretendida"*. Esta metodología -también conocida como lección (*lecture*)- se centra fundamentalmente en la exposición verbal por parte del profesor de los contenidos sobre la materia objeto de estudio. El término "lección magistral" se suele utilizar para denominar un tipo específico de lección impartida por un profesor en ocasiones especiales.

Análisis intensivo y completo de un hecho, problema o suceso real con la finalidad de conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y, en ocasiones, entrenarse en los posibles procedimientos alternativos de solución.

Situaciones en las que se solicita a los estudiantes que desarrollen las soluciones adecuadas o correctas mediante la ejercitación de rutinas, la aplicación de fórmulas o algoritmos, la aplicación de procedimientos de transformación de la información disponible y la interpretación de los resultados. Se suele utilizar como complemento de la lección magistral.

Método de enseñanza-aprendizaje cuyo punto de partida es un problema que, diseñado por el profesor, el estudiante ha de resolver para desarrollar determinadas competencias previamente definidas.

Método de enseñanza-aprendizaje en el que los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado para resolver un problema o abordar una tarea mediante la planificación, diseño y realización de una serie de actividades, y todo ello a partir del desarrollo y aplicación de aprendizajes adquiridos y del uso efectivo de recursos.

Enfoque interactivo de organización del trabajo en el aula en el cual los alumnos son responsables de su aprendizaje y del de sus compañeros en una estrategia de corresponsabilidad para alcanzar metas e incentivos grupales.
Es tanto un método, a utilizar entre otros, como un enfoque global de la enseñanza, una filosofía.

Un acuerdo establecido entre el profesor y el estudiante para la consecución de unos aprendizajes a través de una propuesta de trabajo autónomo, con una supervisión por parte del profesor y durante un período determinado. En el contrato de aprendizaje es básico un acuerdo formalizado, una relación de contraprestación recíproca, una implicación personal y un marco temporal de ejecución.

BREVE DESCRIPCIÓN DE LAS MODALIDADES ORGANIZATIVAS UTILIZADAS Y METODOS DE ENSEÑANZA EMPLEADOS	
CLASES DE TEORIA	
SEMINARIOS TALLERES	Explicación de técnicas para el desarrollo de controles en un caso de negocio Explicación para el desarrollo de controles de seguridad en un caso de negocio
CLASES PRÁCTICAS	Aplica técnicas para realizar auditoría de Sistemas de Información
PROYECTO	Desarrollo de un caso práctico de auditoría. Elaboración de un informe
TRABAJOS AUTONOMOS	Estudiar, analizar artículos proporcionados para los temas de Riesgos y Control de Seguridad
TRABAJOS EN GRUPO	Desarrollo de un análisis y gestión de riesgos Desarrollo de controles en un caso de negocio Desarrollo de controles de seguridad en un caso de negocio
TUTORÍAS	Presenciales. Aclaración de dudas para la certificación de la ISO 27000 Las individuales por Internet

8. Recursos didácticos

RECURSOS DIDÁCTICOS	
BIBLIOGRAFÍA	Normas ISO 38500, 31000, 27001, 27002, 27004, 27006, 15408
	COBIT 4.1
	Marco para el desarrollo de una auditoría de TI, ISACA
	Manual para la certificación de ISO27000
	Normas y decretos oficiales sobre organismos de certificación
RECURSOS WEB	Página web de la asignatura (http://)
	Sitio Moodle de la asignatura (http://) Campus virtual UPM
EQUIPAMIENTO	
	Aula de trabajo colaborativo
	Sala de trabajo en grupo

9. Cronograma de trabajo de la asignatura

Semana	Actividades en Aula	Actividades en Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades de Evaluación	Otros
Semana 1 (7 horas)	1.1 Relación entre gobernanza de TI, riesgos y cumplimiento 2 horas 1.2 Organización de la función de Riesgos en la empresa (ISO31000 y COSO) 1 hora	(horas)	Estudio (4 horas)	(horas)	(horas)	
Semana 2 (11 horas)	1.3 Análisis de Riesgos de la Información (ISO27006) 2 horas 1.4 Gestión de Riesgos de la Información (ISO 27006) 1 hora	(horas)	Estudio (4 horas) Estudiar, analizar artículos proporcionados para los temas de Riesgos (4 horas)	(horas)	(horas)	
Semana 3 (15 horas)	1.4 Gestión de Riesgos de la Información (ISO 27006) 1 hora 1.5 Métodos, Técnicas y Herramientas para el Análisis la Gestión de Riesgos 2	(horas)	Estudio (4 horas)	Desarrollo de análisis de riesgos (8 horas)	(horas)	

	horas					
Semana 4 (13 horas)	2.1 Marco de control interno 1 hora 2.2 Definición, desarrollo, implantación y prueba de controles 2 horas	(horas)	Estudio (4 horas)	Trabajo de controles (6 horas)	(horas)	
Semana 5 (13 horas)	2.2 Definición, desarrollo, implantación y prueba de controles1 hora 2.3 Estudio y aplicación de marcos objetivos de control (COBIT, ValueIT) 2 horas	(horas)	Estudio (4 horas)	Trabajo de controles (6 horas)	(horas)	
Semana 6 (13 horas)	2.3 Estudio y aplicación de marcos objetivos de control (COBIT, ValueIT) 1 hora 3.1 Organización de la función de Auditoría 2 horas	(horas)	Estudio (4 horas)	Proyecto auditoría (6 horas)	(horas)	
Semana 7 (13 horas)	3.2 El proceso de auditoría. Conceptos generales e Informe de auditoría (3 horas)	(horas)	Estudio (4 horas)	Proyecto auditoría (6 horas)	(horas)	
Semana 8 (9 horas)	3.3 Conceptos financieros para un auditor (3 horas)	(horas)	Estudio (4 horas)	(horas)	Examen (2 horas)	
Semana 9 (5 horas)	3.4 Certificación del auditor (CISA) 1 hora 4.1 Principales técnicas a utilizar en auditoría. Concepto de CAATS 2 horas	(horas)	Estudio (2 horas)	(horas)	(horas)	
Semana 10 (7 horas)	4.1 Principales técnicas a utilizar en auditoría. Concepto de CAATS 1 hora 4.2 Taxonomía de herramientas 1 hora 4.3 Metodología para	(horas)	Estudio (4 horas)	(horas)	(horas)	

Nota: Para cada actividad se especifica la dedicación en horas que implica para el alumno.