

<b>FICHA DE LA ASIGNATURA AUDITORÍA Y ANÁLISIS DE RIESGOS</b>			
<b>CARÁCTER:</b>	Obligatorio	<b>LENGUA/S EN LA/S QUE SE IMPARTE:</b>	Español
<b>ECTS:</b>	4	<b>CUATRIMESTRE</b>	1
<b>Asignatura de la MATERIA REGULACIÓN</b>			
<b>PROFESORES QUE IMPARTEN LA ASIGNATURA</b>			
Gerardo Aburruzaga García Juan Boubeta Puig (coordinador) Antonia Estero Botaro (coordinadora)			
<b>COMPETENCIAS QUE SE ADQUIEREN:</b> <i>(indicar código)</i>			
<b>Comp. Básicas</b>	<b>Comp. Generales</b>	<b>Comp. Específicas</b>	<b>Comp. Transversales</b>
CB6 CB9 CB10	CG3	CE1 CE2	CT1
<b>RESULTADOS DE APRENDIZAJE:</b> Distinguir entre auditoría interna, externa y control interno. Conocer el marco jurídico y las normas internacionales relacionadas con la auditoría informática. Conocer las fases de realización de una auditoría informática, las fuentes de información y procedimientos de obtención de información. Conocer la estructura y características que debe reunir un informe de auditoría informática. Conocer los objetivos y metodologías existentes para el análisis y gestión de riesgos. Conocer cuáles son las etapas del proceso de análisis y gestión de riesgos, y ser capaz de llevarlas a la práctica.			
<b>CONTENIDOS:</b>  Tema 1: Auditoría 1.1 Concepto de auditoría informática 1.2 Marco jurídico de la auditoría informática 1.3 Control Interno Informático 1.4 Auditorías internas 1.5 Auditorías externas 1.6 Fases en la realización de una auditoría informática 1.7 Estándares relacionados con la auditoría informática  Tema 2: Análisis y gestión de riesgos de los sistemas de información 2.1 Objetivos de análisis y gestión de riesgos 2.2 Metodología de análisis y gestión de riesgos: MAGERIT 2.3 Etapas del proceso de análisis y gestión de riesgos 2.4 Identificación y valoración de activos 2.5 Dependencia entre activos 2.6 Identificación y valoración de amenazas 2.7 Identificación y valoración de salvaguardas 2.8 Cálculo del riesgo real y planificado 2.9 Plan de tratamiento de riesgos  <b>Prácticas:</b> Análisis y gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT			

<b>OBSERVACIONES / REQUISITOS PREVIOS:</b>			
<b>ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:</b>	<b>Id de la Actividad Formativa</b>	<b>Nº de horas</b>	<b>Presencialidad (%)</b>
	Clases teórico- prácticas	12	100%
	Clases prácticas	16	100%
	Seminarios y conferencias	4	100%
	Actividades académicas no presenciales	64	0%
	Evaluación	4	100%
<b>METODOLOGÍAS DOCENTES:</b>			
Lección magistral expositiva Resolución de problemas y casos prácticos Prácticas de ordenador Realización de trabajos			
<b>SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:</b>			
<b>Denominación Sistema Evaluación</b>	<b>Ponderación Mínima</b>	<b>Ponderación Máxima</b>	
Trabajos escritos realizados por el alumno	0 %	50 %	
Exposiciones de ejercicios, temas y trabajos	0%	30%	
Participación y trabajo realizado en actividades formativas	10%	30%	
Pruebas escritas u orales	30%	90%	
<b>BIBLIOGRAFÍA RECOMENDADA:</b>			
The Basics of IT Audit: Purposes, Processes, and Practical Information Stephen D. Gantz Syngress Media Incorporated, 2013			
Brink's Modern Internal Auditing: A Commom Body of Knowledge Robert R. Moller John Wiley & Sons, 2015			
IT Audit, Control, and Security. Robert R. Moller. John Wiley & Sons, 2010			
Auditoría de seguridad informática MF0487_3			

Ester Chicano Tejada

IC Editorial, 2014

**Bibliografía complementaria:**

AENOR. <http://www.aenor.es/aenor/inicio/home/home.asp>

Information Systems Audit and Control Association (ISACA). <https://www.isaca.org>

National Institute of Standards and Technology. <http://www.nist.gov/>

Normativa ISO27000. <http://www.iso27000.es/>

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

<https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/metodologia.html>

PILAR: Herramienta de Análisis y Gestión de Riesgos de un Sistema de Información siguiendo la

Metodología MAGERIT: <https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html>