Auditoria y Certificación de Sistemas Informáticos

Curso Académico: (2016 / 2017) **Fecha de revisión: 29-05-2016**

Departamento asignado a la asignatura:

Coordinador/a: RIBAGORDA GARNACHO, ARTURO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No procede

OBJETIVOS

El alumno debe adquirir una serie de competencias genéricas, conocimientos, capacidades y actitudes, que se describen a continuación:
Competencias transversales genéricas:

- Capacidad de análisis y síntesis
- Capacidad de organizar y planificar
- Capacidad de abstracción y deducción.
- Resolución de problemas.
- Trabajo en equipo.
- Capacidad de aplicar los conocimientos en la práctica.

Competencias actitudinales:

- Capacidad para generar nuevas ideas (creatividad)
- Actitud crítica respecto a los conocimientos actuales
- Preocupación por la calidad de los programas y sistemas informáticos
- Motivación de logro
- Interés por investigar y buscar soluciones a nuevos problemas que presentan la auditoría y certificación de los sistemas informáticos

Competencias específicas del módulo de la materia:

1. Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.
2. 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.
3. Capacidad para aplicar los principios de la regulación y normalización de la informática.
4. Capacidad para proyectar, calcular y diseñar procesos de auditoría y certificación de sistemas informáticos.

Resultados de aprendizaje:

- Conocer las metodologías de evaluación y certificación de sistemas y productos de T.I.
- Conocer los acuerdos internacionales de reconocimiento mutuo de certificación de la seguridad y sus requisitos
- Conocer las normas y estándares nacionales, europeos e internacionales relativos a la seguridad de los sistemas de información, principalmente las normas de la familia ISO/IEC 27000
- Analizar y evaluar para su aplicación a un sistema específico diversas metodologías de auditoría
- Ser capaz de llevar a cabo una auditoría de la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos, y de su seguridad.
- Ser capaz de realizar una auditoría de conformidad con la legislación vigente de ficheros y sistemas conteniendo datos de carácter personal

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Normalización, evaluación, certificación y acreditación. Marco legal
2. Certificación de sistemas y productos de T.I.
3. La auditoría y la consultoría informática.
4. La normalización de los SGSI (ISMS). Familia 27xxx. Estudio de las normas UNE-ISO/IEC 27000, 27001, 27002.

5. Auditoría de sistemas distribuidos y redes. Auditoría de ciberseguridad.
6. Auditoría de ficheros y sistemas sujetos a cumplimiento legal.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Clases magistrales.

- Orientadas a la enseñanza de las competencias específicas de la materia. En ellas se presentarán los conocimientos que los alumnos deben adquirir. Para facilitar su desarrollo los alumnos recibirán las notas de clase y tendrán textos básicos de referencia que les permita completar y profundizar en aquellos temas en los cuales estén más interesados. Además, los estudiantes tendrán acceso a normas, estándares y disposiciones legales de uso común en auditoria y certificación de sistemas informáticos.

Prácticas individuales o en grupo.

- Dentro de esta materia se llevarán a cabo prácticas, que podrían ser en grupo. Entre otras actividades, los estudiantes podrían realizar auditorías de componentes determinados de sistemas y redes, para después sacar conclusiones y elaborar el correspondiente informe de auditoría, que podría presentarse en grupo. También llevarán a cabo la auditoría de cumplimiento del R. D. 1720/2007, de desarrollo de la Ley 15/1999 Orgánica de Protección de Datos, de ficheros y sistemas ficticios o reales anonimizados. Así mismo, dado un sistema en un entorno operacional determinado, deberán escoger aquellos productos o equipos de seguridad certificados que minimicen los riesgos que sufre.

Actividades académicamente dirigidas.

- Resolución de ejercicios y casos prácticos de forma participativa. Se incluirán, entre otras actividades el análisis y comentario crítico de informes de la Agencia Española de Protección de Datos (u Órganos correspondientes de alguna Autonomía que los tenga). Así mismo, dado un campo específico de las T.I., deberán hallar aquellos estándares de facto o de iure que lo regulan, comentando los aspectos relevantes de dicha normalización. Finalmente realizarán trabajos de auditoría de la calidad o de la seguridad de un sistema informático.

Trabajo personal y estudio del alumno.

- Orientado especialmente a la adquisición de la Capacidad para la autoorganización y planificación del trabajo individual y del proceso de aprendizaje.

SISTEMA DE EVALUACIÓN

La evaluación tiene como misión conocer el grado de cumplimiento de los objetivos de aprendizaje, por ello se valorará todo el trabajo del alumno, individual o colectivamente, mediante la evaluación continua de sus actividades a través de los ejercicios y exámenes, trabajos prácticos y otras actividades académicas formativas descritas anteriormente.
Se realizará una evaluación formativa a través de la realimentación continua, que permita al alumno evaluar qué conoce y qué se espera de él.
La nota final tendrá en cuenta las actividades individuales del alumno y las actividades de equipo. Las actividades llevadas a cabo durante el curso, individuales o en grupo, supondrán un 50% de la nota, mientras que el examen final individual constituirá el restante 50%. En todo caso, la realización de examen final es obligatoria, siendo necesario obtener, al menos, el 40% de la nota máxima posible en este examen para poder superar la asignatura.
Para la convocatoria extraordinaria, se pueden dar tres situaciones según que el estudiante:
a) Haya seguido el proceso de evaluación continua y desee mantener la nota de esta. En este caso, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.
b) No haya seguido el proceso de evaluación continua. En este caso, tendrá derecho a realizar un examen con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso.
c) Haya seguido el proceso de evaluación continua, pero desee ser calificado en la convocatoria extraordinaria en las mismas condiciones indicadas en el apartado b).

Peso porcentual del Examen Final:	50
Peso porcentual del resto de la evaluación:	50

BIBLIOGRAFÍA BÁSICA

- AENOR UNE-ISO/IEC 27000:2014. UNE-ISO/IEC 27001:2014. UNE-ISO/IEC 27002:2015., AENOR, 2014 Y 2015 (según se indica)
- ISACA CISA (Certified Information Systems Auditor) Review Manual, ISACA.
- ISACA CISM (Certified Information Security Manager), ISACA.

- ISACA COBIT (Information Systems Audit and Control Association) , ISACA.

- ISO/IEC ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model., ISO/IEC, 2009

- JTC1. ISO/IEC ISO/IEC 27007: 2011. Guidelines for information security management systems auditing, ISO/IEC, 2011

- PIATTINI, Mario y otros. Auditoría de Tecnologías y Sistemas de Información., RA-MA. , Madrid, 2008