

Asignatura: Auditoría de la Seguridad**Cuatrimestre:** 2º**ECTS:** 3**Carácter:** OB**Contenidos:**

ID	Descripción
C1	Los sistemas de información y su auditoría.
C2	Controles internos de los sistemas de información.
C3	El proceso de la auditoría de los sistemas de información y sus fases.
C4	Auditoría técnica de seguridad.
C5	Sistemas de gestión de seguridad de la información.

Competencias¹:

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7- Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
- CG1 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en el ámbito de la Ingeniería de Software.
- CG2 - Capacidad para dirigir, planificar y supervisar equipos multidisciplinares.

¹ CB: Competencia básica; CG: Competencia general; CE: Competencia específica ; CT: Competencia transversal

- CG3 - Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería de Software siguiendo criterios de calidad.
- CG4 - Capacidad para la dirección general, dirección técnica y dirección de proyectos de I+D+I, en empresas y centros tecnológicos, en el ámbito de la Ingeniería de Software.
- CG5 - Capacidad para la puesta en marcha, dirección y gestión de procesos de diseño y desarrollo de sistemas informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
- CG6 - Capacidad para aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.
- CE16- Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración entre todos los departamentos de una empresa o entidad.
- CE22 - Realizar un asesoramiento integral que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
- CT1 -Analizar de forma reflexiva y crítica las cuestiones más relevantes de la sociedad actual para una toma de decisiones coherente.
- CT2 -Identificar las nuevas tecnologías como herramientas didácticas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje grupal.
- CT3 - Aplicar los conocimientos y capacidades aportados por los estudios a casos reales y en un entorno de grupos de trabajo en empresas u organizaciones.
- CT4 - Adquirir la capacidad de trabajo independiente, impulsando la organización y favoreciendo el aprendizaje autónomo.

Metodologías docentes:

ID	Denominación	Descripción
MD1	Lección magistral	Presentación de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada.
MD2	Estudios de casos	Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.
MD3	Resolución de ejercicios y problemas	Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral.
MD4	Aprendizaje Basado en Problemas (ABP)	A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas.

ID	Denominación	Descripción
MD5	Contrato de Aprendizaje	Acuerdo establecido entre el profesor y el estudiante para la consecución de unos aprendizajes a través de una propuesta de trabajo autónomo, con la supervisión del profesor.

Temario:

Tema 1. Introducción a los Sistemas de Información y su auditoría

- 1.1 Introducción a los Sistemas de Información y el rol de la auditoría informática
- 1.2 Definiciones de «auditoría informática» y «control interno informático»
- 1.3 Funciones y objetivos de la auditoría informática
- 1.4 Diferencias entre control interno y auditoría informática

Tema 2. Controles internos de los Sistemas de Información

- 2.1 Organigrama funcional de un Centro de Proceso de Datos
- 2.2 Clasificación de los controles de los Sistemas de Información
 - 2.2.1 Controles generales
 - 2.2.2 Controles de aplicación
 - 2.2.3 Controles por área
 - 2.2.4 Controles de productos informáticos
 - 2.2.5 Controles por motivos legales
- 2.3 La regla de oro

Tema 3. El proceso y las fases de la auditoría de Sistemas de Información

- 3.1 Evaluación de Riesgos (EDR) y otras metodologías de auditoría informática
- 3.2 Ejecución de una auditoría de Sistemas de Información. Fases de auditoría
- 3.3 Habilidades fundamentales del auditor de Sistemas de Información

Tema 4. Auditoría técnica de seguridad en sistemas y redes

- 4.1 Auditorías técnicas de seguridad. Test de intrusión. Conceptos previos
- 4.2 Auditoría de seguridad en sistemas y áreas de desarrollo. Herramientas de apoyo
- 4.3 Auditoría de seguridad en redes. Herramientas de apoyo

Tema 5. Auditoría técnica de seguridad en internet y dispositivos móviles

- 5.1. Auditoría de seguridad en Internet. Herramientas de apoyo
- 5.2 Auditoría de seguridad en dispositivos móviles. Herramientas de apoyo
- Anexo 1: Estructura de informe ejecutivo e informe técnico
- Anexo 2: Inventario de herramientas
- Anexo 3: Metodologías

Tema 6. Sistema de Gestión de Seguridad de la Información

- 6.1 Seguridad de los SI: propiedades y factores de influencia

6.2 Riesgos empresariales y gestión de riesgos.

6.3 SG de la Seguridad de la Información (SGSI): concepto y factores críticos para el éxito

6.4 SGSI. Modelo PDCA

6.5 SGSI ISO/IEC 27001: objeto y alcance

6.6 Auditoría interna de SGSI

Bibliografía básica:

Aparte de los apuntes del profesor, se recomienda la siguiente bibliografía:

Álvarez Marañón, G. (2004). Seguridad Informática para empresas y particulares. Madrid: McGrawHill.

Andrés, A., y Gómez Guía, L. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes (2ª ed.). AENOR Ediciones.

Fernández, C. M., Piattini, M., y Peso, E. (2000). Auditoría Informática: Un enfoque práctico. Madrid: Editorial Ra-ma.

Fernández, C.M., Piattini, M. Pino, F. (2015). Modelo de Madurez de Ingeniería del Software. Madrid. Editorial: AENOR Ediciones.

González, P. (2014). Hacking ético. Editorial: OxWORD.