# Guía Didáctica - MASTER

## ASIGNATURA: Seguridad y auditorías de sistemas

Título: Máster Universitario en Ingeniería Informática

Materia: Tecnologías informáticas

Créditos: Ejemplo: 6 ECTS

viu | Universidad Internacional de Valencia

# Índice

# 1. Organización general

## 1.1. Datos de la asignatura

| | |
|---|---|
| **MATERIA** | **Tecnologías Informáticas** |
| **ASIGNATURA** | **Seguridad y auditorías de sistemas**<br>**6 ECTS** |
| **Carácter** | Obligatorio |
| **Curso** | Primero |
| **Cuatrimestre** | Primero |
| **Idioma en que se imparte** | Castellano |
| **Requisitos previos** | No existen |
| **Dedicación al estudio recomendada por ECTS** | 25 horas |

## 1.2. Introducción a la asignatura

## 1.3. Competencias y resultados de aprendizaje

### COMPETENCIAS GENERALES Y BÁSICAS

**CG03.** *Capacidad para dirigir, planificar y supervisar equipos multidisciplinares.*

**CG01.** *Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática.*

**CG02.** *Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio.*

**CG04.** *Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería en Informática.*

**CG05.** *Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería en Informática siguiendo criterios de calidad y medioambientales.*

**CG07.** *Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.*

**CG08.** *Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.*

**CG09.** *Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática.*

**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.*

## COMPETENCIAS ESPECÍFICAS DE LA ASIGNATURA

**CE04**. Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.

**CE05**. Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.

**CE06**. Capacidad para la dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.

**CE07.** 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.

**CE08.** Capacidad para analizar las necesidades de información que se plantean en un entorno y llevar a cabo en todas sus etapas el proceso de construcción de un sistema de información.

**CE09.** Capacidad para diseñar y evaluar sistemas operativos y servidores, y aplicaciones y sistemas basados en computación distribuida.

**CE10.** Capacidad para comprender y poder aplicar conocimientos avanzados de computación de altas prestaciones y métodos numéricos o computacionales a problemas de ingeniería.

**CE11.** Capacidad de diseñar y desarrollar sistemas, aplicaciones y servicios informáticos en sistemas empotrados y ubicuos.

**CE12.** Capacidad para aplicar métodos matemáticos, estadísticos y de inteligencia artificial para modelar, diseñar y desarrollar aplicaciones, servicios, sistemas inteligentes y sistemas basados en el conocimiento.

**CE13.** Capacidad para utilizar y desarrollar metodologías, métodos, técnicas, programas de uso específico, normas y estándares de computación gráfica.

**CE14.** Capacidad para conceptualizar, diseñar, desarrollar y evaluar la interacción persona-ordenador de productos, sistemas, aplicaciones y servicios informáticos.

**CE15.** Capacidad para la creación y explotación de entornos virtuales, y para la creación, gestión y distribución de contenidos multimedia.

# 2. Contenidos/temario

- Seguridad física. Principales amenazas: Acceso físico, Desastres naturales, Alteraciones del entorno. Aplicación de barreras físicas y procedimientos de control frente amenazas físicas al hardware.
- Ciberseguridad en sistemas. Principales amenazas. Herramientas de análisis. Identificación y gestión de vulnerabilidades de software. Identificación y gestión de vulnerabilidades en la web.
- Ciberseguridad en redes. Principales amenazas. Cortafuegos y segmentación. Herramientas de detección y prevención de ataques.
- Actuaciones frente a compromisos de seguridad. Respuesta a incidentes: Plan de respuesta a incidentes y continuidad de negocio (ISO 22301). Análisis forense: La evidencia electrónica (custodia, preservación de pruebas, peritaje y jurisprudencia).
- Gobierno de la seguridad. Sistemas de Gestión de la Seguridad de la Información (ISO/IEC Serie 27000). Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT).
- Auditorías técnicas de seguridad. Auditorías de certificación de SGSI.

# 3. Actividades Formativas

| Actividades formativas |
|---|
| Clases expositivas |
| Sesiones con expertos en el aula |
| Observación y evaluación de recursos didácticos audiovisuales |
| Estudio y seguimiento de material interactivo |
| Clases prácticas: estudio de casos, resolución de problemas, simulación de casos de intervención y/o diseño de proyectos. |
| Clases prácticas: laboratorio informático virtual |
| Prácticas observacionales |
| Actividades de seguimiento de la asignatura |
| Tutorías |
| Lectura, análisis y estudio del manual de la asignatura |
| Lectura, análisis y estudio de material complementario |
| Desarrollo de actividades del portafolio |
| Trabajo cooperativo |
| Prueba objetiva final |

# 4. Metodologías Docentes

| Metodologías docentes |
|---|
| Lección magistral |
| Lección magistral participativa |
| Debate crítico |
| Laboratorio informático virtual |
| Estudio de casos |
| Resolución de problemas |
| Diseño de proyectos |
| Observación |
| Seguimiento |
| Trabajo cooperativo |
| Exposición de trabajos |
| Monitorización de actividades del alumnado |
| Cuaderno reflexivo de la asignatura |