



UNIVERSIDAD  
POLITÉCNICA  
DE MADRID

PROCESO DE  
COORDINACIÓN DE LAS  
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería de  
Sistemas Informáticos

# ANX-PR/CL/001-01

## GUÍA DE APRENDIZAJE

### ASIGNATURA

615000369 - Auditoria Y Control Ti

### PLAN DE ESTUDIOS

61SI - Grado En Sistemas De Informacion

### CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

## Índice

---

### Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	2
4. Competencias y resultados de aprendizaje.....	2
5. Descripción de la asignatura y temario.....	4
6. Cronograma.....	6
7. Actividades y criterios de evaluación.....	8
8. Recursos didácticos.....	10
9. Otra información.....	11

## 1. Datos descriptivos

---

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	615000369 - Auditoria y Control Ti
<b>No de créditos</b>	3 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Cuarto curso
<b>Semestre</b>	Séptimo semestre
<b>Período de impartición</b>	Septiembre-Enero
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	61SI - Grado en Sistemas de Informacion
<b>Centro responsable de la titulación</b>	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
<b>Curso académico</b>	2023-24

## 2. Profesorado

---

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías</b> *
Jesus Sanchez Lopez (Coordinador/a)	1117	jesus.sanchezl@upm.es	Sin horario.

\* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

## 3. Conocimientos previos recomendados

---

### 3.1. Asignaturas previas que se recomienda haber cursado

- Seguridad De La Informacion

### 3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Fundamentos de sistemas de información, sistemas de gestión de seguridad de la información

## 4. Competencias y resultados de aprendizaje

---

### 4.1. Competencias

CC3 - Capacidad para comprender la importancia de la negociación, los hábitos de trabajo efectivos, el liderazgo y las habilidades de comunicación en todos los entornos de desarrollo de software.

CE1 - Capacidad de integrar soluciones de Tecnologías de la Información y las Comunicaciones y procesos empresariales para satisfacer las necesidades de información de las organizaciones, permitiéndoles alcanzar sus objetivos de forma efectiva y eficiente, dándoles así ventajas competitivas.

CE4 - Capacidad para comprender y aplicar los principios y prácticas de las organizaciones, de forma que puedan ejercer como enlace entre las comunidades técnica y de gestión de una organización y participar activamente en la formación de los usuarios.

CE5 - Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.

CE6 - Capacidad para comprender y aplicar los principios y las técnicas de gestión de la calidad y de la innovación tecnológica en las organizaciones.

CT11 - Liderazgo: Cualidades, actitudes, conocimientos y destrezas que posee un individuo, desenvolviéndose de modo que logra inspirar, generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de sinergias, motivaciones y compromisos, y no de manera coercitiva e individualista.

CT7 - Aprendizaje autónomo: El estudiante debe responsabilizarse de su propio aprendizaje, lo que le lleva a utilizar procesos cognitivos de forma estratégica y flexible, en función del objetivo de aprendizaje.

CT8 - Trabajo en equipo: Ser capaz de trabajar como miembro de un equipo interdisciplinar con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

## 4.2. Resultados del aprendizaje

RA296 - Conocer los conceptos básicos de auditoría de los sistemas de información de acuerdo a normas y estándares nacionales e internacionales.

RA297 - Realiza un análisis de riesgos identificando activos, amenazas e impacto según una metodología establecida.

RA140 - Define los conceptos relativos a distintos estándares y marcos de trabajo para la gestión y gobierno de Servicios de TI.

RA137 - Define y distingue las funciones de los distintos roles y competencias en la gestión y gobierno de servicios de TI.

RA141 - Conoce las distintas herramientas que facilitan los procesos estandarizados de gestión y gobierno de servicios de TI en la organización.

RA134 - Conoce y sabe comunicar en qué se basa la cultura de gestión enfocada al cliente en distintas organizaciones.

RA78 - Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales.

RA136 - Conoce y sabe comunicar la necesidad de un buen gobierno y gestión de los servicios de TI.

## 5. Descripción de la asignatura y temario

---

### 5.1. Descripción de la asignatura

El objetivo de esta asignatura es que el alumno sea capaz de analizar el sistema de control interno de una organización, identificar los riesgos asociados a los sistemas y tecnologías de la información y así como de evaluar y auditar el sistema de control con veracidad y concisión.

La información (junto con el sistema de información) es uno de los activos esenciales para las organizaciones. El diseño del SI junto con una gestión y gobierno de las tecnologías de la información es esencial para la supervivencia y posicionamiento de las organizaciones en el mercado. De esta forma, el control sobre las tecnologías de la información y los sistemas que la gestionan se convierte en un objetivo fundamental.

La Auditoría y el Control de las Tecnologías (u Sistemas) de Información se conciben pues como una actividad de alineamiento entre los objetivos y estrategias de la organización y el cumplimiento de normas, políticas y leyes, la protección de los activos de información y el uso eficiente de las tecnologías de la información. Para ello, la asignatura de Auditoría y Control TI pretende capacitar al alumno para implantar, gestionar y auditar el sistema de gestión de la [seguridad de la] información de una organización, tomando como referencia el Esquema Nacional de Seguridad (ENS) y desde una perspectiva de orientación al riesgo. (NOTA: los alumnos ya conocen, por asignaturas previas, otros marcos de seguridad de la información tales como ISO 27001 y RGPD / LOPDyGDD, por lo que no serán objeto de consideración en la asignatura).

Se definirán los distintos tipos de auditoría, la gestión del proceso y del programa de auditoría en una organización. Además de la auditoría basada en cumplimiento, se introducirá la auditoría basada en el riesgo, así como las herramientas y metodologías propias de la actividad de la auditoría. Por último, se introducirá al alumno el perfil profesional del auditor.

## 5.2. Temario de la asignatura

1. La Organización y su Sistema de Información
  - 1.1. La Organización
  - 1.2. El Sistema de Información
  - 1.3. El Departamento de Sistema de Información
  - 1.4. La Unidad de Tecnología (TIC)
  - 1.5. Gestión del Sistema de Información
2. Gestión del riesgo TI
  - 2.1. El método MAGERIT
  - 2.2. Metodolo de Análisis de Riesgos (MAR)
  - 2.3. La herramienta PILAR
3. El Esquema Nacional de Seguridad (ENS)
  - 3.1. Estructura del ENS
  - 3.2. Aplicación del ENS. Medidas de seguridad
  - 3.3. Política de seguridad de la información
  - 3.4. Responsabilidades y funciones
  - 3.5. Control y Auditoría del ENS
4. Auditoría TI
  - 4.1. Proceso de auditoría
  - 4.2. Métodos, pruebas y herramientas en Auditoría
  - 4.3. Perfil profesional del auditor
5. Otros marcos
  - 5.1. ISACA: CISA y CISM
  - 5.2. COBIT e ITIL
  - 5.3. Continuidad de negocio
  - 5.4. Otros

## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	<b>Presentación Introducción a la asignatura</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	<b>Tema 1. La Organización y su Sistema de Información..</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
3		<b>Tema 1. La Organización y su Sistema de Información. Realización de actividades prácticas</b> Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas		
4				<b>Tema 1. La Organización y su Sistema de Información. Presentación de trabajos</b> PG: Técnica del tipo Presentación en Grupo Evaluación continua Presencial Duración: 02:00
5	<b>Tema 2. Gestión del riesgo TI</b> Duración: 01:20 LM: Actividad del tipo Lección Magistral			<b>Tema 1. Cuestionario. El contexto organizativo</b> ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:40
6	<b>Tema 2. Gestión del riesgo TI</b> Duración: 01:00 LM: Actividad del tipo Lección Magistral	<b>Tema 2 Gestión del riesgo TI. Descarga, utilización y uso del programa PILAR.</b> Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		
7				<b>Tema 2. Gestión del riesgo TI. Ejercicio práctico. Gestión de riesgos.</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua Presencial Duración: 02:00
8	<b>Tema 3. El Esquema Nacional de Seguridad (ENS)</b> Duración: 01:20 LM: Actividad del tipo Lección Magistral			<b>Tema 2. Cuestionario. Gestión del riesgo TI</b> ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:40



9				<b>Ejercicio práctico ENS</b> TI: Técnica del tipo Trabajo Individual Evaluación continua Presencial Duración: 02:00
10	<b>Tema 3. Esquema Nacional de Seguridad</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
11	<b>Tema 4. Auditoría TI</b> Duración: 01:20 LM: Actividad del tipo Lección Magistral			<b>Tema 3. Cuestionario. El Esquema Nacional de Seguridad</b> ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:40
12		<b>Tema 4. Auditoría TI</b> Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas		
13				<b>Tema 4. Auditoría TI. Exposición de resultados, entrevistas y auditoría de cierre</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua Presencial Duración: 02:00
14	<b>Tema 5. Otros marcos</b> Duración: 00:20 LM: Actividad del tipo Lección Magistral	<b>Tema 5. Otros marcos. Preparación de trabajos</b> Duración: 01:00 AC: Actividad del tipo Acciones Cooperativas		<b>Tema 4. Cuestionario. Auditoría TI</b> ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:40
15				<b>Tema 5. Otros marcos. Exposición de resultados</b> PG: Técnica del tipo Presentación en Grupo Evaluación continua Presencial Duración: 02:00
16				
17				<b>Ejercicio escrito</b> EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:00  <b>Entrega de actividades</b> TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Presencial Duración: 00:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

## 7. Actividades y criterios de evaluación

### 7.1. Actividades de evaluación de la asignatura

#### 7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Tema 1. La Organización y su Sistema de Información. Presentación de trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	10%	4 / 10	CE1 CE4 CE6 CT7 CT8 CT11 CC3
5	Tema 1. Cuestionario. El contexto organizativo	ET: Técnica del tipo Prueba Telemática	Presencial	00:40	7.5%	4 / 10	CE4 CE6 CT7
7	Tema 2. Gestión del riesgo TI. Ejercicio práctico. Gestión de riesgos.	TG: Técnica del tipo Trabajo en Grupo	Presencial	02:00	20%	4 / 10	CE1 CE5
8	Tema 2. Cuestionario. Gestión del riesgo TI	ET: Técnica del tipo Prueba Telemática	Presencial	00:40	7.5%	4 / 10	CE4 CE6 CT7
9	Ejercicio práctico ENS	TI: Técnica del tipo Trabajo Individual	Presencial	02:00	20%	4 / 10	CE4 CE6 CT7
11	Tema 3. Cuestionario. El Esquema Nacional de Seguridad	ET: Técnica del tipo Prueba Telemática	Presencial	00:40	7.5%	4 / 10	CE4 CE6 CT7
13	Tema 4. Auditoría TI. Exposición de resultados, entrevistas y auditoría de cierre	TG: Técnica del tipo Trabajo en Grupo	Presencial	02:00	10%	4 / 10	CE1 CE6 CT8 CT11 CC3
14	Tema 4. Cuestionario. Auditoría TI	ET: Técnica del tipo Prueba Telemática	Presencial	00:40	7.5%	4 / 10	CE4 CE6 CT7

15	Tema 5. Otros marcos. Exposición de resultados	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	10%	4 / 10	CE1 CE4 CE6 CT7 CT8 CT11
----	---------------------------------------------------	-----------------------------------------------------	------------	-------	-----	--------	-----------------------------------------

### 7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Ejercicio escrito	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE1 CE4 CE5 CE6 CT7
17	Entrega de actividades	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	0%	5 / 10	CE1 CE4 CE5 CE6 CT7

### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Ejercicio escrito	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE1 CE4 CE5 CE6 CT7
Entrega de actividades	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	0%	5 / 10	CE1 CE4 CE5 CE6 CT7

## 7.2. Criterios de evaluación

La evaluación de la asignatura se basa en un mecanismo progresivo. El alumno deberá superar todas y cada una de las actividades y obtener una calificación igual o superior a 5.0 puntos mediante la aplicación de los factores de ponderación indicados en el apartado anterior. En caso de no haber superado alguna/s de ellas, el alumno dispondrá de la posibilidad de volver a realizarla/s y entregarla/s con anterioridad a la fecha oficial de la convocatoria ordinaria del examen.

Para la convocatoria extraordinaria, será condición indispensable para poder presentarse al examen entregar, y superar, TODAS las actividades previstas en el cronograma. Dichas actividades serán calificadas como APTO / NO APTO, permitiendo si APTO presentarse al examen.

## 8. Recursos didácticos

### 8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Aula-laboratorio	Equipamiento	Aula de la ETSISI con al menos un PC por alumno para que puedan realizar las prácticas y cañón de video para poder guiar dicha realización
Materiales de la asignatura	Recursos web	Material de elaboración propia así como recursos didácticos de la plataforma de teleformación on-line ( <a href="https://moodle.upm.es/titulaciones/oficiales">https://moodle.upm.es/titulaciones/oficiales</a> ).
MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.- Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8	Bibliografía	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información utilizada en las AAPP de España.

Materiales de consulta y referencias complementarias	Bibliografía	Real Decreto 311/2022 Guías CCN STIC de la serie 800
Programa PILAR	Otros	Herramienta software de soporte a la metodología MAGERIT

## 9. Otra información

---

### 9.1. Otra información sobre la asignatura

Se utilizará la plataforma Moodle de la UPM (<https://moodle.upm.es/titulaciones/oficiales/>) tanto para el alojamiento de contenidos como para la gestión de actividades (incluida evaluación) y comunicación interpersonal. Adicionalmente, y en caso de que las circunstancias lo requieran, se utilizará la herramienta de videoconferencia Zoom (integrada en Moodle) para apoyo complementario.