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

2021/22 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615000369 - Auditoria y Control Ti
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Cuarto curso
Semestre	Séptimo semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	61SI - Grado en Sistemas de Informacion
Centro responsable de la titulación	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Curso académico	2021-22

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Carolina Gallardo Perez (Coordinador/a)	1210	carolina.gallardop@upm.es	Sin horario.
Jesus Sanchez Lopez	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

RA297 - Realiza un análisis de riegos 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.

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

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) se está convirtiendo en 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 se concibe 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 organizacion, tomando como referencia los marcos ISO 27001 y Esquema Nacional de Seguridad (ENS) desde una perspectiva de orientación al riesgo.

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. La familia ISO27k
    3.1. SGSI. ISO27001 & 27002
    3.2. SGSI. Medición y Certificación
4. Esquema Nacional de Seguridad (ENS)
    4.1. Estructura del ENS
    4.2. Medidas de seguridad
    4.3. Política de seguridad de la información
    4.4. Responsabilidades y funciones
    4.5. Control y Auditoría del ENS
5. Auditoría TI
    5.1. Proceso de auditoría
    5.2. Métodos, pruebas y herramientas en Auditoría
    5.3. Perfil profesional del auditor

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Presentación Introducción a la asignatura** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	**Tema 1. La Organización y su Sistema de Información..** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Caracterización de una organización** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 02:00 **Cuestionario. El contexto organizativo** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00
3	**Tema 2. Gestión del riesgo TI** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Informe de estado de riesgo.** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 03:00
4		**Tema 2 Gestión del riesgo TI. Descarga, utilización y uso del programa PILAR.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
5		**Tema 2. Gestión del riesgo TI. Ejercicio práctico. Gestión de riesgos.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Cuestionario. Gestión del riesgo TI** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00
6	**Tema 3. Familia ISO2700** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Elaboración de SoA y Análisis de GAP** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 03:00
7	**Tema 3. La familia ISO27k** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
8		**Tema 3. Actividad práctica transversal. Alcance y elaboración de la SoA.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Definición de una política de seguridad.** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 04:00 **Cuestionario. La familia ISO 27k** ET: Técnica del tipo Prueba Telemática

				Evaluación continua No presencial Duración: 01:00
9	**Tema 4. Esquema Nacional de Seguridad** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
10	**Tema 4. Esquema Nacional de Seguridad** Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas			**Ejercicio práctico ENS** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 04:00
11		**Tema 4. Esquema Nacional de Seguridad** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Cuestionario. El Esquema Nacional de Seguridad** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00
12	**Tema 4. Auditoría TI** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Informe de auditoría** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 03:00
13	**Tema 4. Auditoría TI** Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas			
14	**Tema 4. Auditoría TI** Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas			
15		**Tema 4. Auditoría TI. Exposición de resultados, entrevistas y auditoría de cierre.** Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas		**Cuestionario. Auditoría TI** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00
16				
17				**Examen de teoría** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00 **Examen de teoría** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:00 **Entrega de actividades prácticas** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final No 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.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
2	Actividad práctica transversal. Caracterización de una organización	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	2%	0 / 10	CE4 CT8
2	Cuestionario. El contexto organizativo	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	2%	0 / 10	CE4
3	Actividad práctica transversal. Informe de estado de riesgo.	TG: Técnica del tipo Trabajo en Grupo	No Presencial	03:00	8%	0 / 10	CE5 CT8 CE1
5	Cuestionario. Gestión del riesgo TI	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	2%	0 / 10	CE5 CT7
6	Actividad práctica transversal. Elaboración de SoA y Análisis de GAP	TG: Técnica del tipo Trabajo en Grupo	No Presencial	03:00	6%	0 / 10	CE6 CE4 CT8
8	Definición de una política de seguridad.	TI: Técnica del tipo Trabajo Individual	No Presencial	04:00	10%	3 / 10	CE6 CT7
8	Cuestionario. La familia ISO 27k	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	2%	0 / 10	CT7 CE6 CE4
10	Ejercicio práctico ENS	TI: Técnica del tipo Trabajo Individual	No Presencial	04:00	10%	3 / 10	CE6 CE4 CT7

11	Cuestionario. El Esquema Nacional de Seguridad	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	2%	0 / 10	CE6 CE4 CT7
12	Actividad práctica transversal. Informe de auditoría	TG: Técnica del tipo Trabajo en Grupo	No Presencial	03:00	14%	0 / 10	CT11 CE6 CT8 CE1 CC3
15	Cuestionario. Auditoría TI	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	2%	0 / 10	CE4 CT7 CE6
17	Examen de teoría	EX: Técnica del tipo Examen Escrito	Presencial	02:00	40%	3 / 10	CE6 CE4 CE5 CT7 CE1

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen de teoría	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE4 CE5 CT7 CE1 CE6
17	Entrega de actividades prácticas	EX: Técnica del tipo Examen Escrito	No Presencial	00:00	0%	5 / 10	CT11 CE6 CE4 CE5 CT7 CE1

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen teoría	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE6 CE4 CE5 CT7 CE1

7.2. Criterios de evaluación

Para superar la asignatura mediante el itinerario de evaluación continua, el alumno deberá obtener una calificación igual o superior al 50% en el conjunto de las actividades y en las condiciones indicadas en el apartado anterior. El conjunto de actividades evaluables y sus pesos en el cálculo de la nota final queda así:

TEORÍA [50%]:

- Cuestionarios (5 cuestionarios: 1 por cada tema): 10%
- Examen final: 40%

PRÁCTICA [50%]:

- Actividad práctica transversal [30%]. Dividida en 4 entregas más una prueba oral, modalidad de **trabajo en grupo**.
- Definición de una política de seguridad [10%]. Modalidad de **trabajo individual.**
- Ejercicio ENS [10%]. **Modalidad de trabajo individual.**

NOTAS MÍNIMAS Y REQUISITOS PARA LA EVALUACIÓN

Se establecen las siguiente notas de corte y requisitos:

- Actividades prácticas:

- Definición de una política de seguridad: **3.0 puntos**

- Ejercicio ENS: **3.0 puntos**

- Examen final: **3.0 puntos**.

EVALUACIONES MEDIANTE SOLO PRUEBA FINAL Y CONVOCATORIA EXTRAORDINARIA.

- En el caso de optar por el itinerario de **solo prueba final**, será condición indispensable para poder presentarse al examen entregar TODAS las prácticas previstas en el cronograma. Dichas prácticas serán

calificadas como APTO/NO APTO, permitiendo (si APTO) presentarse al examen.

- El plazo máximo para solicitar evaluación mediante solo prueba final es el **26 de octubre de 2021**.
- **EVALUACIÓN CONVOCATORIA EXTRAORDINARIA**: La evaluación en convocatoria extraordinaria será igual que la EVALUACIÓN mediante SOLO PRUEBA FINAL

RESULTADOS DE APRENDIZAJE

Actividad práctica transversal	RA137 - Define y distingue las funciones de los distintos roles y competencias en la gestión y gobierno de servicios de TI. RA140 - Define los conceptos relativos a distintos estándares y marcos de trabajo para 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. RA296 - Conocer los conceptos básicos de auditoría de los sistemas de información de acuerdo con normas y estándares nacionales e internacionales. RA297 - Realiza un análisis de riesgos identificando activos, amenazas e impacto según una metodología establecida.
Ejercicio ENS	RA141 - Conoce las distintas herramientas que facilitan los procesos estandarizados de gestión y gobierno de servicios de TI en la organización. RA78 - Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo con estándares y normas internacionales.
Definición de política de seguridad	RA78 - Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo con estándares y

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

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
R. Pompon (2016) IT Security Risk Control Management: An Audit Preparation. Apress. ISBN-13: 978-1-4842-2139-6	Bibliografía	Orientado al diseño de un programa de seguridad de la información, desde su concepción hasta la fase de auditoría, integra la visión tecnológica con la organizativa, estratégica y gestión.
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.
M. Piattini y E. del Peso, Emilio. 2000. Auditoría Informática: Un enfoque práctico. 2ª Edición. Madrid: Ra-ma.	Bibliografía	
S. Senft y F. Gallegos. 2009. Information Technology Control and Audit. 3rd Edition. Boston (MA): Auerbach.	Bibliografía	

Materiales de la asignatura	Recursos web	Material de elaboración propia así como recursos didácticos de la plataforma de teleformación on-line (https://moodle.upm.es/titulaciones/oficiales).
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

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.