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

2019/20 - 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....9
8. Recursos didácticos....12

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	2019-20

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Carolina Gallardo Perez	1210	carolina.gallardop@upm.es	Sin horario.
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

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.

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

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

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 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 gestionar y auditar el sistema de control interno TI con conocimientos sobre análisis y gestión de riesgos, sistemas de gestión de la seguridad de la información y de continuidad de negocio.

La asignatura se estructura en los siguientes temas:

1. **Control TI**. En este bloque, se abordarán los distintos marcos de referencia, buenas prácticas, herramientas y modelos de evaluación para el control de las tecnologías y sistemas de la información.
2. **Gestión (análisis y tratamiento) de riesgos TI**. Se abordará el proceso completo de la gestión de riesgos asociados al uso TI. Asimismo, se introducirá el concepto de proceso de continuidad de negocio y su relación con la gestión de riesgos.
3. **Auditoría**. 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. Controles esenciales de TI
    1.1. El contexto organizativo
    1.2. Marcos de referencia: familia 27000
    1.3. Marcos de referencia: Esquema nacional de seguridad
    1.4. Otros marcos
2. Gestión del riesgo TI
    2.1. Concepto, definiciones y metodologías de GR
    2.2. Metodología Magerit
    2.3. Herramientas de ayuda a la toma de decisiones
3. Continuidad de negocio
    3.1. Concepto y estándares
    3.2. Gestión de incidentes
    3.3. Continuidad y recuperación frente a desastres
4. Auditoría TI
    4.1. Áreas de actuación de la auditoría TI
    4.2. Proceso de auditoría
    4.3. Metodología y herramientas
    4.4. La profesión del auditor

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**Presentación Introducción a la asignatura** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	**Tema 1. Controles esenciales de TI. El contexto organizativo** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Cuestionario. El contexto organizativo** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00 **Actividad práctica transversal. Caracterización de una organización** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 04:00
3	**Tema 1. Controles esenciales de TI. Marcos de referencia: la familia ISO 27k** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Cuestionario. La familia ISO 27k** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00
4	**Tema 1. Controles esenciales de TI. Marcos de referencia: la familia ISO 27k** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Elaboración de SoA y Análisis de GAP** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 04:00
5	**Tema 1. Controles esenciales de TI. Marcos de referencia: el Esquema Nacional de Seguridad y otros marcos.** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Cuestionario. El Esquema Nacional de Seguridad** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00
6	**Tema 1. Controles esenciales de TI. Marcos de referencia: el Esquema Nacional de Seguridad y otros marcos.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			**Actividad práctica transversal. Aplicabilidad de medidas de seguridad (ENS)** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 04:00 **Ejercicio práctico ENS** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 05:00
7	**Tema 2. Gestión del riesgo TI** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Cuestionario. Gestión del riesgo TI** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00

8	**Tema 2. Gestión del riesgo TI** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			**Ejercicio práctico Gestión de Riesgos** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final Duración: 05:00 **Actividad práctica transversal. Gestión de riesgos** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 04:00
9			**Informe de estado de riesgo.** Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas	**Informe de estado de riesgo** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 00:00
10	**Tema 3. Continuidad de negocio** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Cuestionario. Continuidad de negocio** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00
11	**Tema 3. Continuidad de negocio** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Continuidad de negocio** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 04:00
12	**Tema 4. Auditoría TI** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Cuestionario. Auditoría TI** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00
13	**Tema 4. Auditoría TI** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
14	**Tema 4. Auditoría TI** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividad práctica transversal. Auditoría fase I y plan de auditoría** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 08:00
15				**Exposición de resultados, entrevistas y auditoría de cierre.** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 02:00
16				**Examen final teoría** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:00 **Examen teoría** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

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.

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	Cuestionario. El contexto organizativo	ET: Técnica del tipo Prueba Telemática	No Presencial	02:00	1%	0 / 10	CE6 CE4 CC3 CE1
2	Actividad práctica transversal. Caracterización de una organización	TG: Técnica del tipo Trabajo en Grupo	No Presencial	04:00	2%	0 / 10	CT11 CE6 CE4 CT7 CT8 CE1
3	Cuestionario. La familia ISO 27k	ET: Técnica del tipo Prueba Telemática	No Presencial	02:00	2%	0 / 10	CE6 CE4 CE1
4	Actividad práctica transversal. Elaboración de SoA y Análisis de GAP	PG: Técnica del tipo Presentación en Grupo	No Presencial	04:00	2%	0 / 10	CT11 CE6 CE4 CT7 CT8
5	Cuestionario. El Esquema Nacional de Seguridad	ET: Técnica del tipo Prueba Telemática	No Presencial	02:00	1.5%	0 / 10	CE5 CE4
6	Actividad práctica transversal. Aplicabilidad de medidas de seguridad (ENS)	TG: Técnica del tipo Trabajo en Grupo	No Presencial	04:00	2%	0 / 10	CT11 CE4 CE5 CT7 CT8
6	Ejercicio práctico ENS	ET: Técnica del tipo Prueba Telemática	No Presencial	05:00	10%	3 / 10	CE6 CE4 CT7
7	Cuestionario. Gestión del riesgo TI	ET: Técnica del tipo Prueba Telemática	No Presencial	02:00	2%	0 / 10	

8	Ejercicio práctico Gestión de Riesgos	TI: Técnica del tipo Trabajo Individual	No Presencial	05:00	10%	3 / 10	CE5 CT7
8	Actividad práctica transversal. Gestión de riesgos	TG: Técnica del tipo Trabajo en Grupo	No Presencial	04:00	2%	0 / 10	CC3 CE4 CE5 CT7 CT8
9	Informe de estado de riesgo	PG: Técnica del tipo Presentación en Grupo	Presencial	00:00	5%	0 / 10	CE5 CT8 CT11 CE4
10	Cuestionario. Continuidad de negocio	ET: Técnica del tipo Prueba Telemática	No Presencial	02:00	1.5%	0 / 10	
11	Actividad práctica transversal. Continuidad de negocio	TG: Técnica del tipo Trabajo en Grupo	No Presencial	04:00	2%	0 / 10	CT11 CE4 CC3 CT7 CT8
12	Cuestionario. Auditoría TI	ET: Técnica del tipo Prueba Telemática	No Presencial	02:00	2%	0 / 10	
14	Actividad práctica transversal. Auditoría fase I y plan de auditoría	TG: Técnica del tipo Trabajo en Grupo	No Presencial	08:00	10%	0 / 10	
15	Exposición de resultados, entrevistas y auditoría de cierre.	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	5%	0 / 10	CE6 CE4 CC3 CT7 CT8 CE1 CT11
16	Examen final teoría	EX: Técnica del tipo Examen Escrito	Presencial	01:00	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

6	Ejercicio práctico ENS	ET: Técnica del tipo Prueba Telemática	No Presencial	05:00	10%	3 / 10	CE6 CE4 CT7
8	Ejercicio práctico Gestión de Riesgos	TI: Técnica del tipo Trabajo Individual	No Presencial	05:00	10%	3 / 10	CE5 CT7
16	Examen teoría	EX: Técnica del tipo Examen Escrito	Presencial	02:00	80%	4 / 10	CE6 CE4 CE5 CC3 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	70%	4 / 10	CE6 CE4 CE5 CC3 CT7 CE1
Trabajo práctico integrador	PI: Técnica del tipo Presentación Individual	Presencial	02:00	30%	4 / 10	CT11 CT8

7.2. Criterios de evaluación

Para superar la asignatura el alumno deberá obtener una calificación igual o superior a 5.0 puntos por la realización de las diferentes actividades de evaluación y en las condiciones indicadas en el apartado anterior.

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