



POLITÉCNICA

CAMPUS
DE EXCELENCIA
INTERNACIONAL

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingenieros de
Telecomunicacion

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93000824 - Ciberseguridad y privacidad: gestión y operación

PLAN DE ESTUDIOS

09AQ - Master Universitario En Ingenieria De Telecomunicacion

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo 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.....	3
6. Cronograma.....	5
7. Actividades y criterios de evaluación.....	7
8. Recursos didácticos.....	9

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93000824 - Ciberseguridad y privacidad: gestión y operación
No de créditos	6 ECTS
Carácter	Optativa
Curso	Segundo curso
Semestre	Cuarto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AQ - Master universitario en ingeniería de telecomunicación
Centro en el que se imparte	09 - Escuela Técnica Superior de Ingenieros de Telecomunicación
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Irene Cristina Romero Ibañez	B423	irenecristina.romero@upm.es	X - 14:00 - 15:00 Contactar por correo electrónico
Victor Abraham Villagra Gonzalez (Coordinador/a)	B-217	victor.villagra@upm.es	X - 14:00 - 15:00

Jose Antonio Mañas Argemi	B-202	joseantonio.manas@upm.es	X - 12:00 - 13:00
Jose Maria Del Alamo Ramiro	C-218	jm.delalamo@upm.es	X - 11:00 - 13:00

* 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

El plan de estudios Master Universitario en Ingeniería de Telecomunicación no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Servicios de Seguridad en Redes, Servicios y Sistemas de Telecomunicación
- Tecnologías de Ciberseguridad

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE6 - Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.

CE7 - Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

4.2. Resultados del aprendizaje

RA205 - Conocer y Diseñar un Centro de Gestión de Ciberincidentes

RA202 - Conocer y comprender los riesgos derivados del procesamiento incorrecto de datos personales

RA200 - Diseñar y desarrollar políticas de seguridad

RA201 - Conocer y aplicar las principales técnicas de ingeniería de privacidad de la información

RA18 - El alumno conoce las arquitecturas correspondientes a los paradigmas de afianzamiento de la seguridad en las redes, aplicaciones y contenidos.

RA199 - Conocer los modelos y estándares de gestión de la seguridad de la información

RA203 - Conocer y comprender la legislación y normativa de aplicación para protección de datos de carácter personal

RA204 - Conocer, comprender y saber aplicar algunos métodos, técnicas y herramientas para el desarrollo de sistemas respetuosos con la privacidad

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Los objetivos de esta asignatura se articulan en tres grandes temas:

- Organización y Gobierno de la Seguridad en Corporaciones
- Gestión y Operación de la Seguridad en Corporaciones
- Ingeniería de Privacidad.

El primer tema tiene como objetivo que el alumno conozca la problemática asociada a la implantación de una política de seguridad en una organización, siendo capaz de realizar una planificación y diseño de la misma, a nivel de estrategia corporativa, análisis de riesgos, políticas de seguridad, organización de la seguridad, desarrollo de normativa, plan director de la seguridad e implantación en un Sistema de Gestión de la Seguridad de la Información.

El segundo tema trata sobre la problemática de la gestión y monitorización de incidentes de ciberseguridad en una organización, tratando los servicios necesarios a implantar en un Centro de Operaciones de Ciberseguridad

(SOC), y los modelos de gestión existentes para estos centros.

El tercer tema trata sobre la ingeniería de la privacidad, en el que se pretende que el alumno conozca y comprenda los riesgos derivados del procesamiento incorrecto de datos personales, la legislación y normativa de aplicación para protección de datos de carácter personal y sepa aplicar algunos métodos, técnicas y herramientas para el desarrollo de sistemas respetuosos con la privacidad

La asignatura incluirá trabajos personales de los alumnos de casos de estudio de situaciones muy cercanas a casos reales en dichos temas.

5.2. Temario de la asignatura

1. Dirección y Gobierno de la Ciberseguridad
 - 1.1. Diseño de Estrategias Corporativas de Ciberseguridad
 - 1.2. Analisis de Riesgos y Tratamiento de Riesgos.
 - 1.3. Diseño y Desarrollo de Políticas de Ciberseguridad
 - 1.4. Desarrollo Normativo de la Ciberseguridad
 - 1.5. Sistemas de Gestión de la Seguridad de la Información
 - 1.6. Gestión de la Continuidad del Negocio
2. Gestión y Operación de la Ciberseguridad
 - 2.1. Servicios de un Centro de Operación de Ciberseguridad
 - 2.2. Diseño de un Centro de Operación de Ciberseguridad
3. Ingeniería de la Privacidad
 - 3.1. Introduccion a la Privacidad y Conceptos Básicos
 - 3.2. Perspectiva Social e Individual de la Ingeniería de la Privacidad
 - 3.3. Legislación para Protección de Datos Personales
 - 3.4. Evaluación y Gestión de Riesgos: evaluación del impacto para la privacidad
 - 3.5. Técnicas y Herramientas Básicas de Ingeniería de la Priivacidad

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	Introducción a la Asignatura Duración: 01:00 LM: Actividad del tipo Lección Magistral Tema 1: Dirección y Gobierno de la Ciberseguridad Duración: 03:00 LM: Actividad del tipo Lección Magistral			
2	Tema 1: Dirección y Gobierno de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	Tema 1: Dirección y Gobierno de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
4			Conferencia de Experto Profesional Duración: 02:00 LM: Actividad del tipo Lección Magistral Tutorías de Trabajos de Alumnos Duración: 02:00 OT: Otras actividades formativas	
5				Presentación de Trabajos PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 04:00
6	Tema 2: Gestión y Operación de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
7	Tema 2: Gestión y Operación de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
8	Tema 2: Gestión y Operación de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
9			Conferencia de Experto Profesional Duración: 02:00 LM: Actividad del tipo Lección Magistral Tutorías de Trabajos de Alumnos Duración: 02:00 OT: Otras actividades formativas	

10				<p>Presentación de Trabajos PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 04:00</p> <p>Examen Final EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00</p>
11	Tema 3: Ingeniería de la Privacidad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
12	Tema 3: Ingeniería de la Privacidad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
13	Tema 3: Ingeniería de la Privacidad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
14			<p>Conferencia de Experto Profesional Duración: 02:00 LM: Actividad del tipo Lección Magistral</p> <p>Tutorías de Trabajos de Alumnos Duración: 02:00 OT: Otras actividades formativas</p>	
15				<p>Presentación de Trabajos PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 04:00</p> <p>Examen Final EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00</p>
16				
17				<p>Examen Final EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00</p> <p>Presentacion de Trabajos PG: Técnica del tipo Presentación en Grupo Evaluación sólo prueba final Duración: 04:00</p>

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
5	Presentación de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	04:00	33%	4 / 10	CE6 CE7
10	Presentación de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	04:00	13%	4 / 10	CE6 CE7
10	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	20%	4 / 10	CE6 CE7
15	Presentación de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	04:00	14%	4 / 10	CE6 CE7
15	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	20%	4 / 10	CE6 CE7

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	60%	4 / 10	CE6 CE7
17	Presentacion de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	04:00	40%	4 / 10	CE6 CE7

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Final Extraordinario	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE6 CE7

7.2. Criterios de evaluación

Los estudiantes serán evaluados, por defecto, mediante evaluación continua. El estudiante que desee renunciar a la evaluación continua y optar a la evaluación por prueba final (formada por una o más actividades de evaluación global de la asignatura), deberá comunicarlo por escrito formalizado en el registro de la ETSI Telecomunicación y dirigido al Coordinador de la Asignatura antes del final del primer mes desde el comienzo de la asignatura. La presentación de este escrito supondrá la renuncia automática a la evaluación continua.

La evaluación comprobará si los estudiantes han adquirido las competencias de la asignatura. Por tanto, la evaluación mediante prueba final usará los mismos tipos de técnicas evaluativas que se usan en la evaluación continua (EX, ET, TG, etc.), y se realizarán en las fechas y horas de evaluación final aprobadas por la Junta de Escuela para el presente curso y semestre..

CONVOCATORIA ORDINARIA: MODALIDAD EVALUACIÓN CONTINUA

La asignatura se aprobará cuando se obtenga una calificación mayor o igual a 5 puntos sobre un total de 10. La nota final se obtendrá mediante la suma de las calificaciones correspondientes a las diferentes partes de la asignatura, con los siguientes pesos:

- E1: Diseño Organizativo de la Ciberseguridad 33'3 %
- E2: Gestión y Operación de la Ciberseguridad: 33'3 %
- E3: Ingeniería de la Privacidad: 33,3 %

La evaluación de cada parte podrá basarse en la elaboración y presentación de trabajos y/o prácticas de laboratorio y/o exámenes escritos.

Se deberá sacar más de un 4 en cada parte individual y un 5 en total para poder ser evaluado en esta modalidad. En caso contrario, deberá presentarse al examen final. En caso de inasistencia o no entrega de alguno de los componentes de cada actividad, se considerará que el alumno no se ha presentado y no podrá seguir la evaluación continua, debiendo optar por evaluación única

CONVOCATORIA ORDINARIA: EVALUACIÓN MEDIANTE UNA ÚNICA PRUEBA FINAL

El 100% de la calificación de los alumnos que presenten el escrito arriba referido se otorgará en función de una única prueba final en la que presentarán asimismo todas las distintas actividades de evaluación de la asignatura..

CONVOCATORIA EXTRAORDINARIA

La evaluación de la asignatura en su convocatoria extraordinaria se realizará mediante una única prueba final, con independencia de la opción elegida en la convocatoria ordinaria.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Moodle	Recursos web	Servidor Moodle de la Asignatura
Equipamiento	Equipamiento	Aula, Laboratorio, Sala de Trabajo en Grupo
Referencias	Bibliografía	Bibliografía