ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93000902 - Seguridad en redes de telecomunicacion

PLAN DE ESTUDIOS

09AS - Master Universitario en Ingenieria de Redes y Servicios Telematicos

CURSO ACADÉMICO Y SEMESTRE

2017/18 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93000902 - Seguridad en redes de telecomunicacion
No de créditos	4.5 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AS - Master Universitario en Ingenieria de Redes y Servicios Telematicos
Centro en el que se imparte	Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2017-18

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Jose Maria Del Alamo Ramiro	C-218	jm.delalamo@upm.es	X - 11:00 - 13:00
Victor Abraham Villagra Gonzalez (Coordinador/a)	B-217	victor.villagra@upm.es	X - 14:00 - 15:00

Irene Cristina Romero Iba?ez	B-423	irenecristina.romero@upm.es	X - 14:00 - 15:00

* 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 Ingenieria de Redes y Servicios Telematicos 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 que adquiere el estudiante al cursar la asignatura

CEC3 - Capacidad para conocer el estado actual de la tecnología relacionada con la seguridad en redes de telecomunicación, analizando las amenazas a la seguridad de acceso y de la propia red en Internet y en las redes IP.

CG3 - - Capacidad para profundizar en la tendencia a la integración de los sistemas telemáticos, englobando aspectos técnicos, de gestión, sociales, económicos, éticos, etc. y para reflexionar sobre todos los aspectos implicados para formular sus juicios.

4.2. Resultados del aprendizaje al cursar la asignatura

RA3 - Conocer el estado del arte actual en el área de Seguridad en Redes de Telecomunicación, saber identificar áreas con problemas y carencias que potencialmente pueden ser objeto de innovación, realizar estudios críticos de propuestas relacionadas y generar nuevas ideas y propuestas para solventar una determinada carencia o problema

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

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

- Análisis de Riesgos, Gestión y Operación de la Seguridad en Corporaciones
- Ingeniería de Privacidad.

El primer tema trata sobre la problemática asociada a la implantación de una política de seguridad en una organización, siendo capaz de entender el proceso de análisis de riesgos en una organización, para posteriormente ahondar en 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, incluyendo la coordinación con Centros de Respuesta a Incidentes (CERT).

El segundo 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 se articula sobre 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. Analisis de Riesgos de Ciberseguridad

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: Análisis de Riesgos en Ciberseguridad** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	**Tema 1: Análisis de Riesgos en Ciberseguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
3	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
4	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
5	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
6	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
7			**Conferencia de Experto Profesional** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Tutorias de Trabajos de Alumnos** Duración: 02:00 OT: Otras actividades formativas	
8				**Presentación de Trabajos** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 03:00
9	**Tema 3: Ingeniería de la Privacidad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			

10	**Tema 3: Ingeniería de la Privacidad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
11	**Tema 3: Ingeniería de la Privacidad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
12	**Tema 3: Ingeniería de la Privacidad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
13			**Tutorias de Trabajos de Alumnos** Duración: 02:00 OT: Otras actividades formativas **Conferencia de Experto Profesional** Duración: 01:00 LM: Actividad del tipo Lección Magistral	
14				**Presentación de Trabajos** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 03:00
15				**Presentación de Trabajos** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 03:00
16				
17				**Examen Final** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00 **Examen Final** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00 **Presentacion de trabajos del curso** PG: Técnica del tipo Presentación en Grupo Evaluación sólo prueba final Duración: 04:00

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
8	Presentación de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	03:00	50%	4 / 10	CG3 CEC3
14	Presentación de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	03:00	25%	4 / 10	CG3 CEC3
15	Presentación de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	03:00	25%	4 / 10	CG3 CEC3
17	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	%	5 / 10	CG3 CEC3

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%	5 / 10	CG3 CEC3
17	Presentacion de trabajos del curso	PG: Técnica del tipo Presentación en Grupo	Presencial	04:00	40%	5 / 10	CG3 CEC3

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Final Extraordianrio	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CG3 CEC3

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 actividades de evaluación, con los siguientes pesos:

- E2: Elaboración y Presentación de un Proyecto sobre Gestión y Operación de la Ciberseguridad: 50%
- E3: Elaboración y Presentación de un Proyecto sobre ingeniería de la Privacidad: 50%

En todos los casos se evaluará tanto el contenido escrito del trabajo (2/3 de la evaluación) como su presentación (1/3 de la evaluación). Deberá sacar más de un 4 en cada trabajo 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 los trabajos 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