ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

Seguridad, confianza y privacidad en servicios de la sociedad de la informacion

CURSO ACADÉMICO - SEMESTRE

2016-17 - Segundo semestre

Datos Descriptivos

Nombre de la Asignatura	Seguridad, confianza y privacidad en servicios de la sociedad de la informacion
Titulación	09AQ - Master Universitario en Ingenieria de Telecomunicacion
Centro responsable de la titulación	Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Semestre/s de impartición	Cuarto semestre
Módulos	Intensificacion-investigacion en telecomunicacion
Materias	Telematica II
Carácter	Optativa
Código UPM	93000824
Nombre en inglés	Security, trust and privacy in services of information society

Datos Generales

Créditos	6	**Curso**	2
Curso Académico	2016-17	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

El plan de estudios Master Universitario en Ingenieria de Telecomunicacion no tiene definidas asignaturas previas superadas para esta asignatura.

Otros Requisitos

El plan de estudios Master Universitario en Ingenieria de Telecomunicacion no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

El coordinador de la asignatura no ha definido asignaturas previas recomendadas.

Otros Conocimientos Previos Recomendados

Servicios de Seguridad en Redes, Servicios y Sistemas de Telecomunicación

Tecnologías de Ciberseguridad

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.

Resultados de Aprendizaje

RA200 - Diseñar y desarrollar políticas de seguridad

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

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

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 caracter personal

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

RA205 - Conocer y Diseñar un Centro de Gestión de Ciberincidentes

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Villagra Gonzalez, Victor Abraham **(Coordinador/a)**	B-217	victor.villagra@upm.es	X - 14:00 - 15:00
Mañas Argemi, Jose Antonio	C-219	joseantonio.manas@upm.es	X - 12:00 - 13:00
Alamo Ramiro, Jose Maria Del	B-204.1	jm.delalamo@upm.es	X - 11:00 - 13:00

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

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 riegos, 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, incluyendo la coordinación con Centros de Respuesta a Incidentes (CERT).

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 se articula sobre trabajos personales de los alumnos de casos de estudio de situaciones muy cercanas a casos reales en dichos temas.

Temario

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

Cronograma

Horas totales: 60 horas

Horas presenciales: 60 horas (38.5%)

Peso total de actividades de evaluación continua: 100%

Peso total de actividades de evaluación sólo prueba final: 100%

Semana	Actividad Prensencial en Aula	Actividad Prensencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 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			
Semana 2	**Tema 1: Dirección y Gobierno de la Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 3	**Tema 1: Dirección y Gobierno de la Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 4			**Conferencia de Experto Profesional** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tutorias de Trabajos de Alumnos** Duración: 02:00 OT: Otras actividades formativas	
Semana 5				**Presentación de Trabajos** Duración: 04:00 PG: Técnica del tipo Presentación en Grupo Evaluación continua Actividad presencial
Semana 6	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 7	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 8	**Tema 2: Gestión y Operación de la Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			

Semana 9			**Conferencia de Experto Profesional** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tutorias de Trabajos de Alumnos** Duración: 02:00 OT: Otras actividades formativas	
Semana 10				**Presentación de Trabajos** Duración: 04:00 PG: Técnica del tipo Presentación en Grupo Evaluación continua Actividad presencial
Semana 11	**Tema 3: Ingeniería de la Privacidad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 12	**Tema 3: Ingeniería de la Privacidad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 13	**Tema 3: Ingeniería de la Privacidad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 14			**Conferencia de Experto Profesional** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tutorias de Trabajos de Alumnos** Duración: 02:00 OT: Otras actividades formativas	
Semana 15				**Presentación de Trabajos** Duración: 04:00 PG: Técnica del tipo Presentación en Grupo Evaluación continua Actividad presencial
Semana 16				
Semana 17				**Examen Final** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad presencial

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
5	Presentación de Trabajos	04:00	Evaluación continua	PG: Técnica del tipo Presentación en Grupo	Sí	33%	4 / 10	CE6, CE7
10	Presentación de Trabajos	04:00	Evaluación continua	PG: Técnica del tipo Presentación en Grupo	Sí	33%	4 / 10	CE6, CE7
15	Presentación de Trabajos	04:00	Evaluación continua	PG: Técnica del tipo Presentación en Grupo	Sí	34%	4 / 10	CE6, CE7
17	Examen Final	02:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%	5 / 10	CE6, CE7

Criterios de Evaluación

Los alumnos que deseen ser evaluados en convocatoria ordinaria mediante una única prueba final deben expresarlo mediante escrito formalizado en el registro de la ETSI Telecomunicación y dirigido al Director del Departamento no más tarde del 30 de Marzo. La presentación de este escrito supondrá la renuncia automática a la evaluación continua.

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:

- E1: Elaboración y Presentación de un Proyecto sobre Diseño Organizativo de la Ciberseguridad: 33'3 %
- E2: Elaboración y Presentación de un Proyecto sobre Gestión y Operación de la Ciberseguridad: 33'3 %
- E3: Elaboración y Presentación de un Proyecto sobre ingeniería de la Privacidad: 33,3 %

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.

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.

Recursos Didácticos

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