Datos Descriptivos

ASIGNATURA:	Desarrollo de Software de Seguridad en Red
MATERIA:	Sistemas y Servicios Distribuidos
CRÉDITOS EUROPEOS:	4,5
CARÁCTER:	Optativa
TITULACIÓN:	Master Ingeniero en Informática
CURSO/SEMESTRE	Primero
ESPECIALIDAD:	

CURSO ACADÉMICO			
PERIODO IMPARTICION	**Septiembre- Enero**	**Febrero - Junio**	
	x		
IDIOMA IMPARTICIÓN	**Sólo castellano**	**Sólo inglés**	**Ambos**
	X		

DEPARTAMENTO:	LENGUAJES Y SISTEMAS INFORMATICOS E INGENIERÍA DEL SOFWARE

PROFESORADO		
NOMBRE Y APELLIDO (C = Coordinador)	**DESPACHO**	**Correo electrónico**
LUIS MENGUAL GALÁN (C)	4303	lmengual@fi.upm.es

CONOCIMIENTOS PREVIOS REQUERIDOS PARA PODER SEGUIR CON NORMALIDAD LA ASIGNATURA	
ASIGNATURAS SUPERADAS	
OTROS RESULTADOS DE APRENDIZAJE NECESARIOS	

Objetivos de Aprendizaje

COMPETENCIAS Y NIVEL ASIGNADAS A LA ASIGNATURA		
Código	**COMPETENCIA**	**NIVEL**
CG10	Conocimiento y comprensión de la informática necesaria para la creación de modelos de información, y de los sistemas y procesos complejos	C, P
CG5	Aplicación de los métodos de resolución de problemas más recientes o innovadores y que puedan implicar el uso de otras disciplinas	A
CG3	Especificación y realización de tareas informáticas complejas, poco definidas o no familiares	A
CE7	Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.	A
CE4	Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos	A
CE1	Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.	A

Nivel de competencia: conocimiento(C), comprensión (P), aplicación(A) y análisis y síntesis(S),

Código	RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA
RA1	Ser capaz de identificar los servicios de seguridad en el diseño de aplicaciones en Red.
RA2	Ser capaz de crear la infraestructura de seguridad necesaria en servicios y aplicaciones.
RA3	Diseñar e implementar Aplicaciones Distribuidas con Mecanismos de Seguridad

Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS (TEMARIO)		
TEMA	**APARTADO**	**Indicadores Relacionados**
Tema 1: Arquitecturas de Seguridad	Servicios de Seguridad en Red. ISO 7498-2	T1
	Mecanismos, Funciones y Protocolos de seguridad	T2
Tema 2: Modelos de Seguridad en Red	Nivel de Sockets Seguro (SSL, Secure Socket Layer)	T2
	Modelo de Kerberos	T2
	Aplicaciones Seguras: Comercio electrónico seguro, Sistemas de Firma Biométrica, correo electrónico seguro s/mime	T2
Tema 3: Desarrollo de aplicaciones con servicios de seguridad	Plataformas, herramientas y librerías de desarrollo de aplicaciones: OpenSSL, Keytool, JCE (Java Cryptography Extension), JSSE (Java Secure Sockets Extension	T3
	Gestión de Certificados y almacenes de seguridad	T3
	Desarrollo de Código seguro	T4
	Código Manejo certificados	T5
	Protocolos de seguridad	T6
	Conexiones SSL (autenticación de cliente, certificados autofirmados/ firmados por una CA, configuración parámetros del protocolo)	T7
	Aplicaciones de Firma/verificación electrónica. Integración sistemas biométricos	T8
	Aplicaciones de comercio electrónico Acceso seguro a Bases de Dato	T9
	Acceso confidencial y autenticado a BD	T10

BREVE DESCRIPCIÓN DE LAS MODALIDADES ORGANIZATIVAS UTILIZADAS Y METODOS DE ENSEÑANZA EMPLEADOS	
CLASES DE TEORIA	Todo tema tendrá un parte de clases teóricas
CLASES PROBLEMAS	
PRACTICAS	Habrá prácticas semanales de desarrollo de código fuente y creación de infraestructura de seguridad
TRABAJOS AUTONOMOS	
TRABAJOS EN GRUPO	
TUTORÍAS	Todas las semanas los alumnos tendrán posibilidad de 4 horas de tutoría con el profesor que les esté impartiendo las clases teóricas

RECURSOS DIDÁCTICOS	
BIBLIOGRAFÍA	Java Network Programming, 4º Edition. E. Rusty Harol, 0`really. 2013. http://www.it-ebooks.info/book/3137/
	Cryptography and Network Security Principles and Practice Fifth Edition. W. Stallings 2011, Pearson Education, Inc., publishing as Prentice Hall http://faculty.mu.edu.sa/public/uploads/1360993259.0858Cryptography%20and%20Network%20Security%20Principles%20and%20Practice,%205th%20Edition.pdf
	Network Security with OpenSSL. J. Viega, M. Messier, P. Chandra. 0`really 2002 http://it-ebooks.info/book/263/
RECURSOS WEB	
EQUIPAMIENTO	

Cronograma de trabajo de la asignatura

Semana	Actividades Aula	Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades Evaluación
1, 2 (16h)	Servicios, Mecanismos y Funciones de seguridad		Estudio y ejercicios		
3, 4 (16h)	Modelos de seguridad en Red		Estudio y ejercicios		
5, 6 (16h)	Plataformas y herramientas de Seguridad (OpenSSL, Keytool)	Gestión de Almacenes y Certificados	Estudio y ejercicios		
7, 8 (16h)	Diseño de código seguro	Código Manejo certificados	Estudio y ejercicios		
9, 10 (16h)	Diseño de código seguro	Desarrollo de Aplicaciones Cliente/Servidor SSL	Estudio y ejercicios		
11, 12 (16h)t	Diseño de código seguro	Desarrollo de Aplicaciones Firma electrónica	Estudio y ejercicios		
13, 14 (16h)	Diseño de código seguro	Desarrollo de Aplicaciones Comercio electrónico	Estudio y ejercicios		
15 (9,5h)	Diseño de código seguro	Desarrollo de Aplicaciones con acceso confidencial y autenticado a una BD	Estudio y ejercicios		

Sistema de evaluación de la asignatura

EVALUACION		
Ref	**INDICADOR DE LOGRO**	**Relacionado con RA:**
T1	Conoce las amenazas que puede sufrir la información que se distribuye en una red telemática	RA1
T2	Es capaz de analizar los servicios de seguridad disponibles así como los mecanismos asociados	RA1
T3	Es capaz de construir certificador y almacenes de seguridad	RA2
T4	Es capaz de diseñar aplicaciones que requieran servicios de seguridad	RA2
T5	Es capaz de Implementar código fuente para el manejo de certificados digitales	RA3
T6	Es capaz de Implementar protocolos de seguridad	RA3
T7	Es capaz de Implementar aplicaciones cliente-servidor SSL	RA3
T8	Es capaz de Implementar aplicaciones de firma electrónica	RA3
T9	Es capaz de Implementar aplicaciones de comercio electrónico seguro	RA3
T10	Es capaz de Implementar aplicaciones con un Acceso confidencial y autenticado a una Base de Datos	RA3

La tabla anterior puede ser sustituida por la tabla de rúbricas.

EVALUACION SUMATIVA			
BREVE DESCRIPCION DE LAS ACTIVIDADES EVALUABLES	**MOMENTO**	**LUGAR**	**PESO EN LA CALIFICACIÓN**
Practicas de Infraestructura Seguridad	3-6 semana	Laboratorio	20%
Practicas Aplicaciones Distribuidas con mecanismos seguridad	6-15 semana	Laboratorio	60%
Examen Final			20%
Total			100%

CRITERIOS DE CALIFICACIÓN

La nota de los alumnos se calculará en base a las resolución de los ejercicios prácticos propuestos en el laboratorio semanalmente y el examen final

Los derechos y deberes de los estudiantes universitarios están desarrollados en los Estatutos de la Universidad Politécnica de Madrid (BOCM de 15 de noviembre de 2010) y en el estatuto del Estudiante Universitario (RD 1791/2010 de 30 de diciembre).

El artículo 124 a) de los EUPM fija como deber del estudiante…"*seguir con responsabilidad y aprovechamiento el proceso de formación, adquisición de conocimiento y aprendizaje correspondiente a su condición de universitario*" .. y el artículo 13 del Estatuto del estudiante universitario en el punto d) especifica también como deber del estudiante universitario "*abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad*".

En el caso de que en el desarrollo de las pruebas de evaluación se aprecie el incumplimiento de los deberes como estudiante universitario, el coordinador de la asignatura podrá ponerlo en conocimiento del director del Centro que de acuerdo con lo establecido en el artículo 74 (n) de los EUPM tiene competencias para "*proponer la iniciación del procedimiento disciplinario a cualquier miembro de la Escuela, por propia iniciativa o a instancia de la Comisión de Gobierno*" al Rector, en los términos previsto en los estatutos y normas de aplicación.