ANX-PR/CL/001-02

GUÍA DE APRENDIZAJE

ASIGNATURA

Desarrollo de software de seguridad en red

CURSO ACADÉMICO - SEMESTRE

2015-16 - Primer semestre

Datos Descriptivos

Nombre de la Asignatura	Desarrollo de software de seguridad en red
Titulación	10AN - Master Universitario en Ingenieria Informatica
Centro responsable de la titulación	E.T.S. de Ingenieros Informaticos
Semestre/s de impartición	Tercer semestre
Carácter	Optativa
Código UPM	103000638
Nombre en inglés	Network Security Software Development

Datos Generales

Créditos	4.5	**Curso**	2
Curso Académico	2015-16	**Período de impartición**	Septiembre-Enero
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Superadas

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

Otros Requisitos

El plan de estudios Master Universitario en Ingenieria Informatica 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

El coordinador de la asignatura no ha definido otros conocimientos previos recomendados.

Competencias

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.

CE4 - Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos.

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.

CG10 - Conocimiento y comprensión de la informática necesaria para la creación de modelos de información, y de los sistemas y procesos complejos

CG3 - Especificación y realización de tareas informáticas complejas, poco definidas o no familiares

CG5 - Aplicación de los métodos de resolución de problemas más recientes o innovadores y que puedan implicar el uso de otras disciplinas

Resultados de Aprendizaje

RA133 - Ser capaz de identiSer capaz de crear la infraestructura de seguridad necesaria en servicios y aplicaciones.ficar los servicios de seguridad en el diseño de aplicaciones en Red.

RA134 - Diseñar e implementar Aplicaciones Distribuidas con Mecanismos de Seguridad.

RA132 - Ser capaz de identificar los servicios de seguridad en el diseño de aplicaciones en Red.

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Mengual Galan, Luis **(Coordinador/a)**		luis.mengual@upm.es	

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

La asignatura de Desarrollo de Software de Seguridad en Red tiene como objetivo que el alumno sea capaz, en primer lugar, de identificar las amenazas y conocer los potenciales ataques que pueden sufrir las aplicaciones distribuidas funcionando en red.

En segundo lugar, el alumno será capaz de construir la infraestructura de seguridad necesaria en servicios y aplicaciones (certificados electrónicos, almacenes de seguridad, listas de revocación de certificados, etc)

Por último, el alumno podrá diseñar e implementar aplicaciones distribuidas con mecanismos de seguridad utilizando herramientas o plataformas abiertas como OpenSSL, Keytool y Java.

En definitiva, el alumno será capaz de diseñar aplicaciones de seguridad, construir aplicaciones de manejo y gestión de certificados electrónicos, crear clientes/servidores SSL(Secure Sockets Layer) para utilizar en aplicaciones de comercio electrónico, desarrollar aplicaciones de firma y validación de documentos o aplicaciones de acceso a Bases de Datos con servicios de seguridad.

Temario

1. Arquitecturas de Seguridad

   1.1. Servicios de Seguridad en Red. ISO 7498-2. X.800

   1.2. Mecanismos, Funciones y Protocolos de seguridad

2. Modelos de Seguridad en Red

   2.1. Nivel de Sockets Seguro (SSL, Secure Socket Layer)

   2.2. Modelo de Kerberos

   2.3. Aplicaciones Seguras: Comercio electrónico seguro, Sistemas de Firma Biométrica, correo electrónico seguro s/mime

3. Desarrollo de aplicaciones con servicios de seguridad

   3.1. Plataformas, herramientas y librerías de desarrollo de aplicaciones: OpenSSL, Keytool, JCE (Java Cryptography Extension), JSSE (Java Secure Sockets Extension

   3.2. Gestión de Certificados y almacenes de seguridad

   3.3. Código Manejo certificados

   3.4. Protocolos de seguridad

   3.5. Conexiones SSL (autenticación de cliente, certificados autofirmados/ firmados por una CA, configuración parámetros del protocolo)

   3.6. Aplicaciones de Firma/verificación electrónica. Integración sistemas biométricos

   3.7. Aplicaciones de comercio electrónico

   3.8. Acceso confidencial y autenticado a Bases de Datos

Cronograma

Horas totales: 45 horas

Horas presenciales: 45 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	**Servicios, Mecanismos y Funciones de seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 2	**Servicios, Mecanismos y Funciones de seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 3	**Modelos de seguridad en Red** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 4	**Modelos de seguridad en Red** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 5	**Plataformas y herramientas de Seguridad (OpenSSL, Keytool)** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Gestión de Almacenes y Certificados** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 6	**Plataformas y herramientas de Seguridad (OpenSSL, Keytool)** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Gestión de Almacenes y Certificados** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prácticas Infraestructura Seguridad** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 7	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Código Manejo certificados** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 8	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Código Manejo certificados** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 9	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Aplicaciones Cliente/Servidor SSL** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 10	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Aplicaciones Cliente/Servidor SSL** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		

Semana 11	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Aplicaciones Firma electrónica** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 12	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Aplicaciones Firma electrónica** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 13	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Aplicaciones Comercio electrónico** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 14	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Aplicaciones Comercio electrónico** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 15	**Diseño de código seguro** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Diseño de código seguro Desarrollo de Aplicaciones con acceso confidencial y autenticado a una BD** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prácticas Aplicaciones Distribuidas con Mecanismos de Seguridad** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 16				**Examen final** Duración: 00:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 17				**Examen Evaluación Final** Duración: 00:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad no 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
6	Prácticas Infraestructura Seguridad	00:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	20%	3 / 10	CG10, CE7
15	Prácticas Aplicaciones Distribuidas con Mecanismos de Seguridad	00:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	60%	3 / 10	CG3, CG5, CE4, CE7
16	Examen final	00:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	20%	3 / 10	CE1
17	Examen Evaluación Final	00:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	No	100%	5 / 10	CG5, CG3, CE4, CE7, CG10, CE1

Criterios de Evaluación

Evaluación Continua:

La asignatura se evaluara con la entrega de los proyectos prácticos realizados en el laboratorio y agrupados en dos bloques Prácticas de Infraestructura de Seguridad y Prácticas de Aplicaciones Distribuidas con Mecanismos de Seguridad. Además habrá un examen teórico de la asignatura. El peso de cada uno de estos elementos en la evaluación continua es:

Prácticas de Infraestructura de Seguridad (20%)

Prácticas de Aplicaciones Distribuidas con Mecanismos de Seguridad (60%)

Examen Teórico (20%)

Es obligatorio la realizar el examen teórico y realizar las entregas de las prácticas.

Evaluación Por prueba final:

Para aquellos alumnos que de forma extraordinaria, no puedan realizar la evaluación continua, y previa petición por escrito durante los primeros 15 días del curso, la forma de evaluación de la asignatura será la siguiente, siendo excluyente con la evaluación continua.

Examen teórico en la fecha establecida en el calendario oficial de exámenes por jefatura de estudios.

Recursos Didácticos

Descripción	Tipo	Observaciones
Java Network Programming, 4º Edition. E. Rusty Harol, 0`really. 2013.	Bibliografía	
Cryptography and Network Security Principles and Practice Fifth Edition. W. Stallings 2011, Pearson Education, Inc., publishing as Prentice Hall	Bibliografía	
Network Security with OpenSSL. J. Viega, M. Messier, P. Chandra. 0`really 2002	Bibliografía	