ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

103000817 - Desarrollo De Software De Seguridad En Red

PLAN DE ESTUDIOS

10AN - Master Universitario En Ingenieria Informatica

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	103000817 - Desarrollo de Software de Seguridad en Red
No de créditos	6 ECTS
Carácter	Optativa
Curso	Segundo curso
Semestre	Tercer semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	10AN - Master Universitario en Ingenieria Informatica
Centro responsable de la titulación	10 - Escuela Tecnica Superior De Ingenieros Informaticos
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Luis Mengual Galan (Coordinador/a)	4303	luis.mengual@upm.es	Sin horario. Preguntar Profesor
Ernestina Menasalvas Ruiz	4303	ernestina.menasalvas@upm.es	Sin horario. Preguntar Profesor

* 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 Informatica no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Conocimientos de Programación Java, C, C++

4. Competencias y resultados de aprendizaje

4.1. Competencias

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

4.2. Resultados del aprendizaje

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

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.

5. Descripción de la asignatura y temario

5.1. 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.

5.2. Temario de la asignatura

1. Arquitecturas de Seguridad

   1.1. Seguridad en las Tecnologías de Transmisión de Datos

   1.2. Elementos de las Arquitecturas de Seguridad: Servicios, Mecanismos y Protocolos de Seguridad

2. Modelos de Seguridad en Red

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

   2.2. Aplicaciones Seguras: Comercio electrónico seguro, correo electrónico seguro s/mime, seguridad en aplicaciones Android

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

   3.9. Aplicaciones seguras en Android

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Arquitecturas de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
2	**Arquitecturas de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
3	**Modelos de seguridad en Red** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
4	**Modelos de seguridad en Red** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
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		
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** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 10:00
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		
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		
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		
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		
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		

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		
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		
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		
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** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 20:00
16				**Examen** ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 02:00 **Examen** ET: Técnica del tipo Prueba Telemática Evaluación sólo prueba final Presencial Duración: 02:00
17				

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 derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
6	Prácticas Infraestructura Seguridad	TI: Técnica del tipo Trabajo Individual	No Presencial	10:00	20%	3 / 10	CG10 CE4 CE7
15	Prácticas Aplicaciones Distribuidas con Mecanismos de Seguridad	TI: Técnica del tipo Trabajo Individual	No Presencial	20:00	60%	3 / 10	CG10 CE4 CE7
16	Examen	ET: Técnica del tipo Prueba Telemática	Presencial	02:00	20%	4 / 10	CG10 CE4 CE7

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
16	Examen	ET: Técnica del tipo Prueba Telemática	Presencial	02:00	20%	4 / 10	CG10 CE4 CE7

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
EXAMEN	ET: Técnica del tipo Prueba Telemática	Presencial	02:00	20%	5 / 10	CG10 CE4 CE7

7.2. Criterios de evaluación

Evaluación Distribuida o Progresiva:

La asignatura se evaluará 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. Estos proyectos prácticos tienen la consideración de actividades de realización obligatoria no recuperables. La fecha de entrega límite de estos proyectos se corresponderá a la fecha de la evaluación mediante prueba global.

La evaluación mediante prueba global consistirá en un examen teórico de la asignatura.

El peso de cada uno de estos elementos en la Evaluación Distribuida o Progresiva 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 los proyectos prácticos, habiendo un mínimo de 3 puntos en cada una de las partes de la Evaluación Distribuida o Progresiva.

Evaluación Extraordinaria:

Para la evaluación extraordinaria se deberán presentar (si no se han realizado en periodo docente) las Prácticas de Infraestructura de Seguridad y Prácticas de Aplicaciones Distribuidas con Mecanismos de Seguridad con consideración de actividades de realización obligatoria no recuperables. La fecha de entrega límite de estos proyectos se corresponderá a la fecha de la Evaluación Extraordinaria. Además, habrá un examen teórico de la asignatura.

El peso de cada uno de estos elementos en la Evaluación Extraordinaria es:

Prácticas de Infraestructura de Seguridad (20%)

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

Examen Teórico (20%)

En el examen extraordinario se establece un mínimo de 3 puntos en los bloques de actividades de realización obligatoria y un mínimo de 5 puntos en el Examen Teórico.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	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	
Criptography and Network Security. 4ª Edition. W. Stallings, Prentice Hall. 2005	Bibliografía	