ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

615000730 - Seguridad en sistemas y redes

PLAN DE ESTUDIOS

61TI - Grado En Tecnologias Para La Sociedad De La Informacion

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos....1
2. Profesorado....1
3. Conocimientos previos recomendados....2
4. Competencias y resultados de aprendizaje....2
5. Descripción de la asignatura y temario....4
6. Cronograma....6
7. Actividades y criterios de evaluación....8
8. Recursos didácticos....12

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615000730 - Seguridad en sistemas y redes
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Tercero curso
Semestre	Sexto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61TI - Grado en tecnologias para la sociedad de la informacion
Centro responsable de la titulación	61 - Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Eduardo Garcia Pardo (Coordinador/a)	4305	eduardo.pardo@upm.es	Sin horario. El horario de tutorías se publicará en la web de la ETSISI al comienzo del cuatrimestre

Jesus Sanchez Lopez	1117	jesus.sanchezl@upm.es	Sin horario. El horario de tutorías se publicará en la web de la ETSISI al comienzo del cuatrimestre

* 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 Grado en Tecnologias para la Sociedad de la Informacion no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Haber cursado y superado "Redes de Computadores" y "Seguridad de la Información"

- Disponer de conocimientos de Redes Avanzadas y Servicios de Internet

4. Competencias y resultados de aprendizaje

4.1. Competencias

CC05 - Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas.

CE01 - Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.

CE02 - Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.

CE04 - Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización

CE06 - Capacidad de concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil.

CE07 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

CT07 - Aprendizaje autónomo: El estudiante debe responsabilizarse de su propio aprendizaje, lo que le lleva a utilizar procesos cognitivos de forma estratégica y flexible, en función del objetivo de aprendizaje.

CT08 - Trabajo en equipo: Ser capaz de trabajar como miembro de un equipo interdisciplinar con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

OB07 - Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento.

4.2. Resultados del aprendizaje

RA136 - Comprende las características de seguridad de un sistema cortafuegos.

RA139 - Establece la mejor solución para un diseño de sistemas de túneles para interconectar usuarios o redes.

RA141 - Audita redes desde el punto de vista de la defensa y seguridad frente ataques, tanto internos como externos.

RA129 - Entiende y aplica los diferentes sistemas de cifrado.

RA130 - Genera y crea todas las estructuras de una PKI.

RA131 - .Configura adecuadamente servidores web seguros con soporte de cifrado con el protocolo SSL/TLS.

RA132 - Conoce y aplica las medidas de seguridad en un sistema operativo

RA133 - Comprende los mecanismos de seguridad en redes WIFI.

RA138 - Configura y dimensiona redes privadas virtuales

RA140 - .Conoce y aplica las técnicas de defensa frente a ataques hacking.

RA137 - Diseña un sistema de defensa de barrera, incorporando herramientas de detección de intrusos.

RA135 - Conoce debilidades de seguridad en los dispositivos móviles y los asegura.

RA134 - Dimensiona y configura adecuadamente el sistema de seguridad de una red WIFI.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

En la asignatura se estudian los contenidos necesarios para comprender los fundamentos de la seguridad en redes en sentido amplio. En el estudio se abarcan todos los aspectos de la seguridad aplicada a las redes imbricando conocimientos de criptografía aplicada con los conocimientos de protección de redes, basados en la esencia de funcionamiento de los protocolos de comunicaciones. En primer lugar se analiza a fondo y se comprenden los métodos de seguridad en redes WIFI, llegando a la posibilidad de indicar la realización de auditorías de estas, desde el punto de vista de la seguridad. Después se estudian los sistemas de protección de barrera como cortafuegos y las topologías de estos, así como el uso y puesta en funcionamiento de redes privadas virtuales. Al final se hace un barrido extenso en técnicas de hacking estableciendo los parámetros que permiten la compresión de los métodos de ataque a redes y las posibilidades de actuación para su defensa.

5.2. Temario de la asignatura

1. Criptografía aplicada. Certificados y estructura PKI. Protocolos SSL, TLS.
    - 1.1. Funciones HASH. Funciones HMAC.
    - 1.2. Criptografía básica. Simétrica. Asimétrica.
    - 1.3. Certificados digitales. Tipos. Formatos.
    - 1.4. Autoridades de Certificación. Firma digital.
    - 1.5. Cifrado de las comunicaciones. Protocolos de cifrado.
    - 1.6. TLS y SSL en Internet. Aplicación para el web.
    - 1.7. Autentificación del Servidor. Autentificación del Cliente.
2. Seguridad en redes wireless.
    - 2.1. Seguridad en redes wireless: Autentificación y confidencialidad.
    - 2.2. Asociación abierta. Asociación con WEP.
    - 2.3. Portal cautivo.
    - 2.4. WEP. Ataques al WEP.
    - 2.5. 802.11i. Fase 1. Acuerdo de política de seguridad.
    - 2.6. 802.11i. Fase2. Autentificación.
    - 2.7. 802.11i. Fase 3. Derivación y distribución de clave. Four way handsake.

2.8. 802.11i. Fase 4. Confidencialidad e integridad de datos. RSNA. Cifrado con TKIP. Cifrado con CCMP (AES).

2.9. Definiciones de WPA. WPA-PSK. WPA2 y WPA2-PSK

2.10. Debilidades y ataques de WPA y WPA2.

2.11. WPS. Wi-Fi Protected Setup. Funcionamiento y debilidades.

3. Seguridad en la red y el acceso. Cortafuegos y topologías.

3.1. Filtros de paquetes de datos.

3.2. Filtros de aplicación. Proxys. Filtros de kernel.

3.3. Ejemplos de proxys, ejemplos de filtros de red: iptables

3.4. Cortafuegos. Topologías de cortafuegos.

3.5. Dual homed host. Screned host. Screned subnet. Backbone.

3.6. Sistemas de detección de intrusos. IDS'S.

3.7. Sistemas de protección de intrusos. IPS'S.

4. Túneles y Redes privadas virtuales.

4.1. Túneles. Concepto. Tipos: de transporte y de red.

4.2. Túneles de transporte. Ejemplos: Sobre ssh. Sobre http.

4.3. Túneles de red.

4.4. IPsec. Protocolos AH y ESP. Modos transporte y túnel.

4.5. OpenVPN.

5. Hacking y prevención de ataques.

5.1. Concepto de hacking. Método para hackear un sistema.

5.2. Sniffers y Scanners de red. Sniffers especiales.

5.3. Detección del sistema operativo.

5.4. Ataques DoS (Denied of Service).

5.5. Hacking de unix. Exploits. Telnet inverso. Desbordamiento de buffers.

5.6. Hijacking de sesión.

5.7. Redirección ARP. Redirección de puertos TCP.

5.8. Rootkits. Defensa.

5.9. Defensa y prevención de ataques.

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
2	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Realización de Cuestionarios y Tareas (RA129,RA130)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
3	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Realización de Cuestionarios y Tareas (RA130, RA131)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
4	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA133, RA134, RA135)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
5	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA136, RA137)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
6	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA136, RA137)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
7				**Realización de prácticas (RA133, RA134, RA135)** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 04:00
8	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA138, RA139)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
9				**Examen parcial (RA133, RA134, RA129, RA137, RA130, RA131, RA136, RA135)** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00

10	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA138, RA139)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
11	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA140, RA141)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
12	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA137, RA141)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
13	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA137, RA141)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
14	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Exposición de conceptos teóricos y/o casos prácticos** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Realización de Cuestionarios y Tareas (RA140, RA141, RA132)** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
15				**Realización de prácticas (RA131)** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 04:00
16				**Examen parcial (RA139, RA140, RA137, RA131, RA138, RA141, RA132)** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00
17				**Examen final (RA129, RA130, RA131, RA132, RA133, RA134, RA135, RA136, RA137, RA138, RA139, RA140, RA141)** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00

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
2	Realización de Cuestionarios y Tareas (RA129,RA130)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CE04 CE07
3	Realización de Cuestionarios y Tareas (RA130, RA131)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CE04 CE06 CE07
4	Realización de Cuestionarios y Tareas (RA133, RA134, RA135)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CC05 CE07
5	Realización de Cuestionarios y Tareas (RA136, RA137)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CE04 CE06
6	Realización de Cuestionarios y Tareas (RA136, RA137)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	2%	0 / 10	CC05 CE06
7	Realización de prácticas (RA133, RA134, RA135)	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	5%	0 / 10	CT07 CT08 CE07
8	Realización de Cuestionarios y Tareas (RA138, RA139)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	2%	0 / 10	CT07 CE04 CE06 CE07
9	Examen parcial (RA133, RA134, RA129, RA137, RA130, RA131, RA136, RA135)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	35%	3 / 10	CE04 CE06 CE07 CT07 CC05

10	Realización de Cuestionarios y Tareas (RA138, RA139)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CE04 CE06 CE07
11	Realización de Cuestionarios y Tareas (RA140, RA141)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CE04 CE06 CE07
12	Realización de Cuestionarios y Tareas (RA137, RA141)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	1%	0 / 10	CT07 CE04 CE06
13	Realización de Cuestionarios y Tareas (RA137, RA141)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	2%	0 / 10	CE01 CE02 OB07 CE06
14	Realización de Cuestionarios y Tareas (RA140, RA141, RA132)	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	2%	0 / 10	CE01 CE02 OB07 CE07
15	Realización de prácticas (RA131)	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	10%	0 / 10	CT07 CT08 OB07 CE06
16	Examen parcial (RA139, RA140, RA137, RA131, RA138, RA141, RA132)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	35%	3 / 10	CE01 CE02 CE04 OB07 CE06 CE07

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen final (RA129, RA130, RA131, RA132, RA133, RA134, RA135, RA136, RA137, RA138, RA139, RA140, RA141)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	0 / 10	CT07 CT08 CC05 CE01 CE02 CE04 OB07 CE06 CE07

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen final (RA129, RA130, RA131, RA132, RA133, RA134, RA135, RA136, RA137, RA138, RA139, RA140, RA141)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	0 / 10	CT07 CT08 CC05 CE01 CE02 CE04 OB07 CE06 CE07

7.2. Criterios de evaluación

EVALUACIÓN CONTINUA:

La evaluación continua se realiza de tal manera que cada actividad, test, práctica, examen parcial o trabajo en grupo tiene un peso en la evaluación indicado por el cronograma de la tabla anterior. Durante el curso se van sumando, de forma ponderada, las puntuaciones obtenidas por la realización de las diversas tareas que se especifican. Teniendo en cuenta que la asistencia puntúa un 5% y la suma de las actividades de evaluación continua el otro 95%, se considerará aprobado todo aquel alumno que obtenga el 50% o más de la nota total considerada sobre 10 puntos.

La ponderación de los apartados de evaluación de la asignatura queda según los siguientes valores:

-Asistencia a clase 5%

-Cuestionarios y Tareas mediante respuesta telemática 15%

-Exámenes parciales 70% (35% el primero, 35% el segundo)

-Practicas de laboratorio 15% (5% la primera, 10% la segunda)

No obstante para que la evaluación sea considerada continua hay que cumplir los siguientes requisitos:

- **No tener más de 2 faltas** de asistencia no justificada.

- **Haber entregado en tiempo y forma el 100%** de las tareas y cuestionarios propuestos.

- **Haber asistido a todos los exámenes parciales** y haber obtenido una **calificación en cada parcial superior a 3 puntos sobre 10**.

- **Haber realizado todas las prácticas.**

En caso contrario el alumno deberá realizar un examen final teórico-práctico que incluirá todos los contenidos de la asignatura. El examen se realizará en la siguiente convocatoria, a aquella en la que ha seguido la evaluación continua.

EVALUACIÓN mediante SOLO EXAMEN FINAL:

Los alumnos que deseen ser evaluados SOLO mediante examen final y no seguir la evaluación continua, deberán solicitarlo en tiempo y forma al inicio del semestre, antes de la realización del primer examen parcial. Una vez finalizado el plazo no se admitirán peticiones excepto por motivos contemplados en la normativa.

El examen final consistirá en una prueba escrita sobre los contenidos teóricos y prácticos de la asignatura. Esta prueba se calificará sobre 10 puntos siendo necesario obtener una nota igual o superior a 5.

EVALUACIÓN CONVOCATORIA EXTRAORDINARIA:

La evaluación en convocatoria extraordinaria será igual que la EVALUACIÓN mediante SOLO PRUEBA FINAL

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Colección de diapositivas para cada tema	Otros	Diapositivas desarrollando el tema que se está impartiendo.
Enlaces web	Recursos web	Enlaces web a artículos con documentación aplicables a cada parte de los contenidos. Artículos situados en la página web de la asignatura.
Enlaces web para documentación	Bibliografía	http://www.kali.org https://es.wikipedia.org/wiki/MD5 https://es.wikipedia.org/wiki/Secure_Hash_Al gorithm https://es.wikipedia.org/wiki/Criptograf%C3% ADa https://es.wikipedia.org/wiki/Criptograf%C3% ADa_sim%C3%A9trica http://www.netfilter.org/
Pataforma moodle	Recursos web	Plataforma moodle de apoyo a la docencia:
Aula equipadas con ordenador proyector de video y pizarra.	Equipamiento	Proyector de video para seguir las explicaciones y demostraciones en directo.
Laboratorio de prácticas	Equipamiento	Laboratorio con 12 ordenadores con software adecuado para la realización de las prácticas.
Routers WIFI	Equipamiento	12 Routers WIFI y portátiles para la realización de las prácticas. Servidor RADIUS, configurado al efecto.