CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL

PLANIFICACIÓN DE LA DOCENCIA UNIVERSITARIA

GUÍA DOCENTE

Seguridad en las Redes y Sistemas Informáticos

1. DATOS DE IDENTIFICACIÓN DE LA ASIGNATURA.

Título:				**Grado en Ingeniería de Desarrollo de Contenidos Digitales**	
Facultad:				**Centro Universitario de Tecnología y Arte Digital**	
Departamento/Instituto:					
Materia:				**Fundamentos de sistemas de software y hardware**	
Denominación de la asignatura:				**Seguridad en las Redes y Sistemas Informáticos**	
Código:				**0048039**	
Curso:				**4**	
Semestre:				**1**	
Tipo de asignatura (básica, obligatoria u optativa):				**Optativa**	
Créditos ECTS:				**6**	
Modalidad/es de enseñanza:				**Presencial**	
Lengua vehicular:				**Castellano**	
Equipo docente:				**López Arredondo, Luis Javier**	
Profesor/a:				**López Arredondo, Luis Javier**	
Grupos:				**IDCD4**	
Despacho:				**Sala de profesores**	
Teléfono:	916402811	Ext.	113	E-mail:	luis.lopez@live.u-tad.com
Página web: u-tad.blackboard.com					

2. CONTENIDOS /TEMARIO / UNIDADES DIDÁCTICAS

Tema 1: Introducción a la Seguridad [1 clase]

1. Actualidad de la seguridad
2. Principios básicos de la seguridad
3. Reconocimiento de un ataque

Tema 2: Introducción a la Criptografía [1 clase]

1. Principios criptográficos
2. Cifrado Simétrico
3. Cifrado Asimétrico
4. Funciones Hash
5. Firma digital

Tema 3: Sistemas de Seguridad y Metodologías de Pruebas [2 clase]

1. Principales sistemas de seguridad
2. Análisis de riesgos
3. Auditorias de seguridad y test de intrusión. Metodologías
4. Preparación del laboratorio de practicas

Tema 4: Seguridad en Sistemas Informáticos [10 clases]

1. Obtención de información
2. Enumeración de equipos y servicios
3. Análisis de vulnerabilidades
4. Explotación de vulnerabilidades
5. Post-Explotación
6. Seguridad en el acceso por credenciales
7. Principios para la fortificación de sistemas

Tema 5: Seguridad en Aplicaciones Web [6 clases]

1. Tecnologías y protocolos
2. OWASP
3. Principales vulnerabilidades web
4. Proceso de auditoria web
5. Principios para la fortificación de aplicaciones web

Tema 6: Seguridad en Redes [3 clases]

1. Obtención y estudio de tráfico de red
2. Identificación y seguridad en dispositivos de red
3. Seguridad en la capa de enlace
4. Seguridad en la capa de red
5. Seguridad en IPv6
6. Evasión de medidas de seguridad en red
7. Principios para la fortificación de redes

Tema 7: Seguridad Wi-Fi [4 clases]

1. Tecnologías, protocolos y herramientas
2. WEP
3. WPA y WPA2
4. Ataques al cliente
5. Métodos de evasión de sistemas de seguridad
6. Principios para la fortificación de redes inalámbricas

3. RESULTADOS DE APRENDIZAJE EN RELACIÓN CON LAS COMPETENCIAS QUE DESARROLLA LA ASIGNATURA.

COMPETENCIAS ESPECÍFICAS	RESULTADOS DE APRENDIZAJE RELACIONADOS CON LAS COMPETENCIAS ESPECÍFICAS
CE3 - Demostrar conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería CE4 - Tener conocimiento de la estructura, arquitectura, organización, funcionamiento e interconexión de los sistemas informáticos y los fundamentos de su programación CE10 - Demostrar capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados	• Comprender los fundamentos de Internet y los protocolos de comunicación. • Comprender y manejar las herramientas para el almacenamiento, procesamiento y acceso a sistemas de información. • Conocer los principios de administración de un servidor o una red de ordenadores basada en sistemas Linux o Windows. • Conocer los potenciales riesgos de seguridad más frecuentes en una red informática y gestionarla para minimizarlos, empleando sistemas de seguridad internos y externos.

4. CONTENIDO Y CRONOGRAMA

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
Tema 0. Introducción a la asignatura	28/09/2015
Tema 1. Introducción a la seguridad	30/09/2015
Tema 2. Introducción a la criptografía	05/10/2015
Tema 3. Sistemas de Seguridad y Metodologías de Pruebas	07/10/2015 12/10/2015 (festivo)
Tema 4. Seguridad en Sistemas Informáticos	14/10/2015 19/10/2015 21/10/2015 26/10/2015 28/10/2015 02/11/2015 04/11/2015 09/11/2015 (festivo) 11/11/2015 16/11/2015
Tema 5. Seguridad en Aplicaciones Web	18/11/2015 23/11/2015 25/11/2015 30/11/2015 02/12/2015 07/12/2015
Tema 6. Seguridad en Redes	09/12/2015 14/12/2015 16/12/2015
Tema 7. Seguridad Wi-Fi	11/01/2016 13/01/2016 18/01/2016 20/01/2016

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DE ENSEÑANZA

MODALIDAD ORGANIZATIVA	MÉTODO DE ENSEÑANZA	COMPETENCIAS RELACIONADAS	HORAS PRESENCIALES	TRABAJO AUTÓNOMO	TOTAL DE HORAS
Clases teóricas	Lección magistral	CE3, CE4, CE10	21	1	22
Seminarios y talleres	Estudio de casos Resolución de ejercicios y problemas		0	0	0
Clases prácticas	Aprendizaje basado en problemas Aprendizaje orientado a proyectos	CE3, CE4, CE10	22	0	22
Practicas externas			0	0	0
Tutorías	Aprendizaje orientado a proyectos Aprendizaje basado en problemas	CE3, CE4, CE10	8	0	8
Actividades de evaluación		CE3, CE4, CE10	8	0	8
Estudio y trabajo en grupo	Aprendizaje cooperativo	CE3, CE4, CE10	1	21	23
Estudio y trabajo autónomo, individual	Estudio de casos Resolución de ejercicios y problemas Aprendizaje basado en problemas Aprendizaje orientado a proyectos	CE3, CE4, CE10	0	68	68

6. SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	CRITERIOS DE EVALUACIÓN	VALORACIÓN RESPECTO A LA CALIFICACIÓN FINAL (%)
Práctica 1: Seguridad en Sistemas Informáticos	Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial.	15%
Práctica 2: Seguridad en Aplicaciones Web	Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial.	15%
Práctica 3: Seguridad en Redes	Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial.	10%
Práctica 4: Seguridad Wi-Fi	Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial.	10%
Exámenes Intermedios	Evaluación de 0 a 10. Es necesario obtener al menos un 5 en el examen para aprobar cada examen.	10%
Examen Final de la asignatura	Evaluación de 0 a 10. Es necesario obtener al menos un 5 en el examen para aprobar la teoría de la asignatura.	25%
Trabajo Investigación	Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor del trabajo y defensa presencial.	15%

Consideraciones generales acerca de la evaluación:

A medida que se avance en el temario habrá problemas o ejercicios cortos planteados por el profesor. Los problemas y ejercicios están pensados para que el alumno los resuelva en el tiempo de clase, pero, si no le da tiempo a acabarlos del todo, deberá finalizarlos fuera de clase.

En clase se explicarán los problemas y ejercicios propuestos. Durante el periodo de ejercicios de cada clase, el profesor irá pasando por cada alumno para corregir y valorar, delante de él, sus ejercicios de la clase anterior. El alumno deberá responder adecuadamente a las preguntas que el profesor le haga sobre sus ejercicios.

A todos los efectos, una nota inferior a un 5 se considera suspensa. Es necesario obtener al menos un 5 en la nota final tanto de teoría como de práctica para poder aprobar la asignatura. Existen dos oportunidades para ello: la convocatoria ordinaria y la extraordinaria.

En la convocatoria ordinaria:

1. Si la nota final de las prácticas es igual o superior a un 5 pero el examen final ordinario está suspenso, la asignatura estará suspensa.

2. Si la nota del examen final ordinario es igual o superior a un cinco, la nota final de la asignatura se calculará obteniendo la media ponderada de ambas. En la evaluación continua y no continua los pesos serán de 50%-50% (prácticas y teoría).

En la convocatoria extraordinaria:

1. Aquellos alumnos que hayan suspendido la asignatura en la convocatoria ordinaria, deberán realizar la parte que tengan suspensa (teoría y/o practica) en la convocatoria extraordinaria.

2. Si se aprueban ambas prácticas por separado así como el examen final extraordinario, la nota final extraordinaria se calculará como la media ponderada (50%-50%) de las prácticas y el examen.

El porcentaje de presencialidad es del 80%. Las notas del examen final y de las prácticas no se guardan entre cursos académicos sucesivos.

Las prácticas o cualquier examen estarán suspensos si se descubre que un alumno (o varios) ha copiado a otro (o a varios, todos los alumnos involucrados estarán suspensos) o bien ha copiado de un libro o de Internet. Además, la Universidad abrirá expedientes disciplinarios a todos los alumnos involucrados, pudiendo desembocar incluso en su expulsión.

Los exámenes y los ejercicios constarán de uno o varios de los siguientes tipos de preguntas:

- Cuestiones teóricas cortas.
- Preguntas de tipo test sobre teoría o elegir el resultado final de un ejercicio.
- Problemas y casos prácticos.
- Preguntas sobre las prácticas.

7. BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía básica (1-3 libros)

- "**Hacking Exposed 6: Network Security Secrets & Solutions**, Editorial: McGraw-Hill"
- "**The Web Application Hacker's Handbook** (Second Edition), Editorial: Wiley"
- "**Mastering Wireless Penetration Testing for Highly Secured Environments**, Editorial: Packtpub"

Bibliografía recomendada (Max 10 libros)

- "Metasploit, Penetration Testers Guide, Editorial: No Starch Press"
- "Violent Python A Cookbook for Hackers Forensic, Editorial: Syngressd"
- "Mastering Kali Linux for Advanced Penetration Testing, Editorial: Wiley"

8. MATERIAL, SOFTWARE Y HERRAMIENTAS NECESARIAS

TIPOLOGÍA DEL AULA:

Aula de ordenadores con ordenador para el profesor conectado a proyector.

MATERIALES:

- Pizarra blanca
- Proyector

SOFTWARE:

- VMware / Virtual Box