UNIVERSIDAD DE EXTREMADURA

Plan Docente de una materia

"Seguridad y Protección de la Información"

I. Descripción y contextualización

Identificación y características de la materia				
Denominación	Seguridad y Protección de la Información			
Curso y Titulación	5º Ingeniería Informática			
Profesor	Lorenzo M. Martínez Bravo			
Área	Ingeniería Telemática			
Departamento	*Informática*			
Tipo y ctos. LRU	Optativa (4,5+1,5 créditos, LRU)		Básica	
Coeficientes	Practicidad: 3 (medio-alto, profesional)		Agrupamiento: 2 (medio-bajo)	
Duración ECTS (créditos)	Cuatrimestral		5,67 (141 h.)	
Distribución ECTS (rangos)	Grupo Grande: 25%	Seminario-Lab.: 5 %	Tutoría ECTS: 4%	No presenciales: 66%
	Horas 36	Horas 7	Horas 6	Horas 92
Descriptores (según BOE)	Integridad, disponibilidad y confidencialidad de la información. Seguridad física y lógica. Criptografía. Seguridad en la transmisión de datos. Planes de recuperación.			

*Contextualización curricular**

Conexión con las competencias genéricas y específicas del Título

26. Gestionar las autorizaciones de acceso para los usuarios.
29. Responsabilidad de la integridad de los datos y de la existencia de copias de seguridad.
39. Evalúa nuevos productos informáticos que pueden aportar mejoras tanto en los sistemas existentes, como para el desarrollo de nuevos sistemas.
42. Estudio de la evolución de las nuevas tecnologías, sobre todo de aquellas que pueden aportar mejoras importantes en los sistemas utilizados en la empresa
49. Establecer políticas de seguridad, técnicas criptográficas, cortafuegos (componentes, configuraciones, productos), instalación y configuración, definición de reglas de filtrado, conexiones y servicios.

Interrelaciones con otras materias
La asignatura *Seguridad y Protección de la Información* está interrelacionada principalmente con las siguientes materias en la titulación de Ingeniería en Informática:

- *Sistemas de Comunicación de Datos* (tercer curso), es la primera toma de contacto con las comunicaciones en la titulación y los alumnos estudian las partes relacionadas con el nivel físico del modelo RM-OSI. Proporciona la base para entender la estructura de las redes, así como su terminología.
- *Autopistas de la Información* (tercer curso), donde, tratándose de una materia optativa, los alumnos se familiarizan con los aspectos tecnológicos, legales, éticos y sociales del diseño, implantación y uso de sistemas telemáticos en la actualidad. Además, se realiza una introducción a la problemática de seguridad en la red Internet.
- *Redes* (cuarto curso), se analiza y estudia en profundidad los niveles superiores de las redes, donde aparecen los principales problemas de seguridad.

II. Objetivos

Relacionados con competencias académicas y disciplinares	*Vinculación*
Descripción	*CET*[i]
1. Establecer políticas de seguridad, técnicas criptográficas, cortafuegos (componentes, configuraciones, productos), instalación y configuración, definición de reglas de filtrado, conexiones y servicios.	26,49
2. Responsabilidad de la integridad de los datos y de la existencia de copias de seguridad.	29
3. Conocimiento sobre las técnicas actuales para la protección de la información y la evolución de las mismas.	39,42
4. Capacidad para construir aplicaciones seguras.	39

Relacionados con otras competencias personales y profesionales	*Vinculación*
Descripción	*CET*
5. Conocer y aplicar la normativa referente a la materia que existe a nivel autonómico, nacional e internacional	12
6. Resolver problemas con creatividad y confianza en los propios conocimientos.	9
7. Ser capaz de comunicar conocimientos especializados.	13
8. Formarse y actualizar conocimientos de forma continuada.	14
9. Trabajar en equipo	13

III. Contenidos

*Selección y estructuración de conocimientos generales**

Secuenciación de bloques temáticos y temas
1. El problema de la Seguridad Informática
1.1. Introducción 1.2. Características de la intrusión informática 1.3. Tipos de brechas en la seguridad 1.4. Puntos de vulnerabilidad en la Seguridad 1.5. Las personas involucradas 1.6. Métodos de defensa
2. Análisis de riesgos. Planes de seguridad
2.1. Introducción 2.2. Análisis de Riesgos 2.3. Plan de Seguridad
3. Evaluación de sistemas seguros
3.1. Introducción 3.2. Libro Naranja 3.3. Criterios Europeos.
4. Aspectos legales de la seguridad
4.1. Introducción 4.2. Propiedad intelectual 4.3. Legislación española
5. Introducción a la criptografía
5.1. Introducción 5.2. Teoría de la Información 5.3. Teoría de los Números 5.4. Teoría de la Complejidad
6. Criptografía clásica
6.1. Historia de la criptografía. 6.2. Clasificación de los Métodos criptográficos 6.3. Métodos de sustitución 6.4. Métodos de transposición 6.5. Máquinas de cifrar
7. Criptografía moderna
7.1. Tipos de algoritmos criptográficos 7.2. Algoritmos de clave privada 7.3. Algoritmos de clave pública 7.4. Modos de operación 7.5. Cifrado continuo
8. Funciones hash
8.1. Funciones hash 8.2. Códigos MAC
9. Gestión de claves
9.1. Introducción 9.2. Generación de claves 9.3. Almacenamiento de claves 9.4. Distribución de claves 9.5. Mantenimiento de claves
10. Esquemas y protocolos de seguridad
10.1. Introducción 10.2. Protocolos de autenticación 10.3. Protocolos de firma digital 10.4. Otros protocolos
11. Introducción a la Seguridad en Internet
11.1. Introducción

11.2. Problemas de seguridad en la Web 11.3. Problemas en otros protocolos 11.4. Cortafuegos
12. Protocolos Seguros en Internet
12.1. Introducción 12.2. IPSec 12.3. SSL 12.4. Otros protocolos
13. PKIs
13.1. Introducción 13.2. Certificados digitales 13.3. Autoridades de certificación 13.4. Estándares
14. Comercio electrónico
14.1. Introducción 14.2. SET 14.3. Otras soluciones

Interrelación			
Requisitos (Rq) y redundancias (Rd)		Tema	*Procedencia*
Introducción a la Seguridad en Internet	Rd	11-14	Autopistas de la Información (3º)
Fundamentos de Redes	Rq	1-14	Redes (3º)/ SCD (3º)

IV. Metodología docente y plan de trabajo del estudiante

Actividades de enseñanza-aprendizaje				*Vinculación*	
Descripción y secuenciación de actividades	*Tipo*[ii]		*D*[iii]	*Tema*	*Objet.*
1. Presentación de la asignatura	GG	C-E	0,5	1-14	Todos
2. Conocimiento de alumnos	GG	C-E	0,5	1-14	Todos
3. Exposición de los problemas de seguridad informática	GG	T	1	1	1-4
4. Estudio de los contenidos explicados	NP	T	1	1	1-4
5. Discusión en clase	GG	T	1	2	1
6. Estudio de los contenidos	NP	T	1	2	1
7. Discusión en clase	GG	T	1	3	1,3,5
8. Realización de supuesto práctico	S	P	4	1-2	1,3,5
9. Estudio de los contenidos	NP	T	1	3	1,3,5
10. Discusión en clase	GG	T	1	4	1,3,5
11. Estudio de los contenidos	NP	T	1	4	1,3,5
12. Exposición de los fundamentos de la criptografía	GG	T	4	5	1-4
13. Estudio de los contenidos	NP	T	2	5	1-4
14. Resolución de ejercicios sobre los fundamentos de la criptografía	NP	P	1	5	1-4
15. Resolución de ejercicios sobre los fundamentos de la criptografía	Tut	T-P	2	5	1-4
16. Exposición de la criptografía clásica	GG	T	3	6	1-4
17. Estudio de los contenidos	NP	T	2	6	1-4
18. Resolución de ejercicios sobre los fundamentos de la criptografía	NP	P	2	6	1-4
19. Exposición de la criptografía moderna	GG	T	8	7-8	1-4
20. Estudio de los contenidos	NP	T	4	7-8	1-4
21. Realización de un supuesto práctico	S	P	2	7-8	1-4
22. Resolución de ejercicios	NP	P	4	7-8	1-4
23. Resolución de ejercicios	Tut	T-P	2	6-8	1-4
24. Exposición de esquemas y protocolos seguros	GG	T	4	9-10	1-4
25. Estudio de contenidos	NP	T	4	9-10	1-4
26. Realización de un supuesto práctico	S	P	4	9-10	1-4
27. Resolución de ejercicios	NP	P	2	9-10	1-4
28. Resolución de ejercicios	Tut	T-P	2	9-10	1-4
29. Exposición de Contenidos	GG	T	2	11	1-4
30. Estudio de contenidos	NP	T	2	11	1-4
31. Exposición de Contenidos	GG	T	2	12	1-4
32. Realización de un supuesto práctico	S	P	4	9-12	1-4
33. Estudio de contenidos	NP	T	2	12	1-4
34. Exposición de Contenidos	GG	T	2	13	1-4
35. Estudio de contenidos	NP	T	2	13	1-4
36. Exposición de Contenidos	GG	T	2	14	1-4
37. Estudio de contenidos	NP	T	2	14	1-4
38. Estudio y preparación del examen final	NP	T-P	20	1-14	Todos
39. Examen final	GG	C-E	3	1-14	Todos
40.					
41.					
42.					
43.					
44.					
45.					
46.					
47.					
48.					
49.					
50.					
51.					
52.					
53.					
54.					
55.					

Distribución del tiempo (ECTS)			*Dedicación del alumno*		*Dedicación del profesor*	
Distribución de actividades		*Nº alumnos*	*H. presenciales*	*H. no presenc.*	*H. presenciales*	*H. no presenc.*
Grupo grande (Más de 20 alumnos)	C-E	40	1	0	1	20
	Teóricas	40	35	22	35	10
	Prácticas	40	-	7	-	10
	SubTotal		36	29	36	40
Seminario-Laboratorio (6-20 alumnos)	C-E	20	-	-	-	10
	Teóricas	20	-	-	-	-
	Prácticas	20	7	7	14	7
	Subtotal		7	7	14	7
Tutoría ECTS (1-5 alumnos)	C-E	5	-	-	-	5
	Teóricas	5	3	-	24	8
	Prácticas	5	3	-	24	8
	Subtotal		6	-	48	21
Tutoría comp. y preparación de ex. (VII)		1	-	20	-	12
Totales			49 (2 ECTS)	92 (3,68 ECTS	98	80

*Otras consideraciones metodológicas**
Recursos y metodología de trabajo en las actividades presenciales
Recursos y metodología de trabajo en las actividades semi-presenciales y no presenciales
Recursos y metodología de trabajo para los alumnos que no han alcanzado los requisitos
Recursos y metodología de trabajo para desarrollar competencias transversales

V. Evaluación

*Criterios de evaluación**	*Vinculación**	
Descripción	*Objetivo*	*CC*
Conocer los conceptos teóricos de la asignatura	Todos	70%
Comparar los distintos métodos y técnicas que se presenten.	Todos	
Resolver problemas y cuestiones sobre los conceptos desarrollados	Todos	
Realizar los supuestos prácticos	Todos	30%

Actividades e instrumentos de evaluación		
Tutorías ECTS	Observación de la participación en las actividades prácticas y teóricas	10%
Seminarios	Realización de los supuestos prácticos	30%
Examen final	Prueba de desarrollo escrita	60%

VI. Bibliografía

Bibliografía de apoyo seleccionada
B. Schneier *"Applied Criptography"* John Weley & Sons Ltd., 1993 (Ba-2424) Richard E. Smith *"Internet Criptography"* Addison-Wesley, 1997
*Bibliografía o documentación de ampliación, sitios web…**
Sitio web de la asignatura, con los apuntes y material necesario: http://it.unex.es/sypi J.L. Morant, A. Ribagorda, J. Sancho *"Seguridad y Protección de la Información"* Centro de Estudios Ramón Areces S.A., Madrid 1994 (Ba-2174) Charles P. Pfleeger *"Security in Computing"* 2ª Edición, Prentice Hall International, Inc., 1997

Códigos.-

[i] *CET: Competencias Específicas del Título* (véase el apartado de Contextualización curricular)

[ii] *Tipos de actividades*: GG (Grupo Grande); S (Seminario o Laboratorio); Tut (Tutoría ECTS); No presenciales (NP); C-E, I (Coordinación o evaluación); T, II (Teórica de carácter expositivo o de aprendizaje a partir de documentos); T, III (Teórica de discusión); P, IV (Prácticas basadas en la solución de problemas); P, V (Prácticas basadas en la observación, experimentación, aplicación de destrezas, estudio de casos…); P, VI (Prácticas con proyectos o trabajos dirigidos); T-P, VII (Otras teórico-prácticas).

[iii] *D: Duración* en sesiones de 1 hora de trabajo presencial o no presencial (considerando en cada hora 50-55 minutos de trabajo neto y 5-10 de descanso).