ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2015/2016

Grado en Ingeniería Informática itinerario Ingeniería de Computadores

DATOS DE LA ASIGNATURA			
Nombre:			
Seguridad de Sistemas Informáticos			
Denominación en inglés:			
Informatic Systems Security			
Código:		**Carácter:**	
606010231		Obligatorio	
Horas:			
	Totales	**Presenciales**	**No presenciales**
Trabajo estimado:	150	60	90
Créditos:			

	Grupos reducidos			
Grupos grandes	**Aula estándar**	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
4.14	0	1.86	0	0

Departamentos:	**Áreas de Conocimiento:**
Ingeniería Electrónica, Sistemas Informáticos y Automática	Ingeniería de Sistemas y Automática
Curso:	**Cuatrimestre:**
4º - Cuarto	Segundo cuatrimestre

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Diego A. López García	diego.lopez@diesia.uhu.es	959217668	Edif. Torreumbría TUP1-05

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

-Conceptos relacionados con la seguridad de sistemas informáticos.
-Áreas de seguridad: acceso, canal y perímetro.
-Políticas de seguridad
-Seguridad de Perímetro: Cortafuegos, Técnicas de filtrado.
-Seguridad en el canal: Criptografía simétrica y asimétrica. Redes Privadas Virtuales. Protocolos seguros.
-Seguridad de acceso: Autenticación. Firma digital. Autoridades certificadoras.
-Seguridad en servidores, en PC clientes, en conmutadores y enrutadores.

1.2. Breve descripción (en inglés):

-Concepts related to the security of computer systems.
-Safety areas: access, perimeter and channel.
-Security Policies.
-Perimeter Security: Firewall, Filtering Techniques.
-Safety in the channel: symmetric and asymmetric cryptography. Virtual Private Networks. secure Protocols.
-Access Security: Authentication. Digital Signature. Certificate authorities.
-Safety in servers, PC, switches and routers.

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

Esta asignatura imparte conocimientos avanzados que requieren conceptos de redes de ordenadores y sistemas operativos. No obstante, no se precisa un dominio exhaustivo por parte del alumno en dichas materias, ya que se recordará en clase los elementos que sean pertinentes.

2.2. Recomendaciones:

No es necesario realizar ninguna preparación para acometer el estudio de esta asignatura.

3. Objetivos (Expresados como resultados del aprendizaje):

-Dominar los contenidos impartidos.
-Ser capaz de configurar VPNs.
-Ser capaz de administrar políticas de seguridad en cortafuegos.
-Ser capaz de detectar debilidades en los equipos y protegerlos.

4. Competencias a adquirir por los estudiantes

4.1. Competencias específicas:

- **CE6-IC:** Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

4.2. Competencias básicas, generales o transversales:

- **CB5:** Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
- **G02:** Capacidad de comunicación oral y escrita en el ámbito académico y profesional con especial énfasis, en la redacción de documentación técnica
- **G05:** Capacidad de trabajo en equipo.
- **T02:** Conocimiento y perfeccionamiento en el ámbito de las TIC’s

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones de Resolución de Problemas.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Resolución de Problemas y Ejercicios Prácticos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Clases teóricas en las que se explicarán los contenidos temáticos y se realizarán actividades académicamente dirigidas para afianzar los conocimientos asimilados. Dichas actividades podrán incluir exposiciones, debates y resolución de problemas. Sesiones prácticas en el laboratorio orientadas a la aplicación de lo aprendido en teoría y al desarrollo de nuevas capacidades y técnicas habituales en el área de la seguridad.

6. Temario desarrollado:

T1. Conceptos relacionados con la seguridad de sistemas informáticos
-Definiciones.
-Áreas de seguridad: acceso, canal y perímetro.
-Políticas de seguridad.
-Instituciones relacionadas con la seguridad
T2. Seguridad en routers.
-Vulnerabilidades de los routers.
-Barreras de seguridad disponibles
-Aplicaciones de detección: Nmap.
T3. Seguridad en PCs
-Keyloggers
-Debilidades en el inicio
-Debilidades en el SO
T4. Seguridad de Perímetro
-Cortafuegos
-Técnicas de filtrado
T5. Seguridad en el canal
-Fundamentos de criptografía
-Criptografía simétrica: Algoritmos DES, 3DES y AES.
-Algoritmos de flujo.
-Criptografía asimétrica: DH, RSA y ElGamal.
T6. Seguridad en el acceso
-Autenticación.
-Firma digital.
-Conexiones seguras (SSL-TLS)
-Autoridades certificadoras.
T7. Seguridad LAN y en servidores
-Vulnerabilidades LAN.
-Medidas de seguridad en conmutadores.
-Vulnerabilidades en servidores web.
-Herramientas de diagnóstico.
T8. Redes Privadas Virtuales
-Tipos de VPN
-Protocolo GRE
-Protocolo IPSec.

7. Bibliografía

7.1. Bibliografía básica:

Seguridad informática - Ethical Hacking (Ediciones ENI). Autores: Marion AGÉ et. al.
CCNP Security SECURE 642-637 Official Cert Guide. Autores: Sean Wilkins, Franklin H. Smith III. Ed. Cisco Press.

7.2. Bibliografía complementaria:

HACKING Y SEGURIDAD EN INTERNET. EDICION 2011. Autores: GARCIA-MORAN, JEAN PAUL et. al. Ed. RA-MA.
HACKER. EDICION 2012, Ed.Anaya.
REDES PRIVADAS VIRTUALES, JAVIER ANDRES ALONSO. Ed. RA-MA, 2009

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos
- Seguimiento Individual del Estudiante

8.2. Criterios de evaluación y calificación:

La evaluación consistirá en un examen teórico (70%) unido a la valoración de las prácticas de laboratorio (30%) para los alumnos que no deseen participar en las actividades de clase. Para aquellos que sí deseen participar, las actividades académicamente dirigidas y actividades de clase se tendrán en cuenta en la evaluación, sustituyendo la evaluación teórica en un 10% (60% el examen teórico y 10% las AAD). Teoría y prácticas han de ser aprobadas independientemente para poder superar la asignatura.

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos Aula Estándar	Grupos Reducidos Aula de Informática	Grupos Reducidos Laboratorio	Grupos Reducidos prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	3	0	0	1.5	0		Tema 1
#2	3	0	0	1.5	0	Practica 1	Tema 1
#3	1.5	0	0	0	0		Tema 1
#4	3	0	0	1.5	0	Practica 2	Tema 2
#5	3	0	0	1.5	0		Tema 2
#6	3	0	0	1.5	0		Tema 3
#7	3	0	0	1.5	0		Tema 3
#8	3	0	0	1.5	0	Practica 3	Tema 4
#9	3	0	0	1.5	0		Tema 4
#10	3	0	0	1.5	0		Tema 5
#11	1.5	0	0	0	0		Tema 5
#12	3	0	0	1.5	0	Practica 4	Tema 6
#13	3	0	0	1.5	0		Tema 6
#14	3	0	0	1.5	0		Tema 7
#15	2.4	0	0	0.6	0	Practica 5	Tema 7
	41.4	0	0	18.6	0		