ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2019/2020

Grado en Ingeniería Informática itinerario Ingeniería de Computadores

DATOS DE LA ASIGNATURA			
Nombre:			
Seguridad de Sistemas Informáticos			
Denominación en inglés:			
Computer 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, de Sistemas Informáticos y Automática	Ingeniería de Sistemas y Automática
Curso:	**Cuatrimestre:**
4º - Cuarto	Segundo cuatrimestre

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*López García, Diego Antonio	diego.lopez@diesia.uhu.es	959217668	Despacho 234, 2ªPlanta, Edif. ETSI, Campus El Carmen

*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.
- **CT2:** Desarrollo de una actitud crítica en relación con la capacidad de análisis y síntesis.
- **CT3:** Desarrollo de una actitud de indagación que permita la revisión y avance permanente del conocimiento.
- **CT4:** Capacidad de utilizar las Competencias Informáticas e Informacionales (CI2) en la práctica profesional.

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 orales (trabajos en grupo orientados a la exposición oral sobre algún ataque informático relevante), debates (uso de una aplicación web de debate para seleccionar las acciones más relevantes que un técnico cualificado debe llevar a cabo antes de una auditoría de seguridad), resolución de problemas (de configuración de equipos, de cifrado), concursos (elaboración de preguntas sobre el tema expuesto), etc. 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 equipos (routers y PCs).
-Vulnerabilidades de los routers.
-Barreras de seguridad disponibles para routers
-Aplicaciones de detección: Nmap.
-Keyloggers
-Debilidades en el inicio de PCs
-Debilidades en el SO (PCs)
T3. Seguridad de Perímetro
-Cortafuegos
-Técnicas de filtrado
T4. Seguridad en LAN y en servidores
-Vulnerabilidades LAN.
-Medidas de seguridad en conmutadores.
-Vulnerabilidades en servidores.
-Técnicas de hacking.
T5. Seguridad en el canal
-Fundamentos de criptografía
-Algortimos de hashing.
-Criptografía simétrica: Algoritmos DES, 3DES y AES. Algoritmos de flujo.
-Criptografía asimétrica: DH, RSA y ElGamal.
-Autenticación y firma digital.
-Conexiones seguras (SSL-TLS)
-Infraestructura PKI.
-Técnicas de Cracking.
-Tor y e-voting
T6. 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:

Ethical Hacking: Teoría y práctica para la realización de un pentesting. Autor: Pablo González Pérez. Editorial, año: 0xWord. ISBN: 978-84-617-0576-4
Metasploit para Pentesters. 4ª Edición revisada y ampliada.Autor: Pablo González Pérez y Chema Alonso.Editorial, año: 0xWord. ISBN: 978-84-617-1516-9
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
Internal hacking y contramedidas en entorno Windows, Kapfer, Philippe Ediciones ENI

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Seguimiento Individual del Estudiante

8.2. Criterios de evaluación y calificación:

Pruebas:
Examen teórico: Consiste en un examen escrito para el que el alumno sólo necesitará el bolígrafo. El tiempo para la prueba será de una hora y media. Se estructura en preguntas (70%) y problemas (30%). Los contenidos sobre los que se inquiere consisten en todo lo explicado en clase y disponible como documentación en la plataforma Moodle.
Prueba práctica: Se trata de la descripción de un caso a resolver mediante la configuración adecuada de los equipos y/o el uso de los programas explicados en las sesiones de prácticas. Para la prueba el alumno sólo necesitará su bolígrafo. Dicha prueba podrá ser en el laboratorio o en un aula y tendrá una duración de una hora. El contenido será el presente en la memoria de las prácticas.
Evaluación contínua:
La evaluación constará de un examen teórico y además de:
-la valoración de las prácticas de laboratorio. Éstas tendrán una serie de hitos (pruebas demostrables ante el profesor) de los cuales los primeros son obligatorios y darán la calificación de 5. Los siguientes hitos son opcionales y permitirán llegar hasta la calificación de 10.
-las actividades académicamente dirigidas y actividades de clase permitirán al alumno obtener puntos. Por ejemplo un punto para una pregunta contestada de forma acertada al final de la clase sobre el tema recién impartido, hasta cuatro puntos para la exposición oral, hasta dos por el debate, etc. Al final de curso cada alumno tendrá una serie de puntos obtenidos: *Po*. Si el máximo de puntos que se podrían obtener es *Pm*, se define el parámetro *p* como *p=Po/Pm*.
La nota en actas de la evaluación contínua será: 0,3 x Prácticas + (0,7 - 0,2 x p) x Teoría + 2 x p. Teoría y prácticas han de ser aprobadas independientemente para poder superar la asignatura.
Evaluación única final (convocatorías ordinarias I, II, III y extraordinaria para finalización del título).
La evaluación final constará de un examen teórico y, para aquellos que no hayan aprobado las prácticas en éste o en algún curso anterior, de una prueba práctica. Si el alumno aprobó las prácticas en algún momento la nota en actas será la del examen teórico en exclusiva. Si no, la nota en actas será 70% el examen teórico y 30% el práctico, teniendo como condición haber aprobado cada parte de forma separada.
Matrícula de honor
Para obtener la matrícula de honor el alumno debe lograr la máxima calificación en todas las áreas evaluables (teoría, prácticas y actividades de clase). En caso de múltiples candidatos se procederá a un examen oral donde se ponderará el conocimiento del alumno que exceda lo impartido en clase.
Competencias
Durante las actividades de clase se evaluará la competencia G02. El examen teórico incluye la evaluación de las competencias CB5, T02 y CE6-IC. Las prácticas y prueba práctica permitirán valorar también la competencia CE6-IC y la G05.

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	0	0		Tema 1
#2	3	0	0	0	0		Tema 1
#3	1.5	0	0	3	0	Práctica 1	Tema 2
#4	3	0	0	0	0		Tema 2
#5	3	0	0	3	0	Práctica 2	Tema 3
#6	3	0	0	0	0		Tema 3
#7	3	0	0	3	0	Practica 3	Tema 4
#8	3	0	0	0	0		Tema 5
#9	3	0	0	3	0	Práctica 4	Tema 5
#10	3	0	0	0	0		Tema 5
#11	3	0	0	3	0	Práctica 5	Tema 5
#12	3	0	0	0	0		Tema 6
#13	3	0	0	0	0		Tema 6
#14	3	0	0	3.6	0	Recuperación	Todos
#15	0.9	0	0	0	0		Todos
	41.4	0	0	18.6	0		