

GUIA DOCENTE DE LA ASIGNATURA

SEGURIDAD EN SISTEMAS OPERATIVOS**Curso 2016 - 2017***(Fecha última actualización: 13/07/2016)*

MÓDULO	MATERIA	CURS O	SEMEST RE	CRÉDITOS	TIPO
Complementos de Ingeniería del Software	Complementos de programación paralela y sistemas operativos	4º	7º	6	Optativa
PROFESOR(ES)		DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)			
José Antonio Gómez Hernández		José Antonio Gómez Hernández, Despacho 10 (3ª Plta.) http://lsi.ugr.es/lsi/jagomez e-mail: jagomez@ugr.es . Tel.: 958-240-572			
		HORARIO DE TUTORÍAS http://lsi.ugr.es/lsi/jagomez			
GRADO EN EL QUE SE IMPARTE		OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR			
Grado en Ingeniería Informática					
PRERREQUISITOS Y/O RECOMENDACIONES (Si ha lugar)					
No es necesario que los alumnos tengan aprobadas asignaturas, materias o módulos previos como requisito indispensable para cursar este módulo. No obstante se recomienda la superación de los contenidos y adquisición de competencias de las materias de formación básica y de rama.					



ugr | Universidad
de Granada

INFORMACIÓN SOBRE TITULACIONES DE LA UGR
<http://grados.ugr.es>

BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)

Conceptos básicos de seguridad. Modelos de seguridad. Especificación e implementación de políticas de seguridad. Auditoría del sistema operativo. Análisis forense. Ingeniería inversa aplicada a la seguridad.

COMPETENCIAS GENERALES Y ESPECÍFICAS**Competencias Básicas**

CB3. Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

Competencias Generales

E8. Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

Competencias Transversales.

T2. Capacidad para tomar decisiones basadas en criterios objetivos (datos experimentales, científicos o de simulación disponibles) así como capacidad de argumentar y justificar lógicamente dichas decisiones, sabiendo aceptar otros puntos de vista.



OBJETIVOS (EXPRESADOS COMO RESULTADOS DE APRENDIZAJE)

- Caracterizar diferentes modelos de seguridad relacionados con el control de acceso en el sistema operativo.
- Identificar diferentes arquitecturas de seguridad de los sistemas operativos actuales.
- Identificar cómo el sistema operativo controla los objetos que él gestiona.
- Entender la importancia de definir una política de seguridad dentro del sistema y expresarla en un lenguaje de seguridad.
- Conocer los mecanismos del lenguaje de política de seguridad que permiten seguridad multinivel y seguridad condicional.
- Poder escribir módulos de política de seguridad para un sistema.
- Conocer los procesos y herramientas necesarias para identificar los problemas de seguridad que puede provocar un programa.
- Identificar la importancia del análisis forense en el contexto actual.
- Identificar las técnicas utilizadas para recolectar, analizar y presentar evidencias.
- Identificar los pasos necesarios para la construcción de software seguro.
- Identificar los usos de la ingeniería inversa desde el punto de vista de la seguridad del sistema con objeto de poder detener posible ataques.



TEMARIO DETALLADO DE LA ASIGNATURA

TEMARIO DE TEORÍA**Tema 1. Introducción a la seguridad**

- 1.1. Principios de seguridad y protección.
- 1.2. Vulnerabilidades, ataques y contramedidas.
- 1.3. Aspectos éticos y legales. Ethical Hacking.

Tema 2. Sistemas operativos seguros

- 2.1. Propiedades.
- 2.2. Autenticación, autorización y control de acceso.
- 2.3. Sistemas operativos confiables.
- 2.4. Garantía de la seguridad.

Tema 3. Desarrollo de sistemas seguro

- 3.1. Programas inseguros y programas maliciosos (malware).
- 3.2. Análisis de malware
- 3.2. Endurecimiento del sistema (System Hardening).
- 3.2. Construcción de sistemas seguros.

Tema 4. Hacking ético, auditoría informática y análisis forense de computadores

- 4.1. Fundamentos de hacking ético, auditoría informática y análisis forense.
- 4.2. Herramientas para el hacking ético y la informática forense.
- 4.3. Técnicas anti-forenses.

TEMARIO DE PRÁCTICAS

Práctica 1: Administración de la seguridad del sistema.

Práctica 2: Ingeniería inversa y vulnerabilidades.

Práctica 3: Auditoría informática y análisis forense.

SEMINARIOS

Seminario práctico 1: Seguridad en sistemas operativos de producción.

Seminario práctico 2: Estudio de amenazas y ataques.

Seminario práctico 3: Integración de seguridad e ingeniería de sistemas.

BIBLIOGRAFÍA**BIBLIOGRAFÍA FUNDAMENTAL:**

- Willian Stallings y Lawrie Brown, *Computer Security. Principles and Practice, 2nd Edition*, Pearson, 2012.
- Allen Harper et al., *Gray Hat Hacking, 3th Edition*, McGraw Hill, 2011.
- Charles P. Pfleeger y Shari Lawrence Pfleeger, *Analyzing Computer Security. A Threat/Vulnerability/Countermeasure Approach*, Prentice Hall, 2012.
- T. Jaeger y R. Sandhu, *Operating Systems Security*, Morgan & Claypool Publishers, 2008.
- M.E. Withman, H.J. Mattord, *Principles of Information Security, 4th Ed.*, Course Technology, CENGAGE



Learning, 2012.

- R. Anderson, *Security Engineering (2/e)*, Wiley, 2008.
- M. Sikorski y A. Honing, *Practical Malware Analysis*, No Starch Press, 2012
- D. Farmer y R. Sandhu, *Forensic Discovery*, Addison-Wesley, 2005.
- E. Eilam, *Reversing: Secrets of Reverse Engineering*, Wiley, 2005.
- B. Nelson, A. Phillips, I. Efinger, y C. Stewart, *Guide to Computer Forensics and Investigations*, Course Technology, 2007.
- CEH, *Ethical Hacking and Countermeasures Attack Phases*, Course Technology, CENGAGE Learning, 2010.
- J. Andress, *The Basics of Information Security*, Syngress, 2011.
- M. Schumacher et al., *Security Patterns. Integrating Security and Systems Engineering*, John Wiley & Sons, 2006.
- Cengage Learning, *Ethical Hacking and Countermeasures. Attack Phases*, EC-Council Press, 2010.
- Chuck Eastton, *Computer Security Fundamentals*, 2nd Ed, Pearson, 2012.
- E. Perla y M. Oldani, *A Guide to Kernel Exploitation. Attacking the Core*, Syngress, 2011.

BIBLIOGRAFÍA COMPLEMENTARIA:

- M. Bishop, *Introduction to Computer Security*, Prentice Hall, 2004.
- T. Howlett, *Open Source Security Tools. Practical Applications for Security*, Prentice Hall, 2005.
- K. Graves, *CEH: Certified Ethical Hacker Study Guide*, Sybex, Wiley Publishing, 2010.
- T. Bradley y H. Carvey, *Essential Computer Security, Everyons's Guide to e-mail, Internet, and Wireless Security*, Syngress, 2006.
- E. Skoudis y T. Liston, *Counter Hack Reload. A Step-by-step Guide to Computer Attacks and Effective Defense, 2nd Ed.*, Prentice Hall, 2005.
- Z. Smith, W. Barker, y C. Edge, *Foundations of Mac OS X Leopard Security*, Apress 2008.
- D. A. Wheeler, *Secure Programming for Linux and Unix HOWTO*, 2004. Disponible en <http://dwheeler.com/secure.programms/>.
- F. Meyer, K. McMillan y D. Caplan, *SELinux by Example: Using Security Enhanced Linux*, Prentice Hall, 2006.
- D. Shackelford, *Virtualization Security*, John Wiley & Sons, 2013.
- A. Jaquith, *Security Metrics. Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, 2007.
- Neil Daswani, Christoh Kern y Anita Kesavan, *Foundations of Security. What Every Programmer Needs to Know*, Apress, 2007.
- C. Pfleeger, *Security in Computing, 4th Ed*, Prentice Hall, 2006.

ENLACES RECOMENDADOS

El material de la asignatura, tanto para teoría como prácticas, estará disponible en la plataforma <http://prado.ugr.es/moodle/>. La página web departamental <http://lsi.ugr.es/lsi/node/941> también contiene información sobre la asignatura.



METODOLOGÍA DOCENTE

1. Lección magistral (Clases teóricas-expositivas) (grupo grande)

Descripción: Presentación en el aula de los conceptos propios de la materia haciendo uso de metodología expositiva con lecciones magistrales participativas y medios audiovisuales. Evaluación y examen de las capacidades adquiridas.

Propósito: Transmitir los contenidos de la materia motivando al alumnado a la reflexión, facilitándole el descubrimiento de las relaciones entre diversos conceptos y formándole una mentalidad crítica

Contenido en ECTS: 30 horas presenciales (1.2 ECTS)

Competencias: CB1, CB3, E8, T2.

2. Actividades prácticas (Clases prácticas de laboratorio) (grupo pequeño)

Descripción: Actividades a través de las cuales se pretende mostrar al alumnado cómo debe actuar a partir de la aplicación de los conocimientos adquiridos

Propósito: Desarrollo en el alumnado de las habilidades instrumentales de la materia.

Contenido en ECTS: 15 horas presenciales (0.6 ECTS)

Competencias: CB1, CB3, E8, T2.

3. Seminarios (a elegir entre grupo grande/grupo pequeño)

Descripción: Modalidad organizativa de los procesos de enseñanza y aprendizaje donde tratar en profundidad una temática relacionada con la materia. Incorpora actividades basadas en la indagación, el debate, la reflexión y el intercambio.

Propósito: Desarrollo en el alumnado de las competencias cognitivas y procedimentales de la materia.

Contenido en ECTS: 10 horas presenciales (0.4 ECTS)

Competencias: CB1, CB3, E8, T2.

4. Actividades no presenciales individuales (Estudio y trabajo autónomo)

Descripción: 1) Actividades (guiadas y no guiadas) propuestas por el profesor a través de las cuales y de forma individual se profundiza en aspectos concretos de la materia posibilitando al estudiante avanzar en la adquisición de determinados conocimientos y procedimientos de la materia, 2) Estudio individualizado de los contenidos de la materia 3) Actividades evaluativas (informes, exámenes, ...)

Propósito: Favorecer en el estudiante la capacidad para autorregular su aprendizaje, planificándolo, diseñándolo, evaluándolo y adecuándolo a sus especiales condiciones e intereses.

Contenido en ECTS: 45 horas no presenciales (1.8 ECTS)

Competencias: CB1, CB3, E8, T2.

5. Actividades no presenciales grupales (Estudio y trabajo en grupo)

Descripción: Actividades (guiadas y no guiadas) propuestas por el profesor a través de las cuales y de forma grupal se profundiza en aspectos concretos de la materia posibilitando a los estudiantes avanzar en la adquisición de determinados conocimientos y procedimientos de la materia.

Propósito: Favorecer en los estudiantes la generación e intercambio de ideas, la identificación y análisis de diferentes puntos de vista sobre una temática, la generalización o transferencia de conocimiento y la valoración crítica del mismo.

Contenido en ECTS: 45 horas no presenciales (1.8 ECTS)

Competencias: CB1, CB3, E8, T2.

6. Tutorías académicas (a elegir entre grupo grande/grupo pequeño)

Descripción: manera de organizar los procesos de enseñanza y aprendizaje que se basa en la interacción directa entre el estudiante y el profesor

Propósito: 1) Orientan el trabajo autónomo y grupal del alumnado, 2) profundizar en distintos aspectos de la materia y 3) orientar la formación académica-integral del estudiante

Contenido en ECTS: 5 horas presenciales, grupales e individuales (0.2 ECTS)

Competencias: CB1, CB3, E8, T2.



EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

Se utilizarán las siguientes técnicas de evaluación:

- Para la parte teórica, cuya ponderación global será del 40%, se realizarán (a) pruebas objetivas individuales (que supondrán el 20% de la calificación de este bloque), y (b) un trabajo en grupo (20%) sobre la disciplina que se evaluará mediante rúbrica. La calificación del trabajo será realizada por el profesor (heteroevaluación) y al menos (dependiendo de los alumnos matriculados) dos compañeros(co-evaluación) y se obtendrá la media de las tres calificaciones.

- Para la parte práctica, se realizarán prácticas de laboratorio utilizando los correspondientes guiones que incluyen actividades a realizar por el alumno y de las que será necesario entregar un informe/memoria individual al final de cada sesión. Estas actividades serán evaluadas al final del cuatrimestre mediante la defensa de practicas, (mediante entrevista personal del profesor o con cuestionario) donde se preguntará sobre el trabajo realizado en dos o tres de las prácticas propuestas. La ponderación de este bloque será del 40%.

- En su caso, la parte de trabajo autónomo y los seminarios se evaluarán teniendo en cuenta la asistencia a los seminarios, los problemas propuestos que hayan sido resueltos y entregados por los alumnos, y la presentación oral de los trabajos desarrollados. La ponderación de estos será del 20%.

La asistencia tanto a clases teóricas como de prácticas no será obligatoria, si bien se considera que el alumno sigue evaluación continuada si realiza al menos un 80% de las actividades totales propuestas en la Asignatura.

La calificación global corresponderá por tanto a la suma de los diferentes elementos citados y actividades que integran el sistema de evaluación. Por tanto, el resultado de la evaluación será una calificación numérica obtenida mediante la suma de las calificaciones correspondientes a una parte teórica y una parte práctica, con la ponderación anteriormente indicada.

Para aprobar la asignatura es necesario una calificación numérica igual o superior a 5 (sobre 10). Además, se establece el requisito adicional de que tanto la calificación de teoría como las de prácticas deben de ser mayores o iguales a 4 (sobre 10).

La evaluación final única, y la evaluación de convocatorias extraordinarias, constará de un examen de teoría y prácticas. Para la parte teórica constará de preguntas, ejercicios y/o problemas similares a los planteados en evaluación continua. Para la parte práctica, se propondrán supuestos prácticas de la misma complejidad que los realizados en las sesiones presenciales. Los pesos de las partes serán idénticos a los anteriormente descritos.

Todo lo relativo a la evaluación se regirá por la normativa sobre planificación docente y organización de exámenes vigente (disponible en <http://secretariageneral.ugr.es/pages/normativa/fichasugr/ncg7121?lang=en>) en la Universidad de Granada.

El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el art. 5 del R. D 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en el territorio nacional.

INFORMACIÓN ADICIONAL

Definición de grupo grande y grupo pequeño:

Los grupos grandes son grupos de 45 a 60 estudiantes.

Los grupos pequeños son grupos de 15 a 20 estudiantes.

