

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Complementos de Ingeniería del Software	Complementos de programación paralela y sistemas operativos	4º	7º	6	Optativa
PROFESORES			DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)		
<ul style="list-style-type: none"> José Antonio Gómez Hernández: Grupos únicos de Teoría y Prácticas 			Dpto. Lenguajes y Sistemas Informáticos, E.T.S. de Ingenierías Informática y de Telecomunicación. Despacho nº 10, 3ª Planta Correo electrónico: jagomez@ugr.es Tfno: 958 240 572		
COORDINADOR DE LA ASIGNATURA:			ENLACE A LA PÁGINA WEB DONDE PUEDAN CONSULTARSE LOS HORARIOS DE TUTORÍAS*		
<ul style="list-style-type: none"> José Antonio Gómez Hernández 			https://lsi.ugr.es/lsi/jagomez		
GRADO EN EL QUE SE IMPARTE			OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR		
Grado en Ingeniería Informática			Cumplimentar con el texto correspondiente, si procede		
PRERREQUISITOS Y/O RECOMENDACIONES (si procede)					
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.					
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 ESPERABLES DE LA ENSEÑANZA)

- O1: Caracterizar diferentes modelos de seguridad relacionados con el control de acceso en el sistema operativo.
- O2: Identificar diferentes arquitecturas de seguridad de los sistemas operativos actuales.
- O3: Identificar cómo el sistema operativo controla los objetos que él gestiona.
- O4: Entender la importancia de definir una política de seguridad dentro del sistema y expresarla en un lenguaje de seguridad.
- O5: Conocer los mecanismos del lenguaje de política de seguridad que permiten seguridad multinivel y seguridad condicional.
- O6: Poder escribir módulos de política de seguridad para un sistema.
- O7: Conocer los procesos y herramientas necesarias para identificar los problemas de seguridad que puede provocar un programa.
- O8: Identificar la importancia del análisis forense en el contexto actual.
- O9: Identificar las técnicas utilizadas para recolectar, analizar y presentar evidencias.
- O10: Identificar los pasos necesarios para la construcción de software seguro.
- O11: 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 TEÓRICO:

- **Tema 1.** Introducción a la seguridad
 - 1.1. Principios de seguridad y protección.
 - 1.2. Vulnerabilidades, ataques y contramedidas.
 - 1.3. Aspectos legales y éticos. *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*
- 3.3. Fortalecimiento del sistema (*System Hardening*).
- 3.4. Construcción de sistemas seguros.
- **Tema 4. Hacking ético y análisis forense de computadores**
 - 4.1. Fundamentos y herramientas de *hacking* ético.
 - 4.2. Conceptos y herramientas de Informática Forense.
 - 4.3. Técnicas anti-forenses.

TEMARIO PRÁCTICO:

Prácticas de Laboratorio: cada prácticas cuenta con una o varias sesiones semanales donde se abordan diferentes aspectos de la seguridad.

- **Práctica 1:** Administración de la seguridad del sistema: privilegios y permisos, fortalecimiento del sistemas, análisis de vulnerabilidades, anti-rootkits, controles de acceso obligatorios, cifrado y esteganografía.
- **Práctica 2:** Ingeniería inversa y vulnerabilidades: formato de ejecutables, mecanismos de protección y ataques.
- **Práctica 3:** Análisis digital forense: adquisición de evidencias de discos y memoria RAM, análisis forense de las mismas.

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 <https://prado.ugr.es/>. La página web departamental <https://lsi.ugr.es/lsi/node/941> también contiene información sobre la asignatura.

METODOLOGÍA DOCENTE

Para alcanzar las competencias establecidas se realizan diferentes actividades en las que se emplea la metodología que mejor se adapta según el caso y la materia:

- **Lección magistral** (Clases teóricas-expositivas)

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. La asistencia no es obligatoria salvo para las actividades que así lo requieran: pruebas objetivas y presentación de trabajos grupales.

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.

Metodologías empleadas: Lección magistral y resolución de problemas.

- **Actividades prácticas** (Clases prácticas de laboratorio)

Descripción: Actividades propuestas en los guiones de prácticas a través de las cuales se pretende mostrar al alumnado cómo debe actuar a partir de la aplicación de los conocimientos adquiridos tanto en clase de teoría como en la propia descripción de los guiones de prácticas. La asistencia no es obligatoria salvo las actividades que si lo requieren: defensa de prácticas.

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.

Metodologías empleadas: Resolución de problemas y aula de informática.



- **Seminarios** (grupos reducidos)

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, que culmina con la presentación y debate sobre trabajos realizados.

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.

Metodologías empleadas: Desarrollo de proyectos, taller de programación, demos y exposición de trabajos tutelados.

- **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.

Metodologías empleadas: Aula de informática, prácticas de laboratorio, y tutorías académicas.

- **Actividades no presenciales grupales** (Estudio y trabajo en grupo)

Descripción: Actividades (guiadas y no guiadas) bien propuestas por el profesor o elegidas por el estudiante, 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.

Metodologías empleadas: Desarrollo de proyectos y tutorías académicas.

- **Tutorías académicas** (tanto individuales como por grupos de trabajo)

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.)

- **Convocatoria ordinaria**

En la convocatoria ordinaria se utilizará la evaluación continua. Para la misma se utilizarán las técnicas, todas ellas obligatorias, de evaluación y ponderaciones respecto a la calificación final que se indican a continuación:

- *Teoría* - tiene un ponderación total será del 20%, y consta de 2 pruebas objetivas individuales, cada una de las cuales supondrá el 10% de la calificación de este bloque. Se realizará una prueba cada dos temas y constará de varias preguntas cortas y/o ejercicios sobre los contenidos de temas en estudio. Es necesario obtener al menos un 40% de la calificación del bloque para que sea considerada en la suma final.
- *Prácticas* - se realizarán en el laboratorio utilizando los Guiones de Prácticas (un guion por semana y sesión) elaborados a tal fin y que incluyen los contenidos a abordar y las actividades a realizar por el alumno. Para mejor programación del trabajo del estudiante, las soluciones de las actividades propuestas en cada sesión deben ser entregadas con formato de informe/memoria individual de prácticas (conteniendo las evidencias de haber entendido y realizado los supuestos prácticos) en el plazo establecido al inicio de la misma (si bien el plazo puede modificarse).. Estas actividades serán evaluadas globalmente al final del cuatrimestre mediante dado que el estudiante puede conocer por si mismo si están correctamente resueltas. Los elementos que se valora para la calificación final de prácticas son:
 - a) La *defensa de practicas* – se realiza mediante entrevista personal con el estudiantes o con cuestionario escrito, que se realiza la última semana lectiva, donde se preguntará sobre el trabajo realizado en una actividad de una sesión de cada una de las tres prácticas que previamente ha debido resolver. Se realiza en el laboratorio con ordenador por lo que es posible probar o completar la respuesta a las actividades previamente resueltas en los informes de cada sesión. Se valorará la calidad, claridad y completitud de las soluciones dadas. Esta defensa se pondera con un 30% de la calificación global, y es necesario obtener al menos un 50% de la calificación para sumar las otras partes.
 - b) Los *informes/memorias de prácticas* se entregaran tras cada sesión de prácticas en la fecha establecida al publicar la sesión. Se evalúan globalmente y se valoran con un 10% la calificación. En los mismos se valorará la calidad, claridad y completitud de las soluciones dadas así como los detalles de como se ha resuelto. Para superar las prácticas es necesario entregar la memorias de al menos un 80% de las sesiones. Se considera superada si al menos se obtiene un 50% de la calificación del bloque.
- *Trabajos grupales* - Consta de los siguientes elementos:
 - (a) Un trabajo escrito en grupo (20% de la calificación global) de carácter técnico y contenidos teórico-prácticos sobre un tema relacionad con la Ciberseguridad y cuyo formato estará disponible en la plataforma docente al inicio de curso. Se evaluará mediante una rúbrica, también publicada en la plataforma docente junto con el formato de trabajo). La calificación del trabajo grupal se reparte en la forma: 50% proviene de la calificación del profesor (hetero-evaluación) y el otro 50% es la media de la calificación dada por varios compañeros (co-evaluación) – el número de compañeros evaluadores y de los grupos dependerá de los alumnos matriculados en el curso. El trabajo deberá entregarse dos semanas antes de la finalización de las clases presenciales.
 - (b) *Presentación* del trabajo grupal - En la última semana, todos los estudiantes que ha realizado trabajo



grupales deberán exponer en clase el trabajo realizado. La valoración de la presentación grupal se realizará mediante rúbrica por parte del profesor (la rúbrica estará disponible en la plataforma docente con la antelación suficiente). La ponderación de la misma será del 20% del global.

Además, se establecen las siguientes consideraciones generales:

- La asistencia tanto a clases teóricas (salvo la presentación de trabajos grupales) como de prácticas no será obligatoria, si bien se considera que el alumno se beneficiará de la misma para alcanzar las competencias propuestas. No obstante, se considera que se sigue el método de evaluación continua si realizan al menos un 80% de las actividades totales propuestas en la Asignatura.
 - Para superar 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 calificación global corresponderá a la suma de los diferentes elementos/actividades citados en los puntos anteriores y 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 partes: teoría, práctica, trabajo y presentación grupal, cada una con la ponderación indicada.
- **Convocatoria extraordinaria y Convocatoria Especial**

Tanto en la Convocatoria Extraordinaria como en la Convocatoria Especial (establecida en en Artículo 21), la forma y condiciones de la evaluación serán las mismas que se establecen para la la Convocatoria Única Final, que se describe en el Apartado que sigue.

Todo lo relativo a la evaluación se regirá por la normativa sobre planificación docente y organización de exámenes vigente en la Universidad de Granada (accesible a través de la dirección web: https://lsi.ugr.es/normativa_examenes)

DESCRIPCIÓN DE LAS PRUEBAS QUE FORMARÁN PARTE DE LA EVALUACIÓN ÚNICA FINAL ESTABLECIDA EN LA “NORMATIVA DE EVALUACIÓN Y DE CALIFICACIÓN DE LOS ESTUDIANTES DE LA UNIVERSIDAD DE GRANADA”

Tanto para la Evaluación Final Única como para las evaluaciones de la convocatoria extraordinaria y la convocatoria especial, la forma de evaluación será idéntica y constará de los siguientes elementos:

- a) *Teoría* – examen final escrito que constará de preguntas cortas y/o ejercicios sobre los temas teóricos de la Asignatura. Su ponderación a la calificación final será del 50%.
- b) *Prácticas* - Se hará una defensa de prácticas que consistirá en tres preguntas, una por cada práctica, varias preguntas sobre las actividades prácticas propuestas en la Guía de prácticas de la Asignatura (similares a las realizadas en la defensa de prácticas de la evaluación continua) y que se realizará en el laboratorio o con su ordenador personal. Para su realización, el estudiante deberá entregar previamente una memoria de prácticas al igual que en la convocatoria ordinaria. La defensa de las prácticas supondrá un 40% de la calificación y la memoria un 10%.

Se mantienen las mismas consideraciones generales que en la convocatoria ordinaria:

- Para superar 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 calificación global corresponderá a la suma de las calificaciones obtenidas en teoría y prácticas. Por tanto, el resultado de la evaluación será una calificación numérica obtenida mediante la suma de las calificaciones correspondientes a teoría y práctica.



INFORMACIÓN ADICIONAL



**UNIVERSIDAD
DE GRANADA**

INFORMACIÓN SOBRE TITULACIONES DE LA UGR
grados.ugr.es