



SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Guía de Aprendizaje – Información para los Estudiantes

1. Datos Descriptivos

Asignatura	SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
Materia	SISTEMAS OPERATIVOS, SISTEMAS DISTRIBUIDOS Y REDES
Departamento responsable	LENGUAJES Y SISTEMAS INFORMÁTICOS E INGENIERÍA DEL SOFTWARE
Créditos ECTS	6,00
Carácter	OBLIGATORIA
Titulación	GRADUADO EN INGENIERÍA INFORMÁTICA
Curso	TERCER CURSO
Especialidad	NO APLICA

Año Académico	2010/2011
Semestre en que se imparte	Ambos
Semestre principal	1 ^{er} Semestre
Idioma en que se imparte	Español
Página Web	http://porsche.ls.fi.upm.es



2. Profesorado

NAME and SURNAME	DESPACHO	Correo electrónico
Jorge Dávila Muro (Coord.)	5.205	jdavila@fi.upm.es
José Luis Morant Ramón	5.203	jlmorant@fi.upm.es
M ^a del Socorro Bernardos Galindo	5.206	sbernardos@fi.upm.es

3. Conocimientos previos requeridos para poder seguir con normalidad la asignatura

Asignaturas superadas	No se precisa superar asignatura alguna.
Otros resultados de aprendizaje necesarios	No se precisan otros resultados previos de aprendizaje.



4. Objetivos del Aprendizaje

Competencias Asignadas a la Asignatura y su Nivel de Adquisición		
Código	Competencia	Nivel
CE-6	Comprender intelectualmente el papel central que tienen los algoritmos y las estructuras de datos, así como una apreciación del mismo.	2
CE-8	Poseer destrezas fundamentales de la programación que permitan la Implementación de los algoritmos y las estructuras de datos en el software.	3
CE-22	Capacidad de aplicar sus conocimientos e intuición para diseñar el hardware/software que cumple unos requisitos especificados.	1
CE-26/27	Definir, evaluar y seleccionar plataformas hardware y software, incluyendo el sistema operativo, y concebir, llevar a cabo, instalar y mantener arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes.	2
CE-29	Diseñar, desarrollar, y evaluar la seguridad de los sistemas, aplicaciones, servicios informáticos y sistemas operativos sobre los que se ejecutan, así como de la información que proporcionan.	3
CE-31	Desarrollar, desplegar, organizar y gestionar servicios informáticos en contextos empresariales para mejorar sus procesos de negocio.	2
CE-48	Gestionar sistemas y servicios informáticos en contextos empresariales o institucionales para mejorar sus procesos de negocio.	2
CG1/21	Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.	2
CG-19	Capacidad para usar las tecnologías de la información y la comunicación.	3

LEYENDA: Nivel de competencia: conocimiento (1), comprensión (2), aplicación (3) y análisis y síntesis (4)



Resultados del Aprendizaje de la Asignatura			
Código	Resultado del Aprendizaje	Competencias Asociadas	Nivel de Adquisición
RA1	Conocer y comprender la importancia de la seguridad para la empresa.	CE22,CE26/27, CE31, CE48	
RA2	Identificar riesgos y posibles ataques	CE6, CE22, CG19	
RA3	Conocer, comprender y saber utilizar servicios criptográficos para la obtención de seguridad.	CE8, CE29, CE31,GC1/21	
RA4	Conocimiento actualizado de soluciones de seguridad para la Sociedad de la Sociedad de la Información	CE22, CE31, CE48	

5. Sistema de Evaluación de la Asignatura

Indicadores del Logro		
Ref	Indicador	Relacionado con RA
I1	Conocimiento de la legislación y normativa nacional esencial que afecta a la seguridad de los sistemas de información.	RA1
I2	Conocer, en su esencia, los riesgos actuales en los sistemas de información empresarial.	RA1, RS2
I3	Conocimiento de los servicios y primitivas criptográfica útiles para la protección de sistemas de información.	R3
I4	Familiaridad con sistemas y aplicaciones de seguridad actuales	R4, R3



EVALUACIÓN INCREMENTAL			
Breve descripción de las actividades evaluables	Momento	Lugar	Peso en la Calif.
Ejercicio I de Evaluación de conocimientos	07/10/2010	Aula	13 %
Ejercicio II de Evaluación de conocimientos	30/11/2010	Aula	17 %
Ejercicio III de Evaluación de conocimientos	21/12/2010	Aula	10 %
Entrega y Evaluación de los Ejercicios Individuales	20/12/2010	Entrega telemática	30 %
Entrega y Evaluación del Ejercicio Práctico	21/12/2010	Entrega Telemática	30 %
			Total: 100%

Criterios de Evaluación

La evaluación de esta asignatura está compuesta por tres elementos:

1. **Ejercicio de Evaluación de Concomimiento:** Será uno o varios ejercicios escritos en los que habrá que responder a una serie de preguntas relacionadas con los temas y conocimientos tratados en las clases de teoría.
2. **Ejercicio Individual Obligatorio:** Será un ejercicio escrito en el que el alumno plasmará los resultados de la actividad indicada por el enunciado del ejercicio (lectura y análisis de artículos científicos y técnicos, indagaciones sobre el estado del arte, realización de pequeños estudios y/o aplicaciones informáticas, etc.) y su entrega se hará mediante procedimientos telemáticos.
3. **Ejercicio práctico:** Consistirá en estudiar, analizar y en muchas ocasiones implementar, una solución relacionada con la seguridad de un sistema de información en un escenario dado. Este trabajo es eminentemente práctico pero requiere adquirir la comprensión y conocimiento básico del escenario que se plantea y su entrega se hará mediante procedimientos telemáticos.

Sistema General de Evaluación Continua

El Sistema de Evaluación Continua es el que se aplica, con carácter general y por defecto u omisión, a todos los estudiantes que cursen esta asignatura.

En esta asignatura no se guardan resultados o logros para otras convocatorias o cursos. La asistencia a clase sólo es obligatoria en las pruebas presenciales de evaluación



que se celebrará a lo largo de las clases de la asignatura.

La realización y entrega de resultados del Ejercicio Individual Obligatorio y del Ejercicio Práctico serán las marcadas para ello en el Cronograma de la Asignatura. El peso de la evaluación de estos dos ejercicios será de un 30% de la calificación final para cada uno de ellos.

Los alumnos que no hayan optado por este sistema de evaluación realizarán tres pruebas como partes del Ejercicio de Evaluación del Conocimiento que se realizarán en las fechas y lugares establecidos para ello en el Cronograma de la Asignatura. En estas pruebas se irán evaluando los logros del alumno en la comprensión y asimilación de las materias presentadas a lo largo de las clases de teoría y como resultado de su trabajo personal. El peso de éste conjunto de pruebas de evaluación será de un 40% de la calificación final.

Sistema de Evaluación mediante sólo Prueba Final

El Sistema de evaluación mediante sólo prueba final sólo se ofrecerá si así lo exige la Normativa Reguladora de los Sistemas de Evaluación en la UPM que esté vigente en el curso académico 2010-2011, y el procedimiento para optar por este sistema estará sujeto a lo que establezca en su caso Jefatura de Estudios de conformidad con lo que estipule dicha Normativa.

En esta asignatura no se guardan resultados o logros para otras convocatorias o cursos. La asistencia a clase sólo es obligatoria en la prueba presencial de evaluación que se celebrará al finalizar las clases de la asignatura.

La realización y entrega de resultados del Ejercicio Individual Obligatorio y del Ejercicio Práctico será en las mismas fechas y mediante los mismos procedimientos que los establecidos para el método de evaluación continua. El peso de la evaluación de estos dos ejercicios será de un 30% de la calificación final para cada uno de ellos.

Los alumnos que no hayan optado por este sistema de evaluación deberán presentarse al Ejercicio de Evaluación Final que se realizará en la fecha y lugar establecidos para ello por Jefatura de Estudios, y que evaluará los logros del alumno en la comprensión y asimilación de las materias presentadas en las clases de teoría. El peso de este ejercicio de evaluación será de un 40% de la calificación final.

Evaluación en el periodo extraordinario

Los criterios de evaluación para este sistema son los mismos que para el sistema de "sólo prueba final" y, como en ese caso, no se guardan resultados o logros para otras convocatorias o cursos.

6. Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS



Bloque	Apartado	Indicadores Relacionados
Bloque I	Introducción y conceptos generales	I1, I2, I3
	Auditoría, Análisis de Riesgos y Planes de Contingencia	I1, I2
	Seguridad de las instalaciones	I2, I4
	Legislación y Estándares	I1
Bloque II	Desarrollo de códigos seguros	I2
	Códigos Maliciosos y Ataques	I2
	Operaciones y Sistemas de Defensa	I3, I4
Bloque III	Servicios criptográficos	I3
	Confidencialidad y Claves	I2, I3
	Integridad y Autenticación	I3
	Identidad, Identidad Digital y Firma Digital	I1, I3, I4
Bloque IV	Control de accesos	I3, I4
	Aplicaciones de seguridad	I4

7. Breve Descripción de las Modalidades Organizativas y los Métodos de Enseñanza

Organización de la Enseñanza		
Escenario	Modalidad Organizativa	Propósito
	Clases de Teoría	Hablar a los estudiantes para facilitar la información a los alumnos, promover la comprensión de conocimientos y estimular su motivación. Se trata de sesiones expositivas, explicativas y/o demostrativas de contenidos (las presentaciones pueden ser tanto del profesor como del alumno)
	Seminarios o Talleres	Construir conocimientos a través de la interacción y la actividad para trabajar con profundidad un aspecto o tema específico, a través de la interacción personal. Según los contenidos a desarrollar pueden adoptar distintas modalidades: la modalidad de Seminario es la más indicada cuando la actividad se centra en debatir, reflexionar e intercambiar puntos de vista, conocimientos; mientras que el Taller es la modalidad más indicada para la adquisición específica de habilidades procedimentales. Sesiones monográficas supervisadas con participación compartida (profesorado, estudiantes, expertos, ...)
	Clases Prácticas	Mostrar cómo se debe actuar y guiar al alumno en la aplicación de los conocimientos adquiridos. Es el contexto más adecuado para desarrollar las competencias relacionadas con el ejercicio de una profesión (estudio de casos, análisis diagnósticos, problemas, laboratorio, de campo, aula informática. Visitas, búsqueda de datos, bibliotecas, en red, internet,...)
	Prácticas Externas	Lograr aprendizajes profesionales en un contexto laboral. La finalidad de esta modalidad es que el alumno desarrolle actividades en un entorno relacionado con el ejercicio de su profesión. Dentro de esta modalidad podemos diferenciar entre: el <i>practicum</i> (puede formar parte o no del plan de estudios como una materia específica); las prácticas en empresa (desarrolladas por los egresados de una titulación); y prácticas clínicas (vinculadas a las Ciencias de la Salud). La formación realizada en empresas y entidades externas a la universidad (prácticas asistenciales,...)
	Tutorías Personales	Atención personalizada a los estudiantes. Se pueden diferenciar tres tipos de tutorías: Tutoría Docente centrada en apoyar al alumno en el aprendizaje de la asignatura, en facilitar la adquisición de técnicas y estrategias para el trabajo autónomo, favorecer el trabajo autónomo, detectar la falta de conocimiento y habilidades; la Tutoría de Seguimiento que se centra en apoyar al alumno en la toma de decisiones y en la orientación en el estudio; y la Tutoría de Orientación Laboral dirigida a apoyar al alumno en la orientación y toma de decisiones vinculadas con su inserción laboral una vez graduado. Relación personal de ayuda, donde un profesor – tutor atiende, facilita y orienta a uno o varios estudiantes en el proceso formativo
	Estudio y Trabajo en Grupo	Hacer que aprendan entre ellos. Modalidad de aprendizaje en donde los estudiantes aprenden unos de otros, del profesor y del entorno. Preparación de seminarios, lecturas, investigaciones, trabajos, memorias, obtención y análisis de datos, etc., para exponer o entregar en clase mediante el trabajo de los estudiantes en grupo
	Trabajo Independiente	Desarrollar la capacidad autodidacta. Modalidad de aprendizaje en donde el alumno deberá desarrollar su capacidad de planificación, desarrollo y evaluación de actividades de aprendizaje. Se trata de las mismas actividades que las descritas en “estudio y trabajo en grupo” pero realizadas de forma individual. Incluye, además, el estudio personal (preparación de exámenes, trabajo en biblioteca, lecturas complementarias, hacer problemas, ejercicios,...) que es fundamental en el aprendizaje autodidacta.



Breve Descripción de las modalidades organizativas y Métodos de Enseñanza.	
Clases de Teoría	Durante una clase de teoría o lección magistral, el profesor realiza una exposición verbal de los contenidos sobre la materia objeto de estudio, mediante la cual suministra a los alumnos información esencial y organizada procedente de diversas fuentes con unos objetivos específicos predefinidos: motivar al alumno, exponer contenidos sobre un tema, explicar conocimientos, presentar experiencias, etc., pudiendo utilizar para ello, además de la exposición oral, otros recursos didácticos (audiovisuales, documentos, etc.).
Ejercicios Individuales	<p>Este método de enseñanza es un complemento de la clase de teoría y consiste en solicitar a los estudiantes encuentren las soluciones adecuadas o correctas a un problema planteado. La solución se alcanzará ejercitando rutinas o mediante la aplicación de fórmulas o algoritmos, y siempre requerirá la interpretación de los resultados.</p> <p>La intención principal de esta actividad es la de aplicar lo ya aprendido, favorecer la comprensión tanto de la importancia como del contenido de un nuevo tema, afianzar conocimientos y estrategias y su aplicación en las situaciones prácticas que se planteen.</p>
Ejercicio Práctico	El alumno trabaja individualmente o en grupos muy reducidos (2-3 estudiantes) en la implementación, aplicación y análisis de un algoritmo criptográfico, de una primitiva de seguridad, o de todo un sistema o servicio de seguridad.
Tutorías Personales	Los alumnos podrán consultar al profesor las dudas que se les planteen, dentro de las horas de tutorías que se marquen para tal efecto.



8. Recursos Didácticos

Recursos Didácticos	
Lecturas Recomendadas	Applied Cryptography. Protocols, Algorithms, and Source Code in C, 2nd Edition , Bruce Schneier (Author) ISBN-10: 0471117099 ISBN-13: 978-0471117094
	Practical Cryptography , Niels Ferguson (Author), Bruce Schneier (Author) ISBN-10: 0471223573 ISBN-13: 978-0471223573
	Handbook of Applied Cryptography. Discrete Mathematics and Its Applications , Alfred Menezes, Paul van Oorschot y Scott Vanstone (Editores) ISBN-10: 0849385237 ISBN-13: 978-0849385230
	Cryptography and Network Security. Principles and Practice, 5th Edition , William Stallings (Author) ISBN-10: 0136097049 ISBN-13: 978-0136097044
	Cryptography for Developers , Tom St Denis (Author) ISBN-10: 1597491047 ISBN-13: 978-1597491044
	BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic . Tom St Denis (Author) ISBN-10: 1597491128 ISBN-13: 978-1597491129
	Codes, Ciphers, Secrets and Cryptic Communication. Making and Breaking Secret Messages from Hieroglyphs to the Internet , Fred B. Wrixon (Author) ISBN-10: 1579124852 ISBN-13: 978-1579124854
	The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography , Simon Singh (Author) ISBN-10: 0385495323 ISBN-13: 978-0385495325
	The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet , David Kahn (Author) ISBN-10: 0684831309 ISBN-13: 978-0684831305
	Security in Computing (4 ^a ed.), Charles P. Pfleeger y Shari Lawrence Pfleeger. Prentice Hall (2006) ISBN-10: 0132390779, ISBN-13: 978-0132390774
	Network Security: Private Communication in a Public World (2 ^a ed). Charlie Kaufman, Radia Perlman y Mike Speciner. Prentice Hall (2002) ISBN-10: 0130460192, ISBN-13: 978-0130460196
	Computer Security Basics (2 ^a ed.) Rick Lehtinen y G.T. Gangemi. O'Reilly Media, Inc. (2006) ISBN-10: 0596006691, ISBN-13: 978-0596006693
	Computer Security (2 ^a ed.). Dieter Gollmann. Wiley (2006) ISBN-10: 0470862939, ISBN-13: 978-0470862933
Introduction to Computer Security . Matt Bishop. Addison-Wesley Professional (November 5, 2004) ISBN-10: 0321247442, ISBN-13: 978-0321247445	
Fundamentals Of Computer Security , Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry ISBN: 3540431012, ISBN-13: 9783540431015, 978-3540431015. Springer 2003	
Recursos Web	Sitio web de la asignatura http://porsche.ls.fi.upm.es Sitio Moodle de la asignatura http://web3.fi.upm.es/AulaVirtual/
Equipamiento	Aula la asignada por Jefatura de Estudios



9. Programación de la Asignatura

Semana	Actividades en clase	Trabajo Individual	Actividades de Evaluación	Otros
Semanas 1 – 4 (12 horas): Introducción y conceptos generales, Auditoría, Análisis de Riesgos y Planes de Contingencia. Seguridad de las instalaciones. Legislación y Estándares	12	16	0	
Semanas 4 – 6 (25 horas): Desarrollo de códigos seguros. Códigos Maliciosos y Ataques. Operaciones y Sistemas de Defensa.	10	13	2	
Semanas 7 – 14 (28 horas): Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.	28	37	2	
Semanas 15 – 17 (25 horas): Control de Accesos. Aplicaciones de Seguridad.	8	12	2	
Totales:	58	78	6	

Nota: La carga de trabajo del estudiante para cada actividad estará expresada en horas.