Datos Descriptivos

ASIGNATURA:	SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
MATERIA:	SISTEMAS OPERATIVOS, SISTEMAS DISTRIBUIDOS Y REDES
CRÉDITOS EUROPEOS:	6.0
CARÁCTER:	OBLIGATORIA
TITULACIÓN:	GRADUADO EN INGENIERÍA INFORMÁTICA
CURSO/SEMESTRE	TERCER CURSO / QUINTO SEMESTRE
ESPECIALIDAD:	NO APLICA

CURSO ACADÉMICO	2014 / 2015		
PERIODO IMPARTICION	**Septiembre- Enero**	**Febrero - Junio**	
	Si	Si	
IDIOMA IMPARTICIÓN	**Sólo castellano**	**Sólo inglés**	**Ambos**
	Si	No	No

DEPARTAMENTO:	LENGUAJES Y SISTEMAS INFORMÁTICOS E INGENIERÍA DEL SOFTWARE

PROFESORADO		
NOMBRE Y APELLIDO (C = Coordinador)	**DESPACHO**	**Correo electrónico**
Jorge Dávila Muro (C)	5.205	jdavila@fi.upm.es
José Luis Morant Ramón	5.203	jlmorant@fi.upm.es
Mª del Socorro Bernardos Galindo	5.206	sbernardos@fi.upm.es

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.

Objetivos de Aprendizaje

COMPETENCIAS Y NIVEL ASIGNADAS A LA ASIGNATURA		
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

Código	ESULTADOS DE APRENDIZAJE DE LA ASIGNATURA	
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

Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS (TEMARIO)		
TEMA / CAPITULO	**APARTADO**	**Indicadores Relacionados**
Bloque I	Servicios criptográficos	I3
	Confidencialidad y Claves	I2, I3
	Integridad y Autenticación	I3
	Identidad, Identidad Digital y Firma Digital	I1, I3, I4
Bloque II	Desarrollo de códigos seguros	I2
	Códigos Maliciosos y Ataques	I2
	Operaciones y Sistemas de Defensa	I3, I4
Bloque III	Control de accesos	I3, I4
	Aplicaciones de seguridad	I4
Bloque IV	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

BREVE DESCRIPCIÓN DE LAS MODALIDADES ORGANIZATIVAS UTILIZADAS Y METODOS DE ENSEÑANZA EMPLEADOS	
CLASES DE TEORIA	Hablar a los estudiantes para facilitar la información a los alumnos, promover la comprensión de conocimientos y estimular su motivación. Se trata der 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.
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,…)
PRACTICAS 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 *practicum* (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,…)
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.

RECURSOS DIDÁCTICOS	
BIBLIOGRAFÍA	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 (4ª 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 (2ª ed). Charlie Kaufman, Radia Perlman y Mike Speciner. Prentice Hall (2002) ISBN-10: 0130460192, ISBN-13: 978-0130460196
	Computer Security Basics (2ª ed.) Rick Lehtinen y G.T. Gangemi. O'Reilly Media, Inc. (2006) ISBN-10: 0596006691, ISBN-13: 978-0596006693
	Computer Security (2ª 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
EQUIPAMIENTO	Aula la asignada por Jefatura de Estudios

Cronograma de trabajo de la asignatura

Semana	Actividades Aula	Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades Evaluación	Otros
Semanas 1 – 7 (28 horas): Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.	28		35		2	
Semanas 4 – 6 (12 horas): Desarrollo de códigos seguros. Códigos Maliciosos y Ataques. Operaciones y Sistemas de Defensa.	16		19		1	
Semanas 15 – 17 (8 horas): Control de Accesos. Aplicaciones de Seguridad.	8		8		1	
Semanas 1 – 4 (12 horas): Introducción y conceptos generales, Auditoría, Análisis de Riesgos y Planes de Contingencia. Seguridad de las instalaciones. Legislación y Estándares	10		16		2	
Totales:	**62**		**78**		**6**	

Sistema de evaluación de la asignatura

EVALUACION		
Ref	**INDICADOR DE LOGRO**	**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

EVALUACION SUMATIVA			
BREVE DESCRIPCION DE LAS ACTIVIDADES EVALUABLES	**MOMENTO**	**LUGAR**	**PESO EN LA CALIFICACIÓN**
Ej. Evaluación del Bloque I	**20/10/2014**	Aula	23 %
Ej. Evaluación de los Bloques II y III	**01/12/2014**	Aula	19 %
Ej. Evaluación del Bloque IV	**19/12/2014**	Aula	8 %
Entrega y Evaluación del Ejercicio Práctico	**20/10/2014**	**Entrega telemática**	25 %
Entrega y Evaluación de los Ejercicios Individuales.	**12/01/2014**	**Entrega Telemática**	25 %
		Total:	100 %

NORMAS GENERALES PARA EL DESARROLLO DE LA ASIGNATURA

1. La asistencia a clase no es obligatoria, por lo que el comportamiento de los asistentes deberá ser respetuoso con los demás. El alumno deberá colaborar en el adecuado desarrollo de las clases y demás actividades formativas del curso.
2. Por innecesario, se prohíbe el uso de ordenadores, ordenadores portátiles, tabletas, smartphones, teléfonos móviles o cualquier otro artefacto electrónico en general, durante el desarrollo de las clases de teoría. El profesor se reserva el derecho de incluir excepciones puntuales a esta norma para mejor desarrollo de las clases.
3. En el caso de que haya desdoblamiento del curso en varios grupos, éste podrá ser suspendido por acuerdo de los profesores de la asignatura si en cualquiera de ellos la asistencia a clase decae por debajo del 50% procediéndose a la reunión de los grupos poco numerosos, independientemente del horario oficial asignado que ellos tengan.
4. El profesorado de la asignatura se reserva la potestad de dividir o reunir grupos para el desarrollo de temas específicos si el desarrollo del temario y sus actividades asociadas así lo aconsejan.
5. Si el desarrollo de la asignatura así lo requiriese o aconsejase, el profesorado de reserva la potestad de cambiar el orden en el que se exponen y desarrollan los distintos bloques que constituyen el Temario de la asignatura.
6. Para el correcto desarrollo de esta asignatura, todos los alumnos deberán inscribirse como tales en el servidor web de la asignatura y obtener una identidad digital que les permita acceder a la parte privada de dicho web así como a firmar digitalmente mensajes de correo electrónico.
7. Está prohibido el plagio tanto en las memorias, como en los códigos o el software que se desarrolle. En todos los casos el alumno deberá indicar explícitamente y con detalle de dónde han salido y cuál es el origen de los materiales que utiliza.
8. Está prohibida la mera traducción de artículos académicos o de cualquier otra índole. El uso de traductores automáticos está completamente prohibido. Las incorrecciones sintácticas, ortográficas y semánticas del lenguaje utilizado podrán ser penalizadas.
9. Cualquier sospecha sobre la autoría de un examen, un ejercicio individual o una práctica, llevará inexorablemente al **Examen Oral de la asignatura** y parte del cuál será la defensa de lo expuesto en su entrega (examen, memoria, código, ejecutables, etc.).

CRITERIOS DE CALIFICACIÓN

La evaluación de esta asignatura está compuesta por tres elementos:

1. **Ejercicios 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. **Ejercicios Individuales Obligatorios**: Serán uno o varios ejercicios escritos en los que el alumno plasmará los resultados de la actividad indicada en el enunciado de cada 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 para aquellos que quieran participar en las pruebas presenciales de evaluación que se celebrarán a lo largo de las clases de la asignatura.

Los alumnos que hayan optado por este sistema de evaluación realizaran 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 la evaluación de estos exámenes será de un 50% de la calificación final.

La realización y entrega de resultados de los Ejercicios Individuales Obligatorio y del Ejercicio Práctico serán las marcadas para ello en el Cronograma de la Asignatura. El peso de la evaluación de estos dos tipos de ejercicios será de un 25% de la calificación final para cada uno de ellos, sumando entre ambos un 50% de la calificación final.

SISTEMA DE EVALUACIÓN MEDIANTE SÓLO PRUEBA FINAL

En la convocatoria ordinaria, la elección entre el sistema de evaluación continua o el sistema de evaluación mediante sólo prueba final corresponde al estudiante. Quien desee seguir el sistema de evaluación mediante sólo prueba final, deberá comunicarlo al **Coordinador de la Asignatura** o, por delegación de éste, a los profesores de la misma, mediante solicitud por escrito y firmada, dentro de los primeros **Veinte Días Naturales** a contar desde el comienzo efectivo de la asignatura. En dicho escrito deberá constar:

D. _____con DNI_____ y Matrícula _____,

SOLICITA:

Ser evaluado en este semestre mediante el "Sistema de evaluación mediante sólo prueba final" en la asignatura:

SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN,

Titulación _____, Curso 2014-2015

Coordinador de la Asignatura: D. JORGE DÁVILA MURO

Departamento: LENGUAJES Y SISTEMAS INFORMÁTICOS E INGENIERÍA DEL SOFTWARE

Fecha: _ _ /_ _ _ /2014

Firmado:

Esta solicitud sólo se considerará a los efectos del semestre en curso. En posteriores semestres deberá necesariamente ser cursada de nuevo.

No obstante, cuando exista causa sobrevenida y de fuerza mayor que justifique el cambio del proceso de evaluación, el estudiante que haya optado (por omisión) por el sistema de evaluación continua podrá solicitar al Tribunal de la Asignatura ser admitido en los exámenes y actividades de evaluación que configuran el sistema de evaluación mediante sólo prueba final. El tribunal de la asignatura, una vez analizadas las circunstancias que se hagan constar en la solicitud, dará respuesta al estudiante con la mayor antelación a la celebración del examen final que sea posible.

En esta asignatura no se guardan resultados o logros para otras convocatorias o cursos. La asistencia a clase sólo es obligatoria para aquellos que quieran participar en la prueba presencial de evaluación que se celebrarán al final de 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 25% de la calificación final para cada uno de ellos, sumando ambos un 50%.

Los alumnos que 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 50% de la calificación final.

EVALUACIÓN EN EL PERIODO EXTRAORDINARIO

Los alumnos matriculados que no hayan aprobado la asignatura en la convocatoria ordinaria, podrán presentarse a examen en la convocatoria extraordinaria en la fecha y lugar fijado para ello por Jefatura de Estudios.

Ninguno de los ejercicios individuales y práctico asignados en para las convocatorias ordinaria tendrán validez en ninguna convocatoria extraordinaria.

Una vez celebrada la convocatoria ordinaria del segundo semestre del curso, se procederá a reasignar los ejercicios individuales y la práctica a todos los alumnos que puedan presentarse a la convocatoria extraordinaria.

En el caso de que en la reasignación al alumno le volviese a corresponder el mismo ejercicio o práctica que ya le hubiese sido asignado con anterioridad, se le asignará la siguiente práctica o ejercicio en el orden correlativo de la lista. Ningún alumno podrá tener asignado en la convocatoria extraordinaria un trabajo que se la haya podido asignar previamente.

La fecha límite para la entrega de los ejercicios será la del examen extraordinario marcado por Jefatura de Estudios. El mecanismo y procedimiento de entrega de todos los ejercicios que habrán de ser evaluados en la convocatoria extraordinaria será mediante CD adecuadamente identificado con el nombre del alumno, la asignatura, el curso y la convocatoria a la que se presenta, y se entregará en la fecha y hora del examen.