ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

Seguridad de las tecnologias de la informacion

CURSO ACADÉMICO - SEMESTRE

2016-17 - Primer semestre

Datos Descriptivos

Nombre de la Asignatura	Seguridad de las tecnologias de la informacion
Titulación	10II - Grado en Ingenieria Informatica
Centro responsable de la titulación	Escuela Tecnica Superior de Ingenieros Informaticos
Semestre/s de impartición	Quinto semestre Sexto semestre
Materias	Sistemas operativos, sistemas distribuidos y redes
Carácter	Obligatoria
Código UPM	105000030
Nombre en inglés	Information technology security

Datos Generales

Créditos	6	**Curso**	3
Curso Académico	2016-17	**Período de impartición**	Septiembre-Enero
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

El plan de estudios Grado en Ingenieria Informatica no tiene definidas asignaturas previas superadas para esta asignatura.

Otros Requisitos

El plan de estudios Grado en Ingenieria Informatica no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

El coordinador de la asignatura no ha definido asignaturas previas recomendadas.

Otros Conocimientos Previos Recomendados

El coordinador de la asignatura no ha definido otros conocimientos previos recomendados.

Competencias

CG-1/21 - Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.

CG-19 - Capacidad de usar las tecnologías de la información y la comunicación.

Ce 22 - Capacidad de aplicar sus conocimientos e intuición para diseñar el hardware/software que cumple unos requisitos especificados.

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.

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.

Ce 31 - Desarrollar, desplegar, organizar y gestionar servicios informáticos en contextos empresariales para mejorar sus procesos de negocio.

Ce 48 - Gestionar sistemas y servicios informáticos en contextos empresariales o institucionales para mejorar sus procesos de negocio.

Ce 6 - Comprender intelectualmente el papel central que tienen los algoritmos y las estructuras de datos, así como una apreciación del mismo.

Ce 8 - Poseer destrezas fundamentales de la programación que permitan la implementación de los algoritmos y las estructuras de datos en el software.

Resultados de Aprendizaje

RA360 - Conocimiento actualizado de soluciones de seguridad para la Sociedad de la Sociedad de la Información

RA317 - Fundamentos, criptografía y criptoanálisis.

RA506 - Conocer y comprender la importancia de la seguridad para la empresa.

RA358 - Identificar riesgos y posibles ataques

RA359 - Conocer, comprender y saber utilizar servicios criptográficos para la obtención de seguridad.

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Bernardos Galindo, Maria Del Socorro	5206	mariadelsocorro.bernardos@upm.es	M - 08:00 - 11:00 J - 08:00 - 11:00
Morant Ramon, Jose Luis	5203	joseluis.morant@upm.es	L - 11:00 - 14:00 V - 10:00 - 13:00
Davila Muro, Jorge **(Coordinador/a)**	5205	jorge.davila@upm.es	J - 12:00 - 14:00 V - 12:00 - 14:00

Nota.- Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

Descripción de la Asignatura

El objetivo de esta asignatura es hacer comprender el papel central que tienen los algoritmos y las estructuras de datos en la seguridad de los sistemas informáticos. Con ella se pretende que el alumno adquiera destrezas fundamentales para la programación e implementación de algoritmos y sistemas que proporcionen seguridad a las TICs. Para ello el alumno habrá que aplicar conocimientos e intuición en el diseño de soluciones válidas según requisitos de seguridad especificados. El objetivo global es que el alumno pueda llegar a diseñar, desarrollar y evaluar la Seguridad de sistemas, aplicaciones y servicios informáticos de todo tipo. Los conocimientos adquiridos siempre apuntaran al desarrollo, despliegue, organización y gestión de servicios informáticos en contextos empresariales que realmenet puedan mejorar los procesos de negocio.

En esta asignatura se favorecerá la capacidad del alumno en la resolución de problemas de seguridad recurriendo a los conocimientos que sean necesarios (matemáticas, ciencias, ingeniería, etc.). Al final, el alumno conocerá y comprenderá la importancia que tiene la seguridad informática para las Administraciones y Empresas, seran capaces de identificar riesgos y posibles ataques. Para ello conocerá, comprenderá y sabrá utilizar servicios criptográficos para proporcionar seguridad TIC y conocerá algunas soluciones de seguridad que están disponibles y son válidas para la protección de la Sociedad de la Información. Como condicion necesaria, el alumno deberá ser capaz de instalar y utilizar una Identidad Digital mediante certificados X509v3 tanto en Navegación web como para la Firma Electrónica de correos electrónicos.

Temario

1. Servicios criptográficos
2. Confidencialidad y Claves
3. Integridad y Autenticación
4. Identidad, Identidad Digital y Firma Digital
5. Desarrollo de códigos seguros
6. Códigos Maliciosos y Ataques
7. Operaciones y Sistemas de Defensa
8. Control de accesos
9. Aplicaciones de seguridad
10. Normas: Introducción y conceptos generales
11. Auditoría, Análisis de Riesgos y Planes de Contingencia
12. Seguridad de las instalaciones
13. Legislación y Estándares

Cronograma

Horas totales: 162 horas

Horas presenciales: 64 horas (41%)

Peso total de actividades de evaluación continua: 100%

Peso total de actividades de evaluación sólo prueba final: 100%

Semana	Actividad Prensencial en Aula	Actividad Prensencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 2	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 3	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 4	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 5	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 6	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 7	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 8	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Examen** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 9	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Practica individual** Duración: 37:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad no presencial
Semana 10	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 11	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			

Semana 12	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 13	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 14	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Examen** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 15	**Clase de teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Practica individual** Duración: 37:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad no presencial
Semana 16				**Examen** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial **Ejercicios individuales** Duración: 24:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad no presencial
Semana 17				**Practica y Ejercicios Individuales** Duración: 60:00 TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Actividad presencial **Examen teorico de toda la asignatura** Duración: 02:15 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad no presencial

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
8	Examen	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	23%		Ce 6, Ce 26/27, CG-1/21, CG-19
9	Practica individual	37:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	No	25%		Ce 22, Ce 8
14	Examen	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	19%		CG-19
15	Practica individual	37:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	No	12.5%		Ce 29, CG-19, Ce 22, Ce 26/27, Ce 8
16	Examen	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	8%		CG-19, Ce 6, Ce 8, CG-1/21, Ce 22, Ce 26/27, Ce 29, Ce 31, Ce 48
16	Ejercicios individuales	24:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	No	12.5%		Ce 22, Ce 8
17	Practica y Ejercicios Individuales	60:00	Evaluación sólo prueba final	TI: Técnica del tipo Trabajo Individual	Sí	50%		Ce 22, CG-19, Ce 6, Ce 26/27, CG-1/21, Ce 8, Ce 29, Ce 31, Ce 48
17	Examen teorico de toda la asignatura	02:15	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	No	50%		Ce 22, Ce 8

Criterios de Evaluación

Correcta respuesta a las preguntas planteadas a cada alumno, así como correcta satisfacción de los objetivos marcados en prácticas y ejercicios individuales.

Cumplir las normas que se establezcan para la asignacion de tareas así como para la entrega de materiales y resultados.

La copia y el plagio estaran gravemente penados y no se procederá a la evaluacion del material presentado.

La correccion sintactica y semántica en castellano o ingles será tenida en cuenta como absolutamente necesaria.

Recursos Didácticos

Descripción	Tipo	Observaciones
Applied Cryptography. Protocols, Algorithms, and Source Code in C	Bibliografía	2nd Edition, Bruce Schneier (Author) ISBN-10: 0471117099 ISBN-13: 978-0471117094
Practical Cryptography	Bibliografía	Niels Ferguson (Author), Bruce Schneier (Author) ISBN-10: 0471223573 ISBN-13: 978-0471223573
Handbook of Applied Cryptography. Discrete Mathematics and Its Applications	Bibliografía	Alfred Menezes, Paul van Oorschot y Scott Vanstone (Editores) ISBN-10: 0849385237 ISBN-13: 978-0849385230
Cryptography and Network Security. Principles and Practice,	Bibliografía	5th Edition, William Stallings (Author) ISBN-10: 0136097049 ISBN-13: 978-0136097044
Cryptography for Developers,	Bibliografía	Tom St Denis (Author) ISBN-10: 1597491047 ISBN-13: 978-1597491044
BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic.	Bibliografía	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,	Bibliografía	Fred B. Wrixon (Author) ISBN-10: 1579124852 ISBN-13: 978-1579124854
The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography,	Bibliografía	Simon Singh (Author) ISBN-10: 0385495323 ISBN-13: 978-0385495325
The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet,	Bibliografía	David Kahn (Author) ISBN-10: 0684831309 ISBN-13: 978-0684831305
Security in Computing	Bibliografía	(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	Bibliografía	(2ª ed). Charlie Kaufman, Radia Perlman y Mike Speciner. Prentice Hall (2002) ISBN-10: 0130460192, ISBN-13: 978-0130460196
Computer Security Basics	Bibliografía	(2ª ed.) Rick Lehtinen y G.T. Gangemi. O'Reilly Media, Inc. (2006) ISBN-10: 0596006691, ISBN-13: 978-0596006693
Computer Security	Bibliografía	(2ª ed.). Dieter Gollmann. Wiley (2006) ISBN-10: 0470862939, ISBN-13: 978-0470862933
Introduction to Computer Security.	Bibliografía	Matt Bishop. Addison-Wesley Professional (November 5, 2004) ISBN-10: 0321247442, ISBN-13: 978-0321247445
Fundamentals Of Computer	Bibliografía	Security, Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry ISBN: 3540431012, ISBN-13: 9783540431015, 978-3540431015. Springer 2003

Otra Información

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.

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.

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.

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.

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.

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.

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.

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.

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.).