ANX-PR/CL/001-02
GUÍA DE APRENDIZAJE

ASIGNATURA

Seguridad de las tecnologias de la informacion

CURSO ACADÉMICO - SEMESTRE

2014-15 - Segundo semestre

FECHA DE PUBLICACIÓN

Diciembre - 2014

Datos Descriptivos

Nombre de la Asignatura	Seguridad de las tecnologias de la informacion
Titulación	10II - Grado en Ingenieria Informatica
Centro responsable de la titulación	E.T.S. de Ingenieros Informaticos
Semestre/s de impartición	Quinto semestre Sexto semestre
Materia	Sistemas operativos, sistemas distribuidos y redes
Carácter	Obligatoria
Código UPM	105000030

Datos Generales

Créditos	6	**Curso**	3
Curso Académico	2014-15	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Superadas

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

RA317 - Fundamentos, criptografía y criptoanálisis.

RA318 - Seguridad de los Datos de carácter Personal.

RA358 - Identificar riesgos y posibles ataques

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

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

RA434 - Conocer y comprender la importancia de la seguridad para la empresa

Profesorado

Profesorado

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

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

Descripción de la Asignatura

Temario

1. Bloque I
   1.1. Servicios criptográficos
   1.2. Confidencialidad y Claves
   1.3. Integridad y Autenticación
   1.4. Identidad, Identidad Digital y Firma Digital
2. Bloque II
   2.1. Desarrollo de códigos seguros
   2.2. Códigos Maliciosos y Ataques
   2.3. Operaciones y Sistemas de Defensa
3. Bloque III
   3.1. Control de accesos
   3.2. Aplicaciones de seguridad
4. Bloque IV
   4.1. Introducción y conceptos generales
   4.2. Auditoría, Análisis de Riesgos y Planes de Contingencia
   4.3. Seguridad de las instalaciones
   4.4. Legislación y Estándares

Cronograma

Horas totales: 72 horas

Horas presenciales: 72 horas (46.2%)

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	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 2	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 3	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 4	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 5	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 6	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 7	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			

Semana 8	**Servicios Criptográficos. Confidencialidad y Claves. Integridad y Autenticación. Identidad, Identidad Digital y Firma Digital.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Examen de Teoría** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 9	**Desarrollo de códigos seguros. Códigos Maliciosos y Ataques. Operaciones y Sistemas de Defensa** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 10	**Desarrollo de códigos seguros. Códigos Maliciosos y Ataques. Operaciones y Sistemas de Defensa** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 11	**Desarrollo de códigos seguros. Códigos Maliciosos y Ataques. Operaciones y Sistemas de Defensa** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 12	**Control de Accesos. Aplicaciones de Seguridad.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 13	**Control de Accesos. Aplicaciones de Seguridad.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Examen de Teoría** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 14	**Introducción y conceptos generales, Auditoría, Análisis de Riesgos y Planes de Contingencia. Seguridad de las instalaciones. Legislación y Estándares** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 15	**Introducción y conceptos generales, Auditoría, Análisis de Riesgos y Planes de Contingencia. Seguridad de las instalaciones. Legislación y Estándares** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 16	**Introducción y conceptos generales, Auditoría, Análisis de Riesgos y Planes de Contingencia. Seguridad de las instalaciones. Legislación y Estándares** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Examen de Teoría** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial

Semana 17				**Examen de Teoria y Entrega de Practicas y Ejercicios** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad presencial **Entrega de Practicas y Ejercicios** Duración: 02:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad 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 de Teoría	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	23%		Ce 6, Ce 8, CG-1/21, CG-19
13	Examen de Teoría	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	19%		Ce 29, CG-19, Ce 26/27
16	Examen de Teoría	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	8%		Ce 31, Ce 48
17	Examen de Teoria y Entrega de Practicas y Ejercicios	02:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%		CG-1/21, CG-19, Ce 6, Ce 8, Ce 22, Ce 26/27, Ce 29, Ce 31, Ce 48
17	Entrega de Practicas y Ejercicios	02:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	50%		Ce 6, Ce 8, Ce 22, Ce 26/27

Criterios de Evaluación

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 2014-2015Coordinador de la Asignatura: D. JORGE DÁVILA MURODepartamento: LENGUAJES Y SISTEMAS INFORMÁTICOS E INGENIERÍA DEL SOFTWAREFecha: __/___/2015Firmado:

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.

Recursos Didácticos

Descripción	Tipo	Observaciones
Applied Cryptography: Protocols, Algorithms, And Source Code In C, Second Edition	Bibliografía	Authors: Bruce Schneier Publisher: Wiley Published: 1996-10-18 ISBN-10: 0471117099 ISBN-13: 9780471117094
Practical Cryptography	Bibliografía	Author: Niels Ferguson, Bruce Schneier, Publisher: Wiley Pages: 432 Published: 2003-03-28 Language: English ISBN-10: 0471223573 ISBN-13: 9780471223573
Handbook of Applied Cryptography Discrete Mathematics and Its Applications	Bibliografía	Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. Published by CRC Press (1996) ISBN 10: 0849385237 ISBN 13: 9780849385230
Cryptography And Network Security: Principles And Practice (5th Edition)	Bibliografía	Authors: William Stallings Publisher: Prentice Hall Published: 2010-01-24 ISBN-10: 0136097049 ISBN-13: 9780136097044
Cryptography For Developers	Bibliografía	Authors: Tom St Denis Publisher: Syngress Published: 2007-01-15 ISBN-10: 1597491047 ISBN-13: 9781597491044
BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic	Bibliografía	Authors: Tom St Denis Publisher: Syngress Published: 2006-09-04 ISBN-10: 1597491128 ISBN-13: 9781597491129
Codes, Ciphers, Secrets And Cryptic Communication: Making And Breaking Secret Messages From Hieroglyphs To The Internet	Bibliografía	Authors: Fred B. Wrixon Publisher: Black Dog & Leventhal Publishers Published: 2005-09-01 ISBN-10: 1579124852 ISBN-13: 9781579124854
The Code Book: The Science Of Secrecy From Ancient Egypt To Quantum Cryptography	Bibliografía	Authors: Simon Singh Publisher: Anchor Published: 2000-08-29 ISBN-10: 0385495323 ISBN-13: 9780385495325
The Codebreakers: The Comprehensive History Of Secret Communication From Ancient Times To The Internet	Bibliografía	Authors: David Kahn Publisher: Scribner Published: 1996-12-05 ISBN-10: 0684831309 ISBN-13: 9780684831305

Descripción	Tipo	Observaciones
Security In Computing, 4th Edition	Bibliografía	Author: Charles P. Pfleeger, Shari Lawrence Pfleeger, Publisher: Prentice Hall Published: 2006-10-23 ISBN-10: 0132390779 ISBN-13: 9780132390774
Network Security: Private Communication In A Public World (2nd Edition)	Bibliografía	Author: Charlie Kaufman, Radia Perlman, Mike Speciner, Publisher: Prentice Hall Published: 2002-05-02 ISBN-10: 0130460192 ISBN-13: 9780130460196
Computer Security Basics	Bibliografía	Author: Rick Lehtinen, G.T. Gangemi Sr., Publisher: O'Reilly Media Published: 2006-06-20 ISBN-10: 0596006691 ISBN-13: 9780596006693
Computer Security	Bibliografía	Editor: John Wiley & Sons; Edición: 1 de febrero de 2006 ISBN-10: 0470862939 ISBN-13: 978-0470862933
Introduction To Computer Security	Bibliografía	Authors: Matt Bishop Publisher: Addison-Wesley Professional Published: 2004-11-05 ISBN-10: 0321247442 ISBN-13: 9780321247445
Fundamentals Of Computer Security (Monographs In Theoretical Computer Science)	Bibliografía	Authors: Josef, Thomas Hardjono And Jennifer Seberry Pieprz Publisher: Springer Berlin Heidelberg Published: 2003-01-21 ISBN-10: 3540431012 ISBN-13: 9783540431015
Sitio web de la Asignatura	Recursos web	http://porsche.ls.fi.upm.es y https://porsche.ls.fi.upm.es