ANX-PR/CL/001-02

GUÍA DE APRENDIZAJE

ASIGNATURA

Seguridad de la informacion

CURSO ACADÉMICO - SEMESTRE

2015-16 - Segundo semestre

Datos Descriptivos

Nombre de la Asignatura	Seguridad de la informacion
Titulación	61IW - Grado en Ingenieria del Software
Centro responsable de la titulación	E.T.S. de Ingenieria de Sistemas Informaticos
Semestre/s de impartición	Cuarto semestre
Materia	Seguridad de la informacion
Carácter	Obligatoria
Código UPM	615000244
Nombre en inglés	Information Security

Datos Generales

Créditos	3	**Curso**	2
Curso Académico	2015-16	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

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

Otros Requisitos

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

Conocimientos Previos

Asignaturas Previas Recomendadas

Fundamentos de seguridad

Algebra

Logica y matematica discreta

Otros Conocimientos Previos Recomendados

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

Competencias

CC1 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

CT8 - Trabajo en equipo: Ser capaz de trabajar como miembro de un equipo interdisciplinar con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

Resultados de Aprendizaje

RA198 - Analiza y aplica el algoritmo RSA para la firma digital.

RA199 - Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA y realiza diferentes ataques al sistema.

RA195 - Conoce y analiza el funcionamiento de las funciones hash MD5 y SHA-1, aplicando los algoritmos..

RA143 - Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

RA200 - Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales

RA201 - Desarrollar sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales

RA197 - Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación

RA118 - Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

RA85 - Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Camara Delgado, Mercedes De La **(Coordinador/a)**	D-1109	mercedes.delacamara@upm.es	Los horarios de tutorías serán publicados al inicio de curso, no obstante pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura
Mahillo Garcia, Maria Angeles	D-1110	mariaangeles.mahillo@upm.es	Los horarios de tutorías serán publicados al inicio de curso, no obstante pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura

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

En esta asignatura se estudia la protección de la información utilizando técnicas de criptografía asimétrica, firma digital y certificados digitales. Tambien introduce en las fases e implantación de un Sistema de Gestión de la Seguridad de la información.

Temario

1. Funciones hash
   1.1. Características y propiedades de las funciones hash.
   1.2. Funciones hash MD5, SHA1.
   1.3. Ataques a las funciones hash y el nuevo estándar del NIST.
2. Criptografía Asimétrica o de clave pública.
   2.1. Introducción
   2.2. Intercambio de clave de Diffie y Hellman.
   2.3. Caracteristicas. Ventajas y desventajas frente al cifrado simétrico
3. Principios del algoritmo (Rivest, Shamir y Adleman)
   3.1. Operaciones típicas con RSA
   3.2. Algoritmo para el cálculo de inversos
   3.3. Algoritmo de exponenciación rápida
4. Cifrado y descifrado con RSA
   4.1. Cifrar y descifrar mensajes de texto
   4.2. Claves parejas
   4.3. Números no cifrables
5. Ataques al RSA
   5.1. Ataque basado en la factorización del módulo n
   5.2. Ataque por cifrado cíclico con la clave pública
   5.3. Ataque basado en la paradoja del cumpleaños
6. Sistemas de Autenticación
   6.1. Firma digital RSA
   6.2. Mecanismos de autenticación
   6.3. Formas de autenticación

7. Certificados digitales

7.1. Conceptos de Autoridades de certificación

7.2. Algoritmos y características de un certificado X.509.

7.3. Tareas típicas con Certificados digitales

8. Sistema de Gestión de la Seguridad de la Información

8.1. Introducción a políticas y planes de seguridad.

8.2. Implantación de un SGSI.

8.3. Fases de un SGSI.

Cronograma

Horas totales: 37 horas

Horas presenciales: 37 horas (47.4%)

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: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 2	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 3	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 4	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 5	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 6	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			

Semana 7	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 8	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 9	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			**Examen Tema 1, 2, 3, 4 (Ev. Continua) (RA195, RA197, RA143, RA85)** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 10	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 11	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 12	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			

Semana 13	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 14	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 15	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 16	**Clase de teoría: Impartición de contenidos** Duración: 02:00 OT: Otras actividades formativas			**Competencia Transversal (R118))** Duración: 00:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad no presencial
Semana 17				**Examen Tema 5, 6, 7, 8 (Ev. Continua) (RA85, RA198 RA201, RA199, RA200)** Duración: 03:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial **Examen "Sólo prueba final" (RA118, RA143, RA195, RA197, RA85, RA198, RA199, RA200, RA201)** Duración: 03:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad presencial **Asistencia a clases** Duración: 00:00 OT: Otras técnicas evaluativas 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
9	Examen Tema 1, 2, 3, 4 (Ev. Continua) (RA195, RA197, RA143, RA85)	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	45%		CC1
16	Competencia Transversal (R118))	00:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	No	5%		CT8
17	Examen Tema 5, 6, 7, 8 (Ev. Continua) (RA85, RA198 RA201, RA199, RA200)	03:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	45%		CC1
17	Examen "Sólo prueba final" (RA118, RA143, RA195, RA197, RA85, RA198, RA199, RA200, RA201)	03:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%	5 / 10	CC1, CT8
17	Asistencia a clases	00:00	Evaluación continua	OT: Otras técnicas evaluativas	Sí	5%		

Criterios de Evaluación

1. ELECCIÓN DEL SISTEMA DE EVALUACIÓN

De acuerdo con el artículo 20 de la normativa reguladora de los sistemas de evaluación en los procesos formativos vinculados a los títulos de grado y máster universitario con planes de estudio adaptados al R.D. 1393/2007.

En la convocatoria ordinaria de esta asignatura, la elección entre el sistema de evaluación continua o el sistema de evaluación mediante sólo prueba final corresponde al estudiante.

El alumno que desee seguir el sistema de evaluación mediante sólo prueba final, deberá comunicarlo por escrito al coordinador de la asignatura o bien responder a la consulta que la asignatura formulará en la plataforma Moodle de la misma. Fecha tope para la solicitud 20 de abril de 2016.

El sistema de evaluación continua será el que se aplique en general a todos los estudiantes de cada asignatura si el alumno no comunica lo contrario por los medios anteriormente expuestos

2. CRITERIOS DE CALIFICACIÓN.

2.1. CONVOCATORIA ORDINARIA.

2.1.1 EVALUACIÓN CONTINUA.

Los instrumentos que se van a utilizar en la evaluación de proceso de aprendizaje de los alumnos en evaluación continua se detallan a continuación

Técnica evaluativa	Descripción	Peso	Fecha
OT: Otras técnicas evaluativas	Asistencia y participación en el aula	5%	
TI: Técnica del tipo Trabajo Individual	Realización de actividades relacionadas con la competencia Trabajo en equipo (CT_8)	5%	Semana 16. Fecha concreta se indicará en la plataforma de la asignatura
EX: Técnica del tipo Examen Escrito	Evaluación de los temas 1, 2, 3 y 4.	45%	Fecha proporcionada por Sub. Ord. Académica y Doctorado

EX: Técnica del tipo Examen Escrito	Evaluación del tema 5, 6, 7 y 8.	45%	Fecha proporcionada por Sub. Ord. Académica y Doctorado

Para superar la asignatura se necesita obtener una nota igual o superior a 5 una vez evaluadas las actividades anteriores.

Para superar la competencia transversal deberán realizarse todas las actividades propuestas para la misma y obtener una calificación APTO. La calificación numérica a sumar a la nota de la asignatura vendrá dada por la evaluación de una o varias de las actividades propuestas.

2.1.2. EVALUACIÓN "SÓLO EXAMEN FINAL".

Los alumnos que hayan decidido no seguir la evaluación continua, tendrán la posibilidad de presentarse a un examen escrito final sobre 9,5 puntos. En el mismo se evaluará tanto los contenidos teóricos como las actividades prácticas realizadas durante el curso. Para aquellos que hayan sido evaluados de la competencia transversal, la nota numérica obtenida en la misma se sumará a la obtenida en el examen de la convocatoria ordinaria. Los alumnos que no hayan sido evaluados de la competencia transversal deberán entregar las actividades propuestas en la fecha que indique la asignatura.

2.2. CONVOCATORIA EXTRAORDINARIA.

De acuerdo con el artículo 19 de la normativa reguladora de los sistemas de evaluación en los procesos formativos vinculados a los títulos de grado y máster universitario con planes de estudio adaptados al R.D. 1393/2007

Todos los alumnos que no hayan superado la asignatura en la convocatoria ordinaria tendrán la posibilidad de presentarse a un examen escrito final sobre 9,5 puntos. En el mismo se evaluará tanto los contenidos teóricos como las actividades prácticas realizadas durante el curso. Para aquellos que hayan sido evaluados de la competencia transversal, la nota numérica obtenida en la misma se sumará a la obtenida en el examen de la convocatoria ordinaria. Los alumnos que no hayan sido evaluados de la competencia transversal deberán entregar las actividades propuestas en la fecha que indique la asignatura.

Recursos Didácticos

Descripción	Tipo	Observaciones
Profesores de la Asignatura. Transparencias. Dpto. de Publicaciones EUI 2015	Otros	Transparencias
Criptografía Digital. Pastor, José; Sarasa, Miguel Angel. Colección Textos Docentes; Prensas Universitarias de Zaragoza	Bibliografía	Ampliación conocimientos
Seguridad Informática y Criptografía. Ramió Aguirre, Jorge. Seguridad Informática y Criptografía v 4.1 Dpto. de Publicaciones E.U.I., 2006 (edición impresa). Libro electrónico gratuito disponible en la página Web del autor.	Bibliografía	Ampliación conocimientos
Seguridad de la Información. Redes, informática y sistemas de información. Areitio, Javier. Paraninfo, 2008	Bibliografía	Ampliación conocimientos
Plataforma Moodle de GATE para la asignatura	Equipamiento	Plataforma Moodle de GATE para la asignatura
Sitios web	Recursos web	Todas aquellos sitios web oficiales que estén relacionados con la materia impartida: Red Temática Iberoamericana de Criptografía y Seguridad de la Información Inteco, Agencia de Protección de Datos, Normas UNE (NorWeb), etc.