GUÍA DOCENTE 2012-2013

SEGURIDAD INFORMÁTICA

1. Denominación de la asignatura:

SEGURIDAD INFORMÁTICA

Código

2. Materia o módulo a la que pertenece la asignatura:

SISTEMAS OPERATIVOS, SISTEMAS DISTRIBUIDOS Y REDES

3. Departamento(s) responsable(s) de la asignatura:

INGENIERÍA CIVIL

4.a Profesor que imparte la docencia (Si fuese impartida por mas de uno/a incluir todos/as) :

JOSÉ MANUEL SÁIZ DIEZ

4.b Coordinador de la asignatura

JOSÉ MANUEL SÁIZ DIEZ

5. Curso y semestre en el que se imparte la asignatura:

Curso: 3 – Semestre: 6

6. Tipo de la asignatura: (Básica, obligatoria u optativa)

Obligatoria

7. Número de créditos ECTS de la asignatura:

6

8. Competencias que debe adquirir el alumno/a al cursar la asignatura

CG1: Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas. CG2: Capacidad para dirigir las actividades objeto de los proyectos del ámbito de la informática. Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan. CG4: Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas. CG5: Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. CG6: Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes. CG7: Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento. CG8: Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones. CG9: Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática. CG10: Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática. IS5: Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse. SI2: Capacidad para determinar los requisitos de los sistemas de información y

comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.

SI5: Capacidad para comprender los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.

CT1: Capacidad de análisis y síntesis.

CT2: Capacidad de organización y planificación.

CT3: Comunicación oral y escrita en la lengua nativa.

CT4: Conocimiento de una lengua extranjera.

CT5: Conocimientos de informática relativos al ámbito de estudio.

CT6: Capacidad de gestión de la información.

CT7: Resolución de problemas.

CT8: Toma de decisiones.

CT9: Trabajo en equipo.

CT12: Habilidades en las relaciones interpersonales.

CT14: Razonamiento crítico.

CT15: Compromiso ético.

CT16: Aprendizaje autónomo.

CT17: Adaptación a nuevas situaciones.

CT18: Creatividad.

CT19: Liderazgo.

CT21: Iniciativa y espíritu emprendedor.

CT22: Motivación por la calidad.

CT24: Comunicarse con personas expertas y no expertas en la materia.

CT25: Elaborar y defender argumentos dentro del ámbito de la Informática.

CT26: Desarrollar habilidades de aprendizaje para emprender estudios posteriores con un alto grado de autonomía.

CT27: Planificación y gestión del tiempo.

9. Programa de la asignatura

9.1- Objetivos docentes
Los objetivos a desarrollar serán: introducir la problemática de la seguridad como elemento básico en el entorno informático, analizar la seguridad en ordenadores personales, sistemas operativos, redes e Internet, analizar y planificar los riesgos y planes de contingencia, introducir las técnicas y productos para la seguridad y analizar el ámbito legal y ético de la seguridad informática.
9.2- Unidades docentes (Bloques de contenidos)
1. Introducción a la problemática de la seguridad informática . **2. Seguridad Física.** **3. Seguridad en Ordenadores Personales.** **4. Seguridad en Sistemas Operativos.** **5. Virus y otras amenazas programadas.** **6. Criptografía.** **7. Seguridad en Redes e Internet.** **8. Análisis y Planificación de Riesgos.** **9. Técnicas y productos para la Seguridad.**

10. Ámbito legal y ético en relación con la Seguridad Informática.

9.3- Bibliografía

BIBLIOGRAFÍA BÁSICA

1. Jorge Ramió Aguirre., 1. Curso de Seguridad Informática y Criptografía, Apuntes, http://www.criptored.upm.es/guiateoria/gt_m001a.htm.

BIBLIOGRAFÍA COMPLEMENTARIA

Amparo Fúster Sabater, Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Masque, (2000) Técnicas Criptográficas de protección de datos, 2, Ra-ma ,

Anónimo, (2000) Edición Especial Linux. Máxima Seguridad, Prentice Hall.,

Anónimo, (1994) 10. Los virus informáticos. Qué son, Cómo actúan y cómo combatirlos, 10. Multimedia Ediciones S.A.,

Anónimo, (2001) ADVANCED ENCRYPTION STANDARD (AES)., 197, Federal Information Processing Standards Publication, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Anónimo, (1999) DATA ENCRYPTION STANDARD (DES), 46-3, Federal Information Processing Standards Publication , http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

Anónimo, (1980) Specifications for DES MODES OF OPERATION, 81,] Federal Information Processing Standards Publication, http://www.itl.nist.gov/fipspubs/fip81.htm.

B. Schneier, (1996) Applied Cryptography, 2, John Wiley & Sons,

Bellovin S. y Cheswick B. , (1994) Firewalls and Internet Security, Addison-Wesley,

C.P. Pfleeger, (1997) Security in Computing, 2, Prentice Hall,

Chapman B. y Zwicky E.D., (1995) Building Internet Firewalls, 2, Prentice Hall,

D. Bell and L. La.Pa.dula, (1975) Secure Computer Systems: Unified Exposit,ion and hZultics Interpretation, MITRE, Bed- ford, Mass,

D. Russell y G.T. Gangemi, (1991) Computer Security Basics, 1. O'Reilly & Associates,

Department of defense standard, Orange Book. Trusted computer system evaluation criteria, Department of defense standard,

Edison Castaño, Dario Melo, Juan Pablo Garzón Ruiz y Andres Gonzalez, (2003) El Modelo de Seguridad Biba, Universidad de los Andes, Bogotá, Colombia,

Fred B. Schneider, Cryptosystem Design and AES, Sin editar, http:// www.cs.cornell.edu/Courses/cs513/2002fa/L23a.html.

Gil Valera J. , (1997) Estudio de Técnicas de Criptografía Aplicadas a las Comunicaciones, Fac. Informática. U. Murcia,

J.M. Morat, A. Ribagorda y J. Sancho, (1994) Seguridad y Protección de la Información, Centro de Estudios Ramón Areces,

José Lucena López, (2003) Criptografía y Seguridad en Computadores, 3, UNED,

José Pastor Franco, Miguel Ángel Sarasa López, (1998) Criptografía digital. Fundamentos y aplicaciones, 2, Prensas Universitarias de Zaragoza. ,

S. Garfinkel y G. Spafford, (1996) Practical UNIX and Internet Security, 2, S. Garfinkel y G. Spafford. O'Reilly & Associates,

10. Metodología de enseñanza y aprendizaje y su relación con las competencias que debe adquirir el estudiante:

Metodología	Competencia relacionada	Horas presenciales	Horas de trabajo	Total de horas
Clases teóricas	IS5, SI2, SI5	24	50	74
Clases prácticas (pequeño grupo)	IS5, SI2, SI5	24	40	64
Exposiciones públicas	IS5, SI2, SI5	2	2	4
Tutorías	IS5, SI2, SI5	1	0	1
Realización de trabajos, informes, memorias	IS5, SI2, SI5	0	4	4
Pruebas de evaluación	IS5, SI2, SI5	3	0	3
Total		54	96	150

11. Sistemas de evaluación:

Cuando no se haya producido el número necesario de aportaciones por parte de los alumnos, la evaluación continua de clases teóricas se tratará como una mejora de nota.
De igual forma si no se hace un suficiente uso de las tutorías su valoración se tratará como una mejora de nota.
Las mejoras de nota se sumarán al 100% de la nota calculada a partir de los otros procedimientos que mantendrán la proporcionalidad de las valoraciones.

La recuperación de las diferentes partes se hará a través de los mismos procedimientos de evaluación para las dos pruebas finales y para la entrega de las prácticas de laboratorio, entrega limitada a la fecha de examen.
Para el caso de la evaluación continua de las clases teóricas y la participación activa en las tutorías se tratarán como mejoras de nota en cualquier caso, siendo el resto de procedimientos el 100% y manteniendo las proporcionalidades.

Procedimiento	Peso en la calificación final
Evaluación continua de clases teóricas	15 %
Evaluación continua de prácticas de laboratorio	40 %
Prueba final escrita de teoría	20 %
Prueba final escrita de problemas	20 %
Participación activa en las tutorías	5 %
Total	**100 %**

12. Recursos de aprendizaje y apoyo tutorial:

Pizarra y Proyectores
Páginas Webs relacionadas
Bibliografía disponible en la Biblioteca
Aplicaciones para ejercitar los contenidos de la materia.
Tutorías individualizadas o en grupo a demanda de los alumnos
El material dedicado a la docencia se hará público desde el comienzo del curso: Material de prácticas y guiones, aplicaciones, transparencias y otros ficheros en Internet

13. Calendarios y horarios:

El calendario aprobado por la Junta de Escuela de la Escuela Politécnica Superior y los horarios publicados en los tablones oficiales de la E.P.S. para el curso 2012-2013

14. Idioma en que se imparte:

Español