Grado en Ingeniería Informática
30227 - Seguridad informática

Guía docente para el curso 2014 - 2015

Curso: 4, Semestre: 1, Créditos: 6.0

Información básica

Profesores

- **Gabriel Fuertes Muñoz** gfuertes@unizar.es
- **Raquel Lacuesta Gilaberte** lacuesta@unizar.es
- **Fernando Tricas García** ftricas@unizar.es
- **Fernando García Vallés** gvalles@unizar.es
- **Félix Serna Fortea** fserna@unizar.es

Recomendaciones para cursar esta asignatura

El adecuado aprovechamiento de esta asignatura se obtiene habiendo adquirido previamente un nivel de conocimientos equivalente al que se obtiene con las asignaturas de Sistemas Distribuidos, Administración de Sistemas, Bases de Datos, Programación, ...

Actividades y fechas clave de la asignatura

El calendario de exámenes y las fechas de entrega de trabajos se anunciará con suficiente antelación.

Inicio

Resultados de aprendizaje que definen la asignatura

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados...

1:
Conoce los fundamentos de la seguridad informática en su vertiente organizacional e implementación en sistemas, redes, bases de datos y software.

2:
Tiene aptitud para diseñar un modelo de seguridad informática integral para una organización siguiendo una metodología adecuada.

3: Domina diferentes herramientas que ayudan en el desarrollo de las diferentes etapas de la metodología utilizada.

4:
Es capaz de evaluar la situación de la seguridad de un sistema informático y sus aplicaciones.

5:
Entiende y sabe aplicar las diferentes normativas y estándares en seguridad informática, así como la legislación relacionada.

Introducción

Breve presentación de la asignatura

En esta asignatura se plantea el aprendizaje de conceptos, actividades y tecnologías requeridas en la seguridad informática.

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

En asignaturas previas, los alumnos han aprendido los conceptos de diferentes ámbitos de la informática, desde la programación, redes, sistemas operativos, administración de sistemas, sistemas distribuidos, …

En cuanto a aspectos de seguridad, las asignaturas de administración de sistemas y de sistemas distribuidos han planteado algunos conceptos y mecanismos básicos.

A partir de esas referencias, esta asignatura afianza los conceptos de seguridad previamente introducidos y desarrolla la problemática de este campo de una forma completa desde la definición de objetivos, el análisis y especificación del problema desde un punto de vista de seguridad, el diseño de soluciones, la implementación de dichas soluciones con los mecanismos y procedimientos adecuados y la validación y comprobación periódica de los objetivos inicialmente planteados.

Contexto y sentido de la asignatura en la titulación

Seguridad informática es una asignatura que integra y amplia los conocimientos ya desarrollados en asignaturas previas como “Sistemas Distribuidos” y “Administración de Sistemas”. Además, supone un apoyo para la mayor parte de conocimientos aprendidos en el resto de asignaturas informáticas, en cuanto que hoy en día los aspectos de seguridad están extendidos en la mayor parte de ellos. Aporta conocimientos esenciales para el funcionamiento de las Tecnologías de la Información hoy en día.

Al superar la asignatura, el estudiante será más competente para...

1:

Para resolver problemas y tomar decisiones con iniciativa, creatividad y razonamiento crítico.

2:
Para la gestión de la información, el manejo y la aplicación de las especificaciones técnicas y la legislación necesarias para la práctica de la Ingeniería.

3:
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.

4:

Para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes.

5:
Para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuado.

6:
Para conocer la normativa y la regulación de la informática en los ámbitos nacional, europeo e internacional.

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

La seguridad informática es, hoy en día, un aspecto esencial de la informática, dada la amplia dependencia actual de la actividad humana en los sistemas informáticos.

Evaluación

Actividades de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluacion

1:
En la En la Escuela de Ingeniería y Arquitectectura de Zaragoza

De acuerdo con la normativa de evaluación aprobada por la Escuela de Ingeniería y Arquitectura (EINA), la evaluación de la asignatura seguirá un **procedimiento de evaluación global**.

La prueba global de evaluación de la asignatura consta de dos partes:

- Examen escrito en el que se deberán resolver problemas, responder preguntas conceptuales, o resolver algún ejercicio. Es necesario una calificación mínima de 4.0 puntos en el examen escrito para aprobar la asignatura. La calificación obtenida en este examen pondera un 70% de la nota de la asignatura.
- Trabajo práctico en el laboratorio. Se valorará que las soluciones aportadas se comporten según las especificaciones, la calidad de su diseño y el tiempo empleado. Es necesario una calificación mínima de 4.0 puntos en el trabajo práctico de laboratorio para aprobar la asignatura. La calificación obtenida pondera un 30% de la nota de la asignatura. Los alumnos que necesiten obtener la calificación mínima exigida o, simplemente, subir su nota en este apartado, podrán presentarse a un examen práctico global que se efectuará el mismo día que el examen escrito de teoría.

La nota en una determinada convocatoria será la que corresponda a la suma ponderada de las calificaciones en las dos pruebas, estando limitada a 4 puntos sobre 10 en el caso de no alcanzar un 4 sobre 10 en cada una de ellas

En el caso de que el alumno no logre superar la asignatura en la primera convocatoria, pero logre superar una de las dos partes de la prueba global, la calificación obtenida en dicha prueba se mantendrá para la convocatoria siguiente del mismo curso académico.

2:
En la Escuela Universitaria Politécnica de Teruel

La prueba global de evaluación de la asignatura consta de dos partes:

- Examen escrito en el que se deberán resolver problemas, responder preguntas conceptuales, o resolver algún ejercicio. Es necesario una calificación mínima de 4.0 puntos en el examen escrito para aprobar la asignatura. La calificación obtenida en este examen pondera un 60% de la nota de la asignatura.
- Trabajo práctico en el laboratorio. Se valorará que las soluciones aportadas se comporten según las especificaciones, la calidad de su diseño y el tiempo empleado. Es necesario una calificación mínima de 4.0

puntos en el trabajo práctico de laboratorio para aprobar la asignatura. La calificación obtenida pondera un 40% de la nota de la asignatura. Los alumnos que necesiten obtener la calificación minima exigida o, simplemente, subir su nota en este apartado, podrán presentarse a un examen práctico global que se efectuará el mismo día que el examen escrito de teoría.

En el caso de que el alumno no logre superar la asignatura en la primera convocatoria, pero logre superar una de las dos partes de la prueba global, la calificación obtenida en dicha prueba se mantendrá para la convocatoria siguiente del mismo curso académico.

Actividades y recursos

Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

- El aprendizaje de conceptos y metodologías para el diseño de sistemas , programas y bases de datos seguros a través de las clases magistrales.
- La aplicación de dichos conocimientos en clase de problemas para solucionar diferentes situaciones y tareas de seguridad informática.
- En las clases prácticas, el alumno implementará, en el laboratorio, diferentes aspectos análisis de riesgos, especificación, diseño e implementación de mecanismos de seguridad y la evaluación del nivel de seguridad obtenida.

Actividades de aprendizaje programadas (Se incluye programa)

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades...

1:
Desarrollo del temario de la asignatura en clases impartidas en el aula.

2:
Resolución de problemas de aplicación de conceptos y técnicas presentadas en el programa de la asignatura durante las clases de problemas.

3:
Desarrollo de sesiones prácticas, en un laboratorio informático, para la aplicación de los temas estudiados en la asignatura.

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

La organización docente de la asignatura prevista es la siguiente:

Escuela de Ingeniería y Arquitectura de Zaragoza

- Clases teóricas y de problemas (3 horas semanales).
- Clases prácticas de laboratorio (2 horas cada 2 semanas). Son sesiones de trabajo de programación en laboratorio, tuteladas por un profesor, en las que participan los alumnos en grupos reducidos.

Escuela Universitaria Politécnica de Teruel

La organización docente de la asignatura prevista en la Escuela Universitaria Politécnica de Teruel es la siguiente:

- Actividad tipo 1 (clases teóricas) 2 horas/semana 1 grupo
- Actividad tipo 2 (clases problemas) 1 hora/semana 2 grupos

- Actividad tipo 3 (clases de prácticas)1 hora/semana 2 grupos

Programa

Programa de la asignatura

Conceptos básico : Objetivos. Riesgos. Ciclo de seguridad. Protección y estados de seguridad. Modelos de seguridad. Matriz de control de accesos.

Análisis de riesgos: Modelos. Vulnerabilidades. Ataques. Evaluación. Herramientas.

Políticas de seguridad: Tipos de políticas. Tipos de control de acceso. Lenguajes de políticas. Composición de políticas. Herramientas.

Mecanismos de seguridad en hardware, sistemas, redes, bases de datos y software:

- Principios de diseño. Aspectos de programación segura. Criptografía.
- Representación de identidad. Mecanismos de control de accesos. Protocolos de seguridad. Flujo de información. Confinamiento.
- Detección y tolerancia de intrusiones.

Legislación, normativas y estándares.

Trabajo

Trabajo del estudiante

La dedicación del estudiante para alcanzar los resultados de aprendizaje en esta asignatura se estima en 150 horas distribuidas del siguiente modo:

- 56 horas, aproximadamente, de actividades presenciales (clases teóricas, de problemas y prácticas en laboratorio).
- 91 horas de estudio personal efectivo (estudio de apuntes y textos, resolución de problemas, preparación clases y prácticas, desarrollo de programas).
- 3 horas de examen final escrito.

Bibliografía

Bibliografía recomendada

- **Introduction to Computer Security**, Michael Goodrich, Roberto Tamassia, Addison-Wesley, 2011, ISBN-13: 9780321512949
- **Security in Computing, Fourth Edition**, Pfleeger and Pfleeger, ISBN 0-13-239077-9.
- **Building Secure Software**. John Viega and Gary McGraw. Addison-Wesley
- **Network Security, Second Edition,** Kaufman, Perlman, and Speciner, ISBN 0-13-046019-2. Michael Howard, David C. LeBlanc. Writing Secure Code. Microsoft Press.
- **Security Engineering: A Guide to Building Dependable Distributed Systems**, **2nd edition**, Ross J. Anderson, Wiley, 2008, ISBN-13: 978-0470068526
- **Innocent Code. A security wake-up call for web programmers**. Sverre H. Huseby. Wiley.

Referencias bibliográficas de la bibliografía recomendada

Escuela Universitaria Politécnica

- Anderson, Ross J.. Security engineering : a guide to building dependable distributed systems / Ross J. Anderson . 2nd ed. Indianapolis (Indiana) : Wiley, cop. 2008
- GOODRICH, M. Introduction to computer security / Michael Goodrich, Roberto Tamassia. Reading (Massachesetts) : Addison-Wesley Longman, 2011
- Huseby, Sverre H.. Innocent code : a security wake-up call for Web programmers / Sverre H. Huseby . Chinchester (England) : John Wiley & Sons, cop. 2004
- KAUFMAN, Ch. Network Security / Charles Kaufman, Radia Perllman, Mike Speciner. New Jersey : Prentice Hall,
- Pfleeger, Ch. Security in computing. Fourth Edition / Charles Pfleeger. New Jersey : Prentice Hall, 2006
- Viega, John. Building secure software : how to avoid security problems the right way / John Viega, Gary McGraw . Boston : Addison-Wesley, cop. 2002

Escuela Politécnica Superior

- 1. Goodrich, Michael. Introduction to Computer Security / Michael Goodrich, Roberto Tamassia, Addison-Wesley, 2011
- 2. Pfleeger, Charles P.. Security in Computing / Pfleeger, C.P. and Pfleeger, S.L.. - Fourth Edition Prentice Hall, 2006
- 3. Viega, John. Building secure software : how to avoid security problems the right way / John Viega, Gary McGraw Boston : Addison-Wesley, cop. 2002
- 4. Kaufman, C . Network Security / C. Kaufman, R. Perlman, and M. Speciner, . Second Edition Prentice Hall, 2002
- 5. Anderson, Ross J.. Security engineering : a guide to building dependable distributed systems / Ross J. Anderson . - 2nd ed. Indianapolis (Indiana) : Wiley, cop. 2008
- 6. Huseby, Sverre H.. Innocent code : a security wake-up call for Web programmers / Sverre H. Huseby Chinchester (England) : John Wiley & Sons, cop. 2004