Universidad Zaragoza

Curso : 2020/21

30227 - Seguridad informática

Información del Plan Docente

Año académico: 2020/21
Asignatura: 30227 - Seguridad informática
Centro académico: 110 - Escuela de Ingeniería y Arquitectura
326 - Escuela Universitaria Politécnica de Teruel
Titulación: 439 - Graduado en Ingeniería Informática
443 - Graduado en Ingeniería Informática
Créditos: 6.0
Curso: 4
Periodo de impartición: 439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
439 - Primer semestre
443 - Primer semestre
443 - Primer semestre
443 - Primer semestre
443 - Primer semestre
Clase de asignatura: Obligatoria
Materia: ---

1.Información Básica

1.1.Objetivos 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.

1.2.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.

1.3.Recomendaciones para cursar la 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 Administración de SIstemas, Sistemas Operativos, Redes de Computadores, Sistemas Distribuidos, Bases de Datos, Programación, ...

2.Competencias y resultados de aprendizaje

2.1.Competencias

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

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

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.

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.

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

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

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

2.2.Resultados de aprendizaje

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

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

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

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

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

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

2.3.Importancia de los resultados de aprendizaje

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.

3.Evaluación

3.1.Tipo de pruebas y su valor sobre la nota final y criterios de evaluación para cada prueba

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

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 tres 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 50% de la nota de la asignatura.
- Trabajo práctico. 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 para aprobar la asignatura. La calificación obtenida pondera un 25% de la nota de la asignatura.
- Realización y/o defensa de un trabajo que profundiza un tema entre los propuestos por el profesorado. Se valorará la capacidad de análisis, síntesis y originalidad del trabajo. Es necesario una calificación mínima de 4.0 puntos en el trabajo para aprobar la asignatura. La calificación obtenida pondera un 25% de la nota de la asignatura.

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

En la Escuela Universitaria Politécnica de Teruel

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

- Prueba teórica en el que se deberán resolver problemas, responder preguntas conceptuales teóricas o de aplicación práctica, o resolver algún ejercicio. Es necesario una calificación mínima de 4.0 puntos para aprobar la asignatura. La calificación obtenida en este examen pondera un 20% de la nota de la asignatura.
- Trabajo práctico. Se valorará que las soluciones aportadas se comporten según las especificaciones, memoria,

calidad de su diseño y tiempo empleado. Es necesario una calificación mínima de 4.0 puntos en el trabajo práctico para aprobar la asignatura. La calificación obtenida pondera un 70% de la nota de la asignatura
- Trabajo dirigido en la que se profundizará sobre aspectos avanzados de la seguridad informática. La calificación obtenida pondera un 10% de la nota de la asignatura.

4.Metodología, actividades de aprendizaje, programa y recursos

4.1.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 teóricas.
- 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 diferentes aspectos análisis de riesgos, especificación, diseño e implementación de mecanismos de seguridad y la evaluación del nivel de seguridad obtenida.
- Preparación de un trabajo para profundizar un tema entre los propuestos por el profesorado.

4.2.Actividades de aprendizaje

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

Desarrollo del temario de la asignatura en clases.

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

Desarrollo de sesiones prácticas para la aplicación de los temas estudiados en la asignatura.

Sesiones tuteladas en las que se realiza el seguimiento y/o la defensa de los trabajos

4.3.Programa

Conceptos básicos: Riesgos, amenazas, vulnerabilidades y ataques. Principios del diseño seguro. Autenticación y autorización. Estándares, regulación y legislación.

Seguridad en computadores: Modelos de seguridad. Control de accesos. Seguridad en Unix. Security-Enhanced Linux.

Seguridad en redes: Aspectos de diseño. Cortafuegos. Redes privadas virtuales. Sistemas de detección de intrusiones.

Fundamentos de la programación segura: Principios de diseño. Condiciones de carrera. Criptografía.

Gestión de la confianza y validación entradas.

Seguridad en bases de datos.

Seguridad en la web.

Auditoría.

4.4.Planificación de las actividades de aprendizaje y calendario de fechas clave

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 (2 horas cada 2 semanas). Son sesiones de trabajo de programación, tuteladas por un profesor, en las que participan los alumnos en grupos reducidos.
- Sesiones tuteladas para el seguimiento y/o defensa de los trabajos según el calendario definido por el profesorado.

Escuela Universitaria Politécnica de Teruel

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

- Clases teóricas y de problemas (2 horas semanales).
- Clases prácticas (2 horas semanales).

- Sesiones tuteladas para el seguimiento y/o defensa de los trabajos según el calendario definido por el profesorado.

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:
  - clases teóricas, problemas, prácticas
  - sesiones tuteladas
- 91 horas de estudio personal efectivo:
  - estudio de apuntes y textos, resolución de problemas, preparación clases y prácticas, desarrollo de programas,
  - realización de trabajos
- 3 horas de examen final escrito.

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

4.5.Bibliografía y recursos recomendados

[BB: Bibliografía básica / BC: Bibliografía complementaria]

Zaragoza:

http://psfunizar7.unizar.es/br13/egAsignaturas.php?codigo=30227&Identificador=14678

- [BB] Viega, John. Building secure software : how to avoid security problems the right way / John Viega, Gary McGraw Boston : Addison-Wesley, cop. 2002
- [BB] Anderson, Ross J. Security engineering : a guide to building dependable distributed systems / Ross J. Anderson . - 2nd ed. Indianapolis (Indiana) : Wiley, cop. 2008
- [BB] Huseby, Sverre H. Innocent code : a security wake-up call for Web programmers / Sverre H. Huseby Chinchester (England) : John Wiley & Sons, cop. 2004
- [BB] Goodrich, Michael T. Introduction to computer security / Michael Goodrich, Roberto Tamassia . Harlow : Pearson, cop. 2014
- [BB] Pfleeger, Charles P. Security in computing / Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies . Fifth edition. Upper Saddle River, NJ : Prentice Hall, 2015
- [BB] Wenliang Du. Computer Security: A Hands-on Approach, CreateSpace Independent Publishing Platform, 2017, ISBN: 978-1548367947
- [BC] Kaufman, C . Network Security / C. Kaufman, R. Perlman, and M. Speciner, . Second Edition Prentice Hall, 2002

Teruel:

http://psfunizar7.unizar.es/br13/egAsignaturas.php?codigo=30227&Identificador=13598

- [BB] Anderson, Ross J.. Security engineering : a guide to building dependable distributed systems / Ross J. Anderson . 2nd ed. Indianapolis (Indiana) : Wiley, cop. 2008
- [BB] Goodrich, Michael T.. Introduction to computer security / Michael Goodrich, Roberto Tamassia . Harlow : Pearson, cop. 2014
- [BB] Huseby, Sverre H.. Innocent code : a security wake-up call for Web programmers / Sverre H. Huseby . Chinchester (England) : John Wiley & Sons, cop. 2004
- [BB] KAUFMAN, Ch. Network Security / Charles Kaufman, Radia Perllman, Mike Speciner. New Jersey : Prentice Hall,
- [BB] Pfleeger, Charles P.. Security in computing / Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies . Fifth edition Upper Saddle River, NJ : Prentice Hall, 2015
- [BB] Viega, John. Building secure software : how to avoid security problems the right way / John Viega, Gary McGraw . Boston : Addison-Wesley, cop. 2002