UNIVERSIDAD INTERNACIONAL DE LA RIOJA unir

Asignatura: Seguridad en el Software

Cuatrimestre: 2º

ECTS: 3

Carácter: OB

Contenidos:

ID	Descripción
C1	Principios de diseño de software seguro.
C2	El ciclo de vida del software seguro.
C3	Codificación segura.

Competencias[1]:

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7- Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
- CG5 - Capacidad para la puesta en marcha, dirección y gestión de procesos de diseño y desarrollo de sistemas informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
- CE14 - Capacidad para diseñar, desarrollar e implantar sitios, servicios y sistemas basados en la Web con garantías de seguridad.
- CE17 - Analizar la infraestructura de red y los entornos de seguridad para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas.

[1] CB: Competencia básica; CG: Competencia general; CE: Competencia específica ; CT: Competencia transversal

- CE18 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
- CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.
- CE23 - Diseñar políticas de recuperación de datos adecuadas para disminuir el impacto ante desastres.
- CT1 -Analizar de forma reflexiva y crítica las cuestiones más relevantes de la sociedad actual para una toma de decisiones coherente.
- CT2 -Identificar las nuevas tecnologías como herramientas didácticas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje grupal.
- CT3 - Aplicar los conocimientos y capacidades aportados por los estudios a casos reales y en un entorno de grupos de trabajo en empresas u organizaciones.
- CT4 - Adquirir la capacidad de trabajo independiente, impulsando la organización y favoreciendo el aprendizaje autónomo.

Metodologías docentes:

ID	Denominación	Descripción
MD1	Lección magistral	Presentación de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada.
MD2	Estudios de casos	Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.
MD3	Resolución de ejercicios y problemas	Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral.
MD4	Aprendizaje Basado en Problemas (ABP)	A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas.
MD5	Contrato de Aprendizaje	Acuerdo establecido entre el profesor y el estudiante para la consecución de unos aprendizajes a través de una propuesta de trabajo autónomo, con la supervisión del profesor.

Temario:

Tema 1. El problema de la Seguridad en el Software

1.1. Introducción al problema de la Seguridad en el Software
1.2. Vulnerabilidades y su clasificación
1.3. Propiedades Software seguro

Tema 2. Principios de diseño de seguridad del software.

1.4. Introducción
1.5. Principios de diseño de seguridad del software
1.6. Tipos Ciclo de Vida del Software Seguro (S-SDLC)
1.7. Seguridad en las fases del S-SDLC
1.8. Metodologías y estándares

Tema 3. Seguridad en el ciclo de vida del Software en las fases de Requisitos y Diseño.

3.1. Introducción
3.2. Modelado de ataques
3.3. Casos de abuso
3.4. Ingeniería de Requisitos de Seguridad
3.5. Análisis de riesgo. Arquitectónico
3.6. Patrones de diseño

Tema 4. Seguridad en el ciclo de vida del Software en las fases de Codificación, Pruebas y Operación

4.1. Introducción.
4.2. Pruebas de seguridad basadas en riesgo
4.3. Revisión de código
4.4. Test de penetración
4.5. Operaciones de Seguridad
4.6. Revisión externa

Tema 5. Codificación Segura de Aplicaciones I

5.1. Introducción.
5.2. Prácticas de codificación segura
5.3. Criterios Selección de lenguaje.
5.4. Manipulación y validación de entradas
5.5. Desbordamiento de memoria
5.6. Errores y excepciones

Tema 6. Codificación Segura de Aplicaciones II

6.1. Introducción
6.2. Integers overflows, errores de truncado y problemas con conversiones de tipo entre números enteros
6.3. Privacidad y confidencialidad
6.4. Programas privilegiados

Bibliografía básica:

Asignatura basada exclusivamente en los apuntes del profesor.