UNIVERSIDAD INTERNACIONAL DE LA RIOJA unir

Asignatura: Seguridad en Aplicaciones On Line

Cuatrimestre: 2º

ECTS: 3

Carácter: OB

Contenidos:

ID	Descripción
C1	Problemas de seguridad en aplicaciones web.
C2	Políticas y estándares de seguridad para aplicaciones on-line.
C3	Vulnerabilidades más frecuentes.
C4	Seguridad de servicios web.

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.

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

- 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.
- 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. **Vulnerabilidades y problemas de seguridad en las aplicaciones online.**

1.1. Introducción a la seguridad en las aplicaciones online.

1.2. Vulnerabilidades de seguridad en el diseño de las aplicaciones web

1.3. Vulnerabilidades de seguridad en la implementación de las aplicaciones web

1.4. Vulnerabilidades de seguridad en el despliegue de las aplicaciones web

1.5. Listas oficiales de vulnerabilidades de seguridad

Tema 2. Políticas y estándares para la seguridad de las aplicaciones online

2.1. Pilares para la seguridad de las aplicaciones online

2.2. Política de seguridad

2.3. Sistema de gestión de seguridad de la información

2.4. Ciclo de vida de desarrollo seguro de software

2.5. Estándares para la seguridad de las aplicaciones

Tema 3. Seguridad en el diseño de las aplicaciones web

3.1. Introducción a la seguridad de las aplicaciones web

3.2. Seguridad en el diseño de las aplicaciones web

Tema 4. Test de la seguridad y protección online delas aplicaciones web

4.1. Análisis y test de la seguridad de las aplicaciones web

4.2. Seguridad en el despliegue y producción de las aplicaciones web

Tema 5. Seguridad en el diseño de los servicios web

5.1. Introducción a la seguridad de los servicios web

5.2. Funciones y tecnologías de la seguridad de los servicios web

Tema 6. Test de la seguridad y protección online de los servicios web

6.1. Evaluación de la seguridad de los servicios web

6.2. Protección *online*. Firewalls XML y Gateways XML

Bibliografía básica:

Aparte de los apuntes del profesor, se recomienda la siguiente bibliografía:

Especificación de vulnerabilidades disponibles en el sitio de OWASP:
https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf