Ingeniería de Sistemas Seguros

Curso Académico: (2019 / 2020) **Fecha de revisión: 23-04-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No procede

OBJETIVOS

COMPETENCIAS

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.

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.

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.

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.

Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido.

Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.

Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.

Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.

Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Conceptos de Ingeniería de Sistemas Seguros
1.1. Propiedades de Seguridad
1.2. Principios de Diseño para la Seguridad
1.3. Gestión de Riesgos
1.4. Regulaciones y Aspectos de Privacidad
1.5. Arquitecturas Software

2. Requisitos de Software Seguro
2.1. Descomposición de Políticas
2.2. Identificación y Elicitación

3. Diseño de Software Seguro
3.1. Procesos de Diseño
3.2. Consideraciones de Diseño
3.3. Seguridad de la Arquitectura
3.4. Tecnologías

4. Implementaciones Seguras
4.1. Seguridad de los Lenguajes de Programación
4.2. Bases de Datos de Vulnerabilidades
4.3. Prácticas y Controles Defensivos
4.4. Código Fuente. Versiones
4.5. Entornos de Desarrollo
4.6. Revisión y Análisis de Código
4.7. Técnicas Anti-manipulación de Código

5. Pruebas
5.1. Estrategias, Planes y Casos de prueba
5.2. Tipos de pruebas
5.3. Evaluación de Impacto y Acciones Correctivas
5.4. Gestión del Ciclo de Vida de los Datos de Prueba

6. Otros aspectos.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clase teórica
Clases prácticas en laboratorio
Tutorías
Trabajo en grupo
Trabajo individual del estudiante

METODOLOGÍAS DOCENTES
Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo
Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

Trabajos individuales o en grupo realizados durante el curso (50%)
Examen final (50%)
La evaluación será similar tanto en la convocatoria ordinaria como en la convocatoria extraordinaria.

Peso porcentual del Examen Final:	50
Peso porcentual del resto de la evaluación:	50

BIBLIOGRAFÍA BÁSICA

- Adam Shostack Threat modeling: Designing for security., John Wiley & Sons, 2014
- Mano Paul Official (ISC)2® Guide to the CSSLP® CBK®. Second edition., CRC Press, 2014