Programación semanal

En la programación semanal te presentamos un **reparto del trabajo de la asignatura** a lo largo de las semanas del cuatrimestre.

	CONTENIDO TEÓRICO	ACTIVIDADES (10 puntos)
Semana 1	**Semana de introducción a la asignatura**	
Semana 2	**Tema 1. El problema de la seguridad en el *software*** 1.1. ¿Cómo estudiar este tema? 1.2. Introducción al problema de la seguridad en el software 1.3. Vulnerabilidades y su clasificación	
Semana 3	**Tema 1. El problema de la seguridad en el *software* (continuación)** 1.4. Propiedades *software* seguro 1.5. Principios de diseño seguridad del *software* 1.6. Amenazas a la seguridad del *software*	
Semana 4	**Tema 1. El problema de la seguridad en el *software* (continuación)** 1.7. Tipos de S-SDLC 1.8. Los pilares de la seguridad del software 1.9. Metodologías y estándares	Trabajo: Comparación de ciclos de vida de desarrollo de *software* seguro (S-SDLC) (2,5 puntos)
Semana 5	**Tema 2. Seguridad en el ciclo de vida del *software*** 2.1. ¿Cómo estudiar este tema? 2.2. Introducción a la seguridad en Ciclo de Vida del Software (S-SDLC) 2.3. Seguridad en las fases del S-SDLC	
Semana 6	**Tema 2. Seguridad en el ciclo de vida del *software* (continuación)** 2.4. Modelado de ataques 2.5. Casos de abuso 2.6. Ingeniería de requisitos de seguridad	
Semana 7	**Semana de repaso**	
Semana 8	**Tema 2. Seguridad en el ciclo de vida del *software* (continuación)** 2.7. Análisis de riesgo. Arquitectónico 2.8. Patrones de diseño 2.9. Pruebas de seguridad basadas en riesgo	

	CONTENIDO TEÓRICO	ACTIVIDADES (10 puntos)
Semana 9	**Tema 2. Seguridad en el ciclo de vida del *software* (continuación)** 2.10. Revisión de código 2.11. Test de penetración 2.12. Operaciones de seguridad 2.13. Revisión externa	Trabajo: Metodologías de modelado de amenazas (2,5 puntos)
Semana 10	**Tema 3. Codificación segura** 3.1. ¿Cómo estudiar este tema? 3.2. Introducción a la codificación segura 3.3. Características de una buena implementación, prácticas y defectos a evitar	
Semana 11	**Tema 3. Codificación segura (continuación)** 3.4. Manejo de la entrada de datos 3.5. Desbordamiento de *buffer*	Foro: Fiabilidad del *software* y *hardware* original (1,25 punto)
Semana 12	**Tema 3. Codificación segura (continuación)** 3.6. *Integers overflows*, errores de truncado y problemas con conversiones de tipo entre números enteros 3.7. Errores y excepciones	
Semana 13	**Tema 3. Codificación segura (continuación)** 3.8. Privacidad y confidencialidad 3.9. Programas privilegiados	
Semana 14	**Tema 4. Análisis de malware** 4.1. ¿Cómo estudiar este tema? 4.2. Introducción al *malware* 4.3. Tipos de *malware*	Trabajo: Análisis dinámico de *malware* (3,75 puntos)
Semana 15	**Tema 4. Análisis de malware (continuación)** 4.4. Obtención del *malware*. Honeynet 4.5. Entorno y herramientas análisis de *malware* 4.6. Metodología de análisis de *malware*	
Semana 16	**Semana de repaso**	
Semana 17	**Examen final**	

NOTA

Esta **Programación semanal** puede ser modificada si el profesor lo considera oportuno para el enriquecimiento de la asignatura.