

Programación semanal

Para conocer la fecha de entrega de las distintas actividades accede a la sección **Actividades** (en el menú lateral). Recuerda que la suma de las puntuaciones de todas las actividades es de 15 puntos. Puedes hacer las que prefieras hasta conseguir un máximo de 10 puntos (que es la calificación máxima que se puede obtener en la evaluación continua).

	Contenido teórico	Actividades (12.5 puntos)	Eventos (2.5 puntos)
Semana 1	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 <i>software</i> 1.3. Vulnerabilidades y su clasificación	Trabajo: Comparación de ciclos de vida de desarrollo de software seguro (S-SDLC) (2.0 puntos)	Asistencia a 2 sesiones presenciales virtuales a lo largo de la asignatura (0,25 puntos cada una)
Semana 2	Tema 1. El problema de la seguridad en el software (continuación) 1.4. Propiedades <i>software</i> seguro 1.5. Principios de diseño seguridad del <i>software</i>		
Semana 3	Tema 1. El problema de la seguridad en el software (continuación) 1.6. Tipos de S-SDLC 1.7. Metodologías y estándares 1.8. Referencias bibliográficas		Test - Tema 1 (0.25 puntos)
Semana 4	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 <i>Software</i> (S-SDLC) 2.3. Seguridad en las fases del S-SDLC	Trabajo: Metodologías de modelado de amenazas (3.6 puntos)	Foro: Fiabilidad del software y hardware original (1.0 puntos)
Semana 5	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 6	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		
Semana 7	Tema 2. Seguridad en el ciclo de vida del software (continuación) 2.10. Revisión de código 2.11. Pruebas de penetración 2.12. Operaciones de seguridad 2.13. Revisión externa 2.14. Referencias bibliográficas		Test - Tema 2 (0.25 puntos)

	Contenido teórico	Actividades (12.5 puntos)	Eventos (2.5 puntos)
Semana 8	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 9	Tema 3. Codificación segura (continuación) 3.4. Manejo de la entrada de datos 3.5. Desbordamiento de <i>buffer</i>	Trabajo: Auditoría de código de una aplicación (3.6 puntos)	
Semana 10	Tema 3. Codificación segura (continuación) 3.6. <i>Integers Overflows</i> , errores de truncado y problemas con conversiones de tipo entre números enteros 3.7. Errores y excepciones		
Semana 11	Tema 3. Codificación segura (continuación) 3.8. Privacidad y confidencialidad 3.9. Programas privilegiados 3.10. Referencias bibliográficas		Test - Tema 3 (0.25 puntos)
Semana 12	Tema 4. Análisis de Malware 4.1. ¿Cómo estudiar este tema? 4.2. Introducción al <i>malware</i> 4.3. Tipos de <i>malware</i>	Trabajo: Análisis dinámico de malware (3.3 puntos)	
Semana 13	Tema 4. Análisis de malware (continuación) 4.4. Obtención del malware. <i>Honeynet</i> 4.5. Entorno y herramientas análisis de <i>malware</i>		Test - Tema 4 (0.25 puntos)
Semana 14	Tema 4. Análisis de malware (continuación) 4.6. Metodología de análisis de <i>malware</i> 4.7. Referencias bibliográficas		
Semana 15	Estudio personal / Consulta de dudas y preparación de exámenes		
Semana 16	Semana de exámenes		