

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).

	Temas	Actividades (15.0 puntos)	Clases en directo
Semana 1	Tema 1. El problema de la seguridad en el software 1.1. Introducción y objetivos 1.2. Introducción al problema de la seguridad en el software 1.3. Vulnerabilidades y su clasificación	Asistencia a 2 clases en directo a lo largo de la asignatura (0,25 puntos cada una)	Presentación de la asignatura y clase del tema 1
Semana 2	Tema 1. El problema de la seguridad en el software (continuación) 1.4. Propiedades software seguro 1.5. Principios de diseño seguridad del software		Clase del tema 1 (continuación)
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 (0.3 puntos)	Clase del tema 1 (continuación)
Semana 4	Tema 2. Seguridad en el ciclo de vida del software 2.1. Introducción y objetivos 2.2. Introducción a la seguridad en ciclo de vida del software (S-SDLC) 2.3. Modelado de amenazas 2.4. Casos de abuso	Actividad: Metodologías de modelado de amenazas (5.0 puntos)	Clase del tema 2 y presentación de la actividad: Metodologías de modelado de amenazas

	Temas	Actividades (15.0 puntos)	Clases en directo
Semana 5	Tema 2. Seguridad en el ciclo de vida del software (continuación) 2.5. Modelado de ataques 2.6. Ingeniería de requisitos de seguridad 2.7. Análisis de riesgo arquitectónico 2.8. Patrones de diseño		Clase del tema 2 (continuación)
Semana 6	Tema 2. Seguridad en el ciclo de vida del software (continuación) 2.9. Pruebas de seguridad basadas en riesgo 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 (0.4 puntos)	Clase del tema 2 (continuación)
Semana 7	Tema 3. Codificación segura 3.1. Introducción y objetivos 3.2. Características de una buena implementación, prácticas y defectos que evitar 3.3. Manejo de la entrada de datos	Caso grupal: Auditoría de código de una aplicación (3.0 puntos)	Clase del tema 3 y presentación del caso grupal: Auditoría de código de una aplicación
Semana 8	Tema 3. Codificación segura (continuación) 3.4. Desbordamiento de <i>buffer</i> 3.5. <i>Integers overflows</i>		Clase del tema 3 (continuación) Clase de resolución de la actividad: Metodologías de modelado de amenazas
Semana 9	Tema 3. Codificación segura (continuación) 3.6. Errores y excepciones 3.7. Privacidad y confidencialidad		Clase del tema 3 (continuación)
Semana 10	Tema 3. Codificación segura (continuación) 3.8. Programas privilegiados 3.9. Referencias bibliográficas	Test Tema 3 (0.4 puntos)	Clase del tema 3 (continuación)

	Temas	Actividades (15.0 puntos)	Clases en directo
Semana 11	Tema 4. Análisis de <i>malware</i> 4.1. Introducción y objetivos 4.2. Tipos de <i>malware</i>	Actividad: Análisis de <i>malware</i> (5.0 puntos)	Clase del tema 4 y presentación de la actividad: Análisis de <i>malware</i>
Semana 12	Tema 4. Análisis de <i>malware</i> (continuación) 4.3. Obtención del <i>malware</i> 4.4. Entorno y herramientas análisis de <i>malware</i>		Clase del tema 4 (continuación) Clase de resolución del caso grupal: Auditoría de código de una aplicación
Semana 13	Tema 4. Análisis de <i>malware</i> (continuación) 4.5. Métodos de análisis de <i>malware</i>		Clase del tema 4 (continuación) Sesión de explicación del modelo de examen
Semana 14	Tema 4. Análisis de <i>malware</i> (continuación) 4.6. Metodología de análisis de <i>malware</i> 4.7. Referencias bibliográficas	Test Tema 4 (0.4 puntos)	Clase del tema 4 (continuación)
Semana 15	Semana de repaso		Clase de repaso Clase de resolución de la actividad: Análisis de <i>malware</i>
Semana 16	Semana de exámenes		