DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Ciclo de Vida Seguro de Software (S-SDLC)
PLAN DE ESTUDIOS: Grado en Ingeniería Informática (PGR-INFORM)
GRUPO: 2526-M1
CENTRO: Escuela Politécnica Superior
CARÁCTER DE LA ASIGNATURA: Optativo
ECTS: 6,0
CURSO: 3º
SEMESTRE: 1º Semestre
IDIOMA EN QUE SE IMPARTE:
Castellano, excepto las asignaturas de idiomas que se impartirán en el idioma correspondiente

DATOS DEL PROFESOR

NOMBRE Y APELLIDOS: CARMELO GONZÁLEZ GARCÍA
EMAIL: cgonzalezg@uemc.es
TELÉFONO: 983 00 10 00
HORARIO DE TUTORÍAS: Jueves a las 16:00 horas

CV DOCENTE:

Docente especializado en informática, con una amplia experiencia en la enseñanza de disciplinas tecnológicas. Desde 2014 ha impartido más de 5.000 horas de formación presencial y online en áreas como ciberseguridad, inteligencia artificial, big data y sistemas informáticos, colaborando con instituciones publicas y plataformas de formación digital. Su sólida base científica, unida a su formación pedagógica, le permite abordar la enseñanza con un enfoque riguroso, práctico y adaptado a las necesidades del alumnado. Además, cuenta con formación en metodologías e-learning aplicadas a entornos como Moodle, lo que le capacita para diseñar experiencias de aprendizaje efectivas en formato digital. Su estilo docente se caracteriza por la claridad expositiva, el uso de recursos actualizados y la conexión constante entre teoría y práctica profesional. Como Físico aporta una visión analítica y estructurada al proceso de enseñanza, fomentando el pensamiento crítico y la comprensión profunda de los conceptos técnicos que conforman la base de las tecnologías emergentes.

CV PROFESIONAL:

Con una sólida trayectoria en el sector tecnológico y más de una década de experiencia profesional en entornos críticos. Ha trabajado como analista, desarrollador de software, gestor y coordinador de proyectos en sistemas informáticos y ciberseguridad, colaborando con entidades de alto nivel tanto a nivel financiero, energético, aeroespacial y de defensa. Su perfil técnico abarca desde la planificación y supervisión de infraestructuras tecnológicas hasta la administración de redes, plataformas de virtualización (VMware) y sistemas de seguridad informática. Está especializado en el análisis de riesgos, implementación de medidas de protección de datos y desarrollo de políticas de ciberseguridad. Además, posee experiencia en bases de datos (SQL, MongoDB), automatización y programación (Python, .NET, Java), así como en el tratamiento de imágenes geoespaciales. Como desarrollador de software, ha participado en el diseño y construcción de soluciones tecnológicas adaptadas a distintos entornos, integrando funcionalidades avanzadas y garantizando la calidad del código. Su enfoque combina rigor técnico, visión estratégica y capacidad para liderar equipos multidisciplinares en proyectos de transformación tecnológica, optimización de sistemas y mejora continua.

DATOS ESPECÍFICOS DE LA ASIGNATURA

DESCRIPTOR DE LA ASIGNATURA:

La creciente complejidad del software y su integración en entornos conectados exige no solo funcionalidades correctas, sino también garantías sólidas de seguridad desde las primeras fases del desarrollo. Esta asignatura introduce al estudiante en los principios, metodologías y buenas prácticas del desarrollo seguro de software, integrando la seguridad como componente transversal a lo largo del ciclo de vida del software (SDLC). Se abordarán técnicas de autenticación, autorización, cifrado, análisis de código, integridad de datos y auditoría, así como marcos de referencia como OWASP. A través de un enfoque práctico y aplicado, se enseñará cómo incorporar controles de seguridad en cada fase del ciclo de vida del software, incluyendo procesos de integración y entrega continua (CI/CD), con el objetivo de formar desarrolladores capaces de diseñar soluciones seguras desde el origen.

CONTENIDOS DE LA ASIGNATURA:

1. **Fundamentos del desarrollo seguro**: Se introduce el ciclo de vida seguro del software (SSDLC), sus principios y los elementos básicos para proteger la integridad y el acceso al sistema.
    1. Introducción al SSDLC y principios del desarrollo seguro: Se analiza el ciclo de vida del software desde una perspectiva de seguridad, destacando la importancia de integrar medidas preventivas desde las fases iniciales.
    2. Técnicas y modelos de codificación segura: Se estudian técnicas de diseño y codificación que minimizan vulnerabilidades, incluyendo el uso de patrones seguros y prácticas de validación temprana.
2. **Técnicas de protección y análisis de seguridad**: Este bloque presenta herramientas y técnicas para proteger la confidencialidad de los datos, auditar el comportamiento del sistema y revisar el código de forma automatizada.
    1. Cifrado y comunicaciones seguras: Se abordan los fundamentos del cifrado simétrico y asimétrico, así como los protocolos para proteger la transmisión de datos.
    2. Auditoría y análisis estático de código: Se exploran métodos para registrar y analizar eventos del sistema y herramientas de análisis estático que permiten detectar vulnerabilidades en el código fuente.
3. **Buenas prácticas, estándares y despliegue seguro**: El último bloque proporciona una visión práctica y actualizada de los marcos de referencia más utilizados, así como la integración de seguridad en entornos de desarrollo modernos.
    1. Buenas prácticas de desarrollo seguro y estándares OWASP: Se revisan las principales guías y buenas prácticas del desarrollo seguro, con especial énfasis en los estándares definidos por OWASP.
    2. Seguridad en entornos CI/CD: Se estudia cómo incorporar medidas de seguridad en los procesos de integración y entrega continua, garantizando la protección durante el ciclo de despliegue.

OBSERVACIONES CONTENIDO DE LA ASIGNATURA:

La asignatura está diseñada para que el estudiante adquiera una visión integral y aplicada del desarrollo seguro de software, integrando la seguridad desde las fases iniciales del ciclo de vida hasta su despliegue. Aunque no se requieren conocimientos previos en ciberseguridad, se recomienda familiaridad con programación y entornos de desarrollo. A lo largo del curso se abordan tanto conceptos fundamentales como técnicas específicas relacionadas con la autenticación, cifrado, integridad, análisis de código, auditoría y despliegue seguro. La estructura en bloques permite una progresión lógica, comenzando por los fundamentos, continuando con técnicas de protección, y finalizando con estándares y prácticas actuales como OWASP o la integración de seguridad en entornos CI/CD. La metodología combina teoría y práctica, fomentando la aplicación directa de los contenidos en escenarios reales del ámbito profesional.

RECURSOS DE APRENDIZAJE:

Las clases se desarrollan en laboratorio, combinando sesiones teóricas con ejercicios prácticos y simulaciones técnicas. Se emplean entornos de desarrollo integrados (IDE), herramientas de análisis de código estático, simuladores de autenticación y cifrado, y plataformas de virtualización para reproducir entornos controlados. Como parte del enfoque práctico, el alumnado dispone de **máquinas virtuales individuales alojadas en un servidor rack**, que permiten trabajar en entornos aislados, simular despliegues seguros y practicar configuraciones reales sin riesgo sobre los sistemas físicos.

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE A ADQUIRIR POR EL ALUMNO

COMPETENCIAS BÁSICAS:

- CB1. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio
- CB2. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
- CB5. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

COMPETENCIAS GENERALES:

- CG01. Capacidad de organización y planificación en el ámbito tecnológico
- CG02. Capacidad y habilidad para la toma de decisiones en el ámbito tecnológico

COMPETENCIAS ESPECÍFICAS:

- CI1. Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- Conocer técnicas de desarrollo seguro.
- Definir control de accesos e implementarlos
- Implementar comunicaciones seguras en los desarrollos de software
- Aplicar buenas prácticas a la hora de desarrollar el software

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- Paul Rascagneres (2016): Seguridad Informática y Malwares. Ediciones ENI. ISBN: 978-2-409-00549-7

BIBLIOGRAFÍA COMPLEMENTARIA:

- Caroline Wong (2020): Security Metrics: A Beginner's Guide. McGraw-Hill. ISBN: 978-0071744003
- Gary McGraw (2006): Software Security: Building Security In. Addison-Wesley. Addison-Wesley.. ISBN: 978-0321356703

WEBS DE REFERENCIA:

Web / Descripcion
OWASP(https://owasp.org/) Referente mundial en estándares y buenas prácticas de seguridad en aplicaciones.
MITRE ATT&CK Framework(https://attack.mitre.org/) Base de conocimiento sobre técnicas y tácticas de ciberataques, muy útil para simular amenazas y entender cómo prevenirlas.
Exploit Database(https://www.exploit-db.com/) Repositorio de vulnerabilidades reales, útil para ver cómo errores de programación pueden convertirse en fallos de seguridad explotables.

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

MÉTODO DIDÁCTICO:

El **método didáctico** se emplea principalmente en las sesiones expositivas, donde el docente presenta los contenidos teóricos mediante explicaciones estructuradas, apoyadas en ejemplos y resolución de ejercicios guiados.

MÉTODO DIALÉCTICO:

El **método dialéctico** se utiliza en la presentación, análisis y corrección de trabajos, promoviendo la participación activa del alumnado mediante el diálogo, la argumentación y el intercambio de ideas en un entorno crítico.

MÉTODO HEURÍSTICO:

El **método heurístico** se aplica en las actividades prácticas y proyectos, fomentando el aprendizaje autónomo, la investigación personal y la resolución de problemas reales, lo que permite al estudiante construir su propio conocimiento a partir de la experiencia.

CONSIDERACIONES DE LA PLANIFICACIÓN:

La asignatura se organiza en torno a diversas actividades formativas planificadas a lo largo del curso. Las **clases presenciales** se desarrollarán semanalmente y estarán orientadas, principalmente, mediante el **método didáctico o expositivo**, facilitando la comprensión de los contenidos teóricos a través de explicaciones estructuradas y ejemplos ilustrativos. El alumnado deberá realizar y entregar **trabajos prácticos** sobre temáticas específicas relacionadas con la asignatura, algunos de los cuales se presentarán en clase para su exposición y defensa, promoviendo así la participación activa y la argumentación técnica. Las **tutorías individuales** se llevarán a cabo en modalidad online, según el horario establecido en esta guía docente, con el fin de atender de forma personalizada las dudas o dificultades que puedan surgir. La **evaluación** de la asignatura se realizará mediante un sistema de evaluación continua, que combinará pruebas escritas parciales asociadas al programa teórico con la entrega de trabajos prácticos, garantizando así una valoración integral del aprendizaje adquirido.

PROGRAMACIÓN DE ACTIVIDADES Y EVALUACIONES:

PROGRAMACIÓN DE ACTIVIDADES:

Actividad	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	¿Se evalúa?	CO	CE
1ª actividad de evaluación continua y entrega de trabajos					X											X	X	X
2ª actividad de evaluación continua y entrega de trabajos										X						X	X	X
3ª actividad de evaluación continua y entrega de trabajos															X	X	X	X

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA ORDINARIA:

La asignatura se organiza mediante un sistema de evaluación continua, estructurado en tres bloques evaluables a lo largo del semestre. Cada bloque incluirá:

- **Una prueba escrita** (40% de la nota del bloque), compuesta por una parte teórica y una parte práctica, orientadas respectivamente a la comprensión conceptual y a la aplicación técnica de los contenidos. Para que esta prueba pueda computar en la media del bloque, será necesario obtener una calificación mínima de **4 puntos en ambas partes (teórica y práctica)**.
- **Un trabajo práctico** (40% de la nota del bloque), en el que el estudiante deberá desarrollar tareas aplicadas relacionadas con los contenidos trabajados en clase.
- **Una evaluación por observación continua** (20% de la nota global), basada en la asistencia y puntualidad, el respeto al profesorado, compañeros y recursos del aula, la participación activa, la actitud colaborativa y la capacidad de análisis y razonamiento crítico.

La calificación final de la asignatura se obtendrá como la media aritmética de las calificaciones obtenidas en los tres bloques evaluables, cada uno de los cuales representa un **33,3%** de la nota final, tanto en la evaluación continua como en la convocatoria ordinaria.

Para superar la asignatura, el estudiante deberá obtener una calificación mínima de **5 puntos en cada bloque**,

tanto en la prueba escrita como en el trabajo práctico. Se permite suspender una de las dos partes (prueba o trabajo) siempre que la calificación no sea inferior a 4 puntos y la media final del bloque sea igual o superior a 5 puntos. En caso contrario, deberá recuperar la parte o partes suspensas en la convocatoria ordinaria.

Para aprobar la asignatura en la **convocatoria ordinaria**, todas las partes recuperadas deben obtener una calificación mínima de 5. En caso contrario, el estudiante pasará a la convocatoria **extraordinaria**. Se recuerda al alumnado que las pruebas teóricas y prácticas tienen una duración máxima de **dos horas (en su conjunto)**, por lo que es fundamental gestionar adecuadamente el tiempo, especialmente si se deben recuperar varias partes en la misma convocatoria. Por todo ello, se recomienda encarecidamente superar la asignatura mediante la evaluación continua.

La **Matrícula de Honor** únicamente podrá obtenerse a través del sistema de evaluación continua, y estará reservada a quienes logren una calificación final de **10 (sobresaliente)** en este régimen. No será posible obtenerla mediante pruebas de recuperación, convocatorias ordinarias o extraordinarias, ni mediante procedimientos de subida de nota.

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA EXTRAORDINARIA:

En la **convocatoria extraordinaria**, el estudiante deberá realizar una **prueba única y global** que evalúe de forma completa los contenidos teóricos de la asignatura. Esta prueba escrita representará el **50% de la calificación final**.

El **otro 50%** corresponderá a la **entrega de los trabajos prácticos** asociados a los bloques temáticos. Para ello, se habilitará un nuevo plazo de entrega específico.

En esta convocatoria no se aplicarán técnicas de observación continua, dado el carácter no presencial o excepcional de algunas de las actividades. Por tanto, la calificación final se obtendrá únicamente a partir de los resultados de la **prueba teórica (50%)** y la **evaluación de trabajos prácticos (50%)**.

Para superar la asignatura será necesario obtener una **calificación mínima de 5 puntos sobre 10**, habiendo alcanzado al menos una nota de **5 en cada una de las dos partes** (prueba escrita y trabajos prácticos), conforme a los criterios establecidos.

SISTEMAS DE EVALUACIÓN:

SISTEMA DE EVALUACIÓN	PORCENTAJE (%)
Ejecución de prácticas	40%
Pruebas escritas	40%
Técnicas de observación	20%