



## FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Optativa Complementaria. Seguridad en Aplicaciones
Código	DTC-MCS-525
Título	<a href="#">Máster Universitario en Ingeniería de Telecomunicación por la Universidad Pontificia Comillas</a>
Impartido en	Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	4,5 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Telemática y Computación
Responsable	Rafael Palacios
Descriptor	Actualmente más del 80% de los ataques se realizan sobre software (principalmente sobre Web), esto implica que deba prestarse especial atención al desarrollo de software. Para ello, debemos entender los problemas desde fases iniciales en las que un Desarrollador codifica un algoritmo hasta su puesta en producción, haciéndose accesible a usuarios finales y hackers. Los nuevos paradigmas de Desarrollo, han propiciado la aparición de metodologías Agiles y de Organización para la construcción de Software Seguro, a la vez que se difunden principios sobre seguridad y bastionado. Por ello, debemos conocer el Ciclo de Vida del Desarrollo de Software (SDLC) y sus metodologías, así como los nuevos enfoques en DevSecOps. Finalmente, se verá cómo detectar (y mitigar) con herramientas automáticas y mediante experiencia (análisis manual) vulnerabilidades en código fuente.

Datos del profesorado	
<b>Profesor</b>	
Nombre	Carlos Manchado Martín
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	cmanchado@icai.comillas.edu
<b>Profesor</b>	
Nombre	Miguel Enrique de Vega Martín
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	medevega@icai.comillas.edu

## DATOS ESPECÍFICOS DE LA ASIGNATURA





## Contextualización de la asignatura

### Prerequisitos

Se recomienda saber programar al menos en un lenguaje, preferiblemente Java u cualquier todo Orientado a Objetos.

## Competencias - Objetivos

### Competencias

## BLOQUES TEMÁTICOS Y CONTENIDOS

### Contenidos – Bloques Temáticos

#### Temario

##### Teoría – SDLC y DevSecOps

1. Introducción a la Seguridad en Aplicaciones y SSDLC
2. Framework de Desarrollo Seguro – Modelo OWASP SAMM y MS DSL for Agile
3. Framework de Desarrollo Seguro – Modelo Estándar I
4. Framework de Desarrollo Seguro – Modelo Estándar II
5. DevSecOps y Seguridad en Contenedores
6. Metodología y Ciclos de Vida Software
7. Casos Prácticos

##### Práctica - Revisión de código y binarios

1. Introducción AppSec.
2. Visión general y controles clásicos.
3. Modelo ACIDA.
  - Autenticación.
  - Autorización.
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.
  - Auditabilidad.
4. Introducción al Desarrollo Seguro.
5. Gestión de sesiones.
6. Validación de Datos.
7. Otros controles de desarrollo seguro generales.
8. Tipos de auditoria de aplicaciones.
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
  - SAST vs DAST



9. Iniciar una auditoria.
10. Herramientas para auditar código.
11. Metodologías.
12. Revisión de código (SAST).
13. Revisión de dependencias (SCA).
14. Creación del Informe.
15. Introducción a Ingeniería inversa.
16. Ingeniería inversa en Java.
17. Ingeniería inversa en móviles.
  - o Ejemplo Aplicación Android.
  - o Ejemplo Aplicación iOS.
18. Ingeniería inversa sobre librerías.
19. Ingeniería inversa sobre binarios.

## METODOLOGÍA DOCENTE

### Aspectos metodológicos generales de la asignatura

## RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES

HORAS NO PRESENCIALES

CRÉDITOS ECTS: 4,5 (0 horas)

## EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

### Calificaciones

La asignatura está compuesta por 4,5 créditos, siendo el reparto:

- Teoría – SDLC y DevSecOps: 1,5 créditos.
- Práctica - Revisión de código y binarios: 3,0 créditos.

La evaluación se efectúa mediante un examen cada parte junto con un trabajo final, siendo el reparto:

- Teoría – SDLC y DevSecOps:
  - o Examen: 35% de la nota final.
- Práctica - Revisión de código y binarios:
  - o Examen: 35% de la nota final.
  - o Trabajo: 30% de la nota final.

## BIBLIOGRAFÍA Y RECURSOS

### Bibliografía Básica



# COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

**GUÍA DOCENTE  
2020 - 2021**

Las fuentes utilizadas durante el curso son los estándares de Seguridad tales como:

- OWASP
- NIST
- MITRE

En cumplimiento de la normativa vigente en materia de **protección de datos de carácter personal**, le informamos y recordamos que puede consultar los aspectos relativos a privacidad y protección de datos que ha aceptado en su matrícula entrando en esta web y pulsando "descargar"

<https://servicios.upcomillas.es/sedelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792>