



COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

GUÍA DOCENTE

2024 - 2025

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Optativa Complementaria: Monitorización, Detección y Análisis Forense
Código	DTC-MCS-524oc
Título	Máster Universitario en Ingeniería de Telecomunicación por la Universidad Pontificia Comillas
Impartido en	Máster Universitario en Ingeniería de Telecomunicación [Segundo Curso] Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [Segundo Curso]
Créditos	3,0 ECTS
Carácter	Optativa
Departamento / Área	Departamento de Telemática y Computación

Datos del profesorado	
Profesor	
Nombre	Agustín Valencia Gil-Ortega
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	avalencia@icai.comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura
Aportación al perfil profesional de la titulación
El objetivo es capacitar al alumno frente a las necesidades de perfiles profesionales para actividades de SOC, respuesta ante incidentes y Análisis Forense
Prerrequisitos
Conocimientos básicos de Máquinas Virtuales

Competencias - Objetivos	
Competencias	
GENERALES	
CB02	Saber aplicar e integrar sus conocimientos, la comprensión de éstos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados
CB07	Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio



CG08	Capacidad para la aplicación de los conocimientos adquiridos y resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinarios, siendo capaces de integrar conocimientos
------	---

Resultados de Aprendizaje

RA01	Aplicar e integrar conocimientos en un contexto multidisciplinar
RA02	Analizar y resolver problemas nuevos y definidos de forma imprecisa en un contexto multidisciplinar.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Monitorización y Detección

1.1. Monitorización

- Fundamentos de monitorización
- Generación de eventos: Linux
- Generación de eventos: Windows
- Generación de eventos: Agregación de otras Fuentes

1.2 Detección

- Detección de Intrusiones por red (NIDS) y en Host (HIDS)
- Reglas de Detección YARA, STIX-TAXII, SIGMA
- Repositorios

1.3 Correlación

- SIEM
- Fuentes Abiertas
- Respuesta a Incidentes
 - CyberKillChain
 - Mitre Att&ck Enterprise
 - Gestión de SOC
 - Herramientas de SOC (SOAR, email Gateway, EDR)

1.4 Enfoque Industrial

- Ataques
- Protocolos Industriales
- Mitre Att&CK ICS

Análisis Forense

2.1 Fundamentos y Primera Respuesta

2.2 Documentación: Acta de Ocupación, Cadena de Custodia, Hoja de Trabajo



2.3 Herramientas de Primera Respuesta

2.4 Análisis de Evidencias Digitales

2.5 Técnicas Avanzadas. Almacenamiento. Estudio a bajo nivel

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES	
Clase magistral y presentaciones generales	
24.00	
HORAS NO PRESENCIALES	
Trabajos de carácter práctico individual	
6.00	
CRÉDITOS ECTS: 3,0 (30,00 horas)	

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Calificaciones

Sistema de evaluación:

Monitorización (66.6% de la nota final)

- 60% Prácticas
- 40% Examen Final

Análisis Forense (33.3% de la nota final)

- 50% Prácticas, cumplimentación de documentos (Acta, bolsas de indicios, hojas de trabajo) y elaboración de Informe pericial.
- 50% Cuestiones planteadas antes de cada sesión (investigación individual y defensa) y Examen Final

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

MONITORIZACIÓN:

OSSIM: <https://cybersecurity.att.com/products/ossim>

Snort: <https://www.snort.org/>



Yara: <https://virustotal.github.io/yara/>

Sigma: <https://github.com/Neo23x0/sigma>

Sysinternals: <https://docs.microsoft.com/en-us/sysinternals/>

Ossec: <https://www.ossec.net/>

Wireshark: <https://www.wireshark.org/>

Censys: <https://censys.io/>

Shodan: <https://www.shodan.io/>

MISP: <https://www.misp-project.org/>

<https://oasis-open.github.io/cti-documentation/>

FORENSE:

SANS: <https://digital-forensics.sans.org/>

Forensic focus: <https://www.forensicfocus.com/>

Interpol: <https://www.interpol.int/How-we-work/Innovation>

Europol: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

ENFSI: <http://enfsi.eu/about-enfsi/structure/working-groups/information-technology/>

XDA developers: <https://www.xda-developers.com/>

NFI: <https://www.forensischinstituut.nl/>

Informes de evaluación de herramientas forenses: <https://www.dhs.gov/>

Estándares y metodologías USA: <https://www.nist.gov/>

Estándares ISO: <https://www.iso.org/>

Android: <https://developer.android.com/>

Autopsy: <https://www.sleuthkit.org/>

Ftk Imager: <https://accessdata.com/product-download/ftk-imager-version-4-2-0>

Nirsoft:

USBdview: https://nirsoft.net/utills/usb_devices_view.html

Launcher: <https://launcher.nirsoft.net/>

Volatility: <https://www.volatilityfoundation.org/>

Testdisk y photorec: https://www.cgsecurity.org/wiki/TestDisk_ES

Bibliografía Complementaria

Ciberseguridad Industrial e Infraestructuras Críticas

https://www.ra-ma.es/libro/ciberseguridad-industrial-e-infraestructuras-criticas_119432/

Herramientas comerciales:

<https://www.acelaboratory.com/>

<https://rusolut.com/>

<https://www.guidancesoftware.com/encase-forensic> (y Tableau).

<https://www.cellebrite.com/>

<https://www.magnetforensics.com/>

<https://www.msab.com/>

Distribuciones forenses:



COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

GUÍA DOCENTE
2024 - 2025

<https://sumuri.com/software/paladin/>

<https://sumuri.com/software/carbon/>

<https://www.caine-live.net/>

<https://digital-forensics.sans.org/community/downloads>

Otros:

<https://gsmserver.es/>

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](https://servicios.upcomillas.es/sedeelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792)