



FICHA TÉCNICA DE LA ASIGNATURA

| Datos de la asignatura | |
|------------------------|--|
| Nombre completo | Monitorización, Detección y Análisis Forense |
| Código | DTC-MCS-524 |
| Título | Máster Universitario en Ingeniería de Telecomunicación por la Universidad Pontificia Comillas |
| Impartido en | Máster en Ciberseguridad [Primer Curso] |
| Nivel | Master |
| Cuatrimestre | Semestral |
| Créditos | 3,0 ECTS |
| Carácter | Obligatoria |
| Departamento / Área | Departamento de Telemática y Computación |
| Descriptor | Familiarizar al alumno con los fundamentos en que se basan las herramientas de detección como los logs y eventos de Windows y Linux y el análisis de tráfico y su volcado. Establecer las bases sobre la herramientas el funcionamiento de los sistemas de monitorización, eventos e información de sistemas (SIEM), la aproximación específica para detección de intrusiones (IDS), y entender los mecanismos de correlación, generación o importación de reglas. También se abarcará la parte específica de sistemas industriales, tanto por la inclusión de monitorización con herramientas específicas en redes industriales como por el descubrimiento de herramientas específicas para fuentes abiertas. La parte forense incluirá tanto el entendimiento del forense relacionado con ámbito judicial (normativa, preservación de evidencias, cadena de custodia) como la familiarización con herramientas propias del analista forense para equipos informáticos (volcado de memoria, volcado de disco, análisis de evidencias) |

| 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 |
|--|
| Prerequisitos |
| Conocimientos y manejo de máquinas virtuales |



Competencias - Objetivos

Competencias

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 Fuentes
- Monitorización de tráfico

1.2 Detección

- Detección IDS
- Detección YARA y SIGMA
- Repositorios

1.3 Correlación

- Fuentes Abiertas
- Fuentes Externas
- Correlación SIEM

1.4 Enfoque Industrial

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, adquisición y análisis.

2.4 Análisis de evidencias digitales

2.5 Técnicas avanzadas. Almacenamiento. Estudio a bajo nivel

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Metodología Presencial: Actividades



- Lecciones en clase
- Prácticas de laboratorio

RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES

HORAS NO PRESENCIALES

CRÉDITOS ECTS: 3,0 (0 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:

Libros: Security Information and Event Management (SIEM) Implementation. McGrawHill. 2011. David R.Miller

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

IBM

Qradar:

https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_oview.html

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/>

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:

USBdeview: 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

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:

<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/>



COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

**GUÍA DOCENTE
2020 - 2021**

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>