**Programación didáctica del módulo: *Análisis Forense Informático***

***Ciclo formativo: Curso de Especialización de formación profesional en ciberseguridad en entornos de las tecnologías de la información***

**Curso: 2021/2022**

**Profesor: Carlos Martínez García**

Índice

[1.1 Criterios de evaluación 3](#_Toc53397302)

## Criterios de evaluación

Los criterios de evaluación, agrupados por resultados del aprendizaje, son los siguientes:

**1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.**

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.

b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.

c) Se ha asegurado la escena y conservado la cadena de custodia.

d) Se ha documentado el proceso realizado de manera metódica.

e) Se ha considerado la línea temporal de las evidencias.

f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.

g) Se han presentado y expuesto las conclusiones del análisis forense realizado.

**2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.**

Criterios de evaluación:

a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.

b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.

c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.

d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.

**3. Realiza análisis forenses en *Cloud*, aplicando metodologías establecidas, actualizadas y reconocidas.**

Criterios de evaluación:

a) Se ha desarrollado una estrategia de análisis forense en *Cloud*, asegurando la disponibilidad de los recursos y capacidades necesarios una vez ocurrido el incidente.

b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.

c) Se han realizado las fases del análisis forense en *Cloud*.

d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).

e) Se han cumplido los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y directiva *NIS* (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente pudieran sustituirlas.

f) Se han presentado y expuesto las conclusiones del análisis forense realizado.

**4. Realiza análisis forense en dispositivos del *IoT*, aplicando metodologías establecidas, actualizadas y reconocidas.**

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.

b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias

c) Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.

d) Se han realizado análisis de evidencias de manera manual y mediante herramientas.

e) Se ha documentado el proceso de manera metódica y detallada.

f) Se ha considerado la línea temporal de las evidencias.

g) Se ha mantenido la cadena de custodia

h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.

i) Se han presentado y expuesto las conclusiones del análisis forense realizado.

**5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.**

Criterios de evaluación:

a) Se ha definido el objetivo del informe pericial y su justificación.

b) Se ha definido el ámbito de aplicación del informe pericial.

c) Se han documentado los antecedentes.

d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.

e) Se han recogido los requisitos establecidos por el cliente.

f) Se han incluido las conclusiones y su justificación.