CONTENIDOS DE LA UNIDAD, CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE

La siguiente tabla responde al Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en Ciberseguridad en Entornos de las Tecnologías de la Información y se fijan los aspectos básicos del currículo, al Real Decreto 261/2021, de 13 de abril, por el que se modifican diversos reales decretos por los que se establecen cursos de especialización y los aspectos básicos del currículo y al Real Decreto 497/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen, en el ámbito de la Formación Profesional, cursos de especialización de grado medio y superior y se fijan sus enseñanzas mínimas. Se incluye también una columna con las unidades didácticas que forman el curso, en las que se desarrollan los diferentes bloques de contenidos.

CONTENIDOS	CRITERIOS DE EVALUACIÓN	RESULTADOS DE APRENDIZAJE	UNIDAD DIDÁCTICA
Bloque 1. Metodologías de análisis forense			
Aplicación de metodologías de análisis forenses: − Identificación de los dispositivos a analizar. − Recolección de evidencias (trabajar un escenario). − Análisis de la línea de tiempo (*TimeStamp*). − Análisis de volatilidad – Extracción de información (*Volatility*). − Análisis de *Logs*, herramientas más usadas.	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	1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.	UT01
Bloque 2. Realización de análisis forense			
Realización de análisis forenses en dispositivos móviles:	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.	2. Realiza análisis forenses en dispositivos móviles, aplicando	UT02

− Métodos para la extracción de evidencias. − Herramientas de mercado más comunes.	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.	metodologías establecidas, actualizadas y reconocidas.	
Realización de análisis forenses en *Cloud*: − Nube privada y nube pública o híbrida. − Retos legales, organizativos y técnicos particulares de un análisis en *Cloud*. − Estrategias de análisis forense en *Cloud*. − Realizar las fases relevantes del análisis forense en *Cloud*. − Utilizar herramientas de análisis en *Cloud* (*Cellebrite UFED Cloud Analizer, Cloud Trail, Frost, OWADE*, …).	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.	3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.	UT03
Realización de análisis forenses en *IoT*: − Identificar los dispositivos a analizar. − Adquirir y extraer las evidencias. − Analizar las evidencias de manera manual y automática. − Documentar el proceso realizado. − Establecer la línea temporal. − Mantener la cadena de custodia. − Elaborar las conclusiones. − Presentar y exponer las conclusiones.	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. 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.	4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.	UT04

Bloque 3. Informes de análisis forense			
Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe: − Hoja de identificación (título, razón social, nombre y apellidos, firma). − Índice de la memoria. − Objeto (objetivo del informe pericial y su justificación). − Alcance (ámbito de aplicación del informe pericial - resumen ejecutivo para una supervisión rápida del contenido y resultados). − Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales). − Normas y referencias (documentos y normas legales y reglamentos citados en los distintos apartados). − Definiciones y abreviaturas (definiciones, abreviaturas y expresiones técnicas que se han utilizado a lo largo del informe). − Requisitos (bases y datos de partida establecidos por el cliente, la legislación, reglamentación y normativa aplicables). − Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar a ellas, ventajas e	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.	5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.	UT05

inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación). – Anexos.			

Este módulo profesional contiene la formación necesaria para desempeñar la función de análisis forense.

La función de análisis forense incluye aspectos como el análisis de dispositivos de almacenamiento no volátil, de ficheros *Log*s, dispositivos móviles, *Cloud* e *IoT*.

Las actividades profesionales asociadas a esta función se aplican en la extracción de las evidencias para su análisis mediante la estrategia adecuada que garantice la disponibilidad de los recursos.

La formación del módulo contribuye a alcanzar los objetivos generales m), n), q), r), s), t), u) y v) y las competencias h), k), l), m), n) y ñ) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Las metodologías de análisis forense.
- Las herramientas de análisis forense.
- La toma de evidencias.
- El análisis de resultados.
- Los informes de resultados.
- Las fases del análisis *Cloud* y herramientas para llevarlo a cabo.
- La estrategia de análisis forense en *IoT*.