TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Análisis Forense Informático

RA1	Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.	Contenidos: Aplicación de metodologías de análisis forenses:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.	• Identificación de los dispositivos a analizar.	Contenidos Básicos	• Reconocer y asegurar el entorno del incidente	• Asegurar el entorno, no actuando hasta que no estén todos los 'protagonistas'
	b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.	• Recolección de evidencias (trabajar un escenario).		• Adecuar los procesos y herramientas a la situación: 'en vivo' versus apagados	• Establecer los procesos y herramientas en función del lugar donde se realicen: 'in situ' o laboratorio
	c) Se ha asegurado la escena y conservado la cadena de custodia.	• Recolección de evidencias (trabajar un escenario).		• Seguir los protocolos para asegurar la escena y establecer la cadena de custodia	• Determinar qué evidencias son susceptibles de clonarse y analizar en el escenario o no.
	d) Se ha documentado el proceso realizado de manera metódica.	• Análisis de volatilidad – Extracción de información (Volatility).		• Seguir los apartados previstos para un informe.	• Se elaboran informes correctamente
	e) Se ha considerado la línea temporal de las evidencias.	• Análisis de la línea de tiempo (TimeStamp).		• Cumplimentar adecuada y concienzudamente la línea de tiempo	• La documentación tiene todos los apartados y el formato correctos.
	f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.	• Análisis de Logs, herramientas más usadas.		• Observar todas la indicaciones y normalizaciones relacionadas con la elaboración de informes	• Los informes contienen toda la información requerida y necesaria, así como el formato adecuado
	g) Se han presentado y expuesto las conclusiones del análisis forense realizado.	• Análisis de Logs, herramientas más usadas.		• Exponer correcta y adecuadamente al objetivo perseguido	• Se establecen los formatos y parámetros adecuados para la audiencia

RA2	Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.	Contenidos: Realización de análisis forenses en dispositivos móviles.		Saber Hacer	Saber Estar
Criterios de	a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.	• Métodos para la extracción de evidencias.	Contenidos	• Adecuar los procesos y herramientas a la situación: 'en vivo' versus apagados	• Establecer los procesos y herramientas en función del lugar donde se realicen: 'in situ' o laboratorio

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Análisis Forense Informático

RA2	Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.	Contenidos: Realización de análisis forenses en dispositivos móviles.		Saber Hacer	Saber Estar
	b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.	• Métodos para la extracción de evidencias.		• Adecuar los procesos y herramientas a la situación: 'en vivo' versus apagados	• Establecer los procesos y herramientas en función del lugar donde se realicen: 'in situ' o laboratorio
	c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.	• Herramientas de mercado más comunes.		• Seguir los apartados previstos para un informe.	• Se elaboran informes correctamente
	d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.	• Herramientas de mercado más comunes.		• Exponer correcta y adecuadamente al objetivo perseguido	• Se establecen los formatos y parámetros adecuados para la audiencia

RA3	Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.	Contenidos: Realización de análisis forenses en Cloud		Saber Hacer	Saber Estar
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.	• Nube privada y nube pública o híbrida.	Contenidos Básicos	• Adecuar los procesos y herramientas a la situación.	• Establecer los procesos y herramientas en función de la accesibilidad.
	b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.	• Utilizar herramientas de análisis en Cloud (Cellebrite UFED Cloud Analizer, Cloud Trail, Frost, OWADE, …).		• Conseguir resultados aclaratorios utilizando las herramientas adecuadas.	• Se reconoce el entorno y las herramientas adecuadas. Identificando las posibilidades
	c) Se han realizado las fases del análisis forense en Cloud.	• Realizar las fases relevantes del análisis forense en Cloud.		• Analizar, utilizando procedimientos científicos, los datos obtenidos.	• Identifica las fases relevantes del análisis en Cloud.
	d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).	• Estrategias de análisis forense en Cloud.		• Reconocer las características del tipo de nube y sus	• Se elaboran estrategias analíticas adecuadas.

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Análisis Forense Informático

RA3	Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.	Contenidos: Realización de análisis forenses en Cloud		Saber Hacer	Saber Estar
				peculiaridades, documentando la información	
	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.	• Retos legales, organizativos y técnicos particulares de un análisis en Cloud.		• Comprobar que las actuaciones realizadas son respetuosas con la legislación vigente.	• Se analizan los procedimientos y conclusiones alcanzadas para que no se vulneres requisitos legales.
	f) Se han presentado y expuesto las conclusiones del análisis forense realizado.	• Realizar las fases relevantes del análisis forense en Cloud.		• Exponer correcta y adecuadamente al objetivo perseguido	• Se establecen los formatos y parámetros adecuados para la audiencia

RA4	Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.	Contenidos: Realización de análisis forenses en IoT.		Saber Hacer	Saber Estar
Cri	a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.	• Identificar los dispositivos a analizar.	Contenidos Básicos	• Reconocer y asegurar el entorno o los dispositivos involucrados en el incidente	• No actuando hasta que no estén todos los 'protagonistas'
	b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias	• Adquirir y extraer las evidencias.		• Aplicar los procesos y herramientas a la situación: 'en vivo' versus apagados	• Establecer los procesos y herramientas adecuados
	c) Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.	• Adquirir y extraer las evidencias. Garantizando su autenticidad (hash)		• Establecer los mecanismos adecuados para no modificar los datos	• Verificar antes y después la autenticidad de los datos.
	d) Se han realizado análisis de evidencias de manera manual y mediante herramientas.	• Analizar las evidencias de manera manual y automática.		• Verificar los datos y evidencias de 'visu' y utilizando herramientas automáticas.	• Validar las herramientas y contar con apoyo técnico si es necesario
	e) Se ha documentado el proceso de manera metódica y detallada.	• Documentar el proceso realizado.		• Seguir los apartados previstos para un informe.	• Se elaboran informes correctamente

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Análisis Forense Informático

	f) Se ha considerado la línea temporal de las evidencias	• Establecer la línea temporal.		• Cumplimentar adecuada y concienzudamente la línea de tiempo	• La documentación tiene todos los apartados y el formato correctos.
	g) Se ha mantenido la cadena de custodia	• Mantener la cadena de custodia.		• Se ha mantenido la cadena de custodia	• Se gestiona adecuadamente la cadena de custodia.
	h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.	• Elaborar las conclusiones.		• Observar las indicaciones relacionadas con la elaboración de informes	• Los informes contienen la información y el formato requeridos
	i) Se han presentado y expuesto las conclusiones del análisis forense realizado.	• Presentar y exponer las conclusiones.		• Exponer correcta y adecuadamente a	• Se establecen los formatos y parámetros adecuados

RA5	Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.	Contenidos: Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe		Saber Hacer	Saber Estar
Criteri	a) Se ha definido el objetivo del informe pericial y su justificación.	• Objeto (objetivo del informe pericial y su justificación).	Conte	• Definir e identificar el objetivo y alcance del informe pericial	• Se elabora al esquema (índice) del informe
	b) Se ha definido el ámbito de aplicación del informe pericial.	• Alcance (ámbito de aplicación del informe pericial-resumen ejecutivo para una supervisión rápida del contenido y resultados).		• Analizar y supervisar el informe y su adecuación al objetivo perseguido.	• Existen los elementos formales ajustados al ámbito de aplicación
	c) Se han documentado los antecedentes.	• Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales).		• Establecer y estudiar los antecedentes para determinar la adecuación del informe elaborado y las conclusiones.	• Están todos los aspectos formales necesarios para comprender los porqués y las conclusiones
	d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.	• Normas y referencias (documentos y normas legales y reglamentos citados en los distintos apartados).		• Contemplar todas las normas y referencias relacionadas con la elaboración de los informes.	• Los informes están adecuados a las normativas y referencias que los regulan.

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Análisis Forense Informático

	e) Se han recogido los requisitos establecidos por el cliente.	• Requisitos (bases y datos de partida establecidos por el cliente, la legislación, reglamentación y normativa aplicables).		• Aplicar los requisitos que el cliente ha establecido para la AFI y la elaboración de los informes	• Están contemplados en los informes los requisitos establecidos por el cliente.
	f) Se han incluido las conclusiones y su justificación.	• Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar a ellas, ventajas e inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación).		• Incluir de forma clara y resumida la conclusiones del informe pericial.	• El documento final contiene las conclusiones y la justificación