Ciberseguridad e informática forense

Número total de créditos ECTS	6	
Tipología	Optativa	
Organización temporal	Curso 4; Semestre 8	
Modalidad	Presencial y Virtual	
Idioma	Castellano	
Contenidos	• Introducción a la informática forense y peritaje informático • Ciberamenazas, riesgos, incidencias • Legalidad y regulación, informe y juicio • Análisis forense digital en sistemas operativos • Incident response y técnicas necesarias	
Resultados de aprendizaje TÍTULO	**Conocimientos y contenidos**	CC01 Comprender las implicaciones del Derecho como instrumento que sirve para regular las relaciones sociales en los marcos nacional e internacional CC02 Identificar los criterios derivados de la esencia del ordenamiento jurídico para aplicarlos en la resolución de conflictos jurídicos
	Habilidades y destrezas	HD10 Defender ideas y argumentos propios en un contexto profesional HD11 Trabajar en entornos multiculturales e internacionales en base al reconocimiento y el respeto a la diversidad
	Competencias	CP02 Desarrollar destrezas y habilidades para la elección de la estrategia correcta para la defensa de los derechos de los clientes, con pleno respeto a la ética y a la deontología profesional CP03 Asesorar jurídicamente a entidades públicas, privadas y particulares con la finalidad de solucionar todas las cuestiones jurídicas que se planteen en la práctica diaria CP05 Proyectar enfoques alternativos, buscar soluciones y generar valor en contextos complejos y cambiantes CP06 Actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional.
Resultados de aprendizaje MENCIÓN		
CPLT1 Analizar las indicencias del Derecho penal en el ámbito de la ciberseguridad CPLT2 Aplicar el derecho para resolver problemas jurídicos relacionados con el ámbito del LegalTech.		
Resultados de aprendizaje ASIGNATURA		
• Conocer las ciberamenazas, riesgos e incidencias, para dar una respuesta jurídica adecuada • Conocer la doctrina y buscar la jurisprudencia aplicable en la materia al caso en concreto para dar la mejor solución a la problemática planteada • Saber responder ante un incidente forense para detectar la entrada de ataques en el sistema de la empresa y configurar la estrategia más oportuna		

	Actividades formativas	**Horas totales**	
Modalidad Presencial	Clases Expositivas	38	
	Seminarios	2	
	Clases prácticas	18	
	Tutorías	12	
	Trabajo autónomo	76	
	Prueba de evaluación final	4	
	Total	**150**	
	Sistemas de evaluación	**MÍNIMO**	**MÁXIMO**
	Evaluación Final: prueba o examen presencial	60	60
	Resolución de problemas	10	30
	Estudio de casos - Proyectos	10	30
	Otras actividades de evaluación continua	0	10
	Total	**80**	**130**

Modalidad Virtual	**Actividades formativas**	**Horas totales**	
	Clases Expositivas Síncronas	18	
	Seminarios síncronos	2	
	Clases prácticas Síncronas	8	
	Actividades Dirigidas Asíncronas	30	
	Tutorías	12	
	Trabajo autónomo	76	
	Prueba de evaluación final	4	
	Total	**150**	
	Sistemas de evaluación	**MÍNIMO**	**MÁXIMO**
	Evaluación Final: prueba o examen virtual	60	60
	Resolución de problemas	10	30
	Estudio de casos - Proyectos	10	30
	Otras actividades de evaluación continua	0	10
	Total	**70**	**120**