

**Cumplimiento Normativo, Regulación y Estándares de la Ciberseguridad**

<b>Número total de créditos ECTS</b>	6	
<b>Tipología</b>	Obligatoria	
<b>Organización temporal</b>	Semestre 1	
<b>Modalidad</b>	Virtual	
<b>Idioma</b>	Castellano	
<b>Contenidos</b>	<ul style="list-style-type: none"> <li>• Normativas legales y límites éticos de las mismas.</li> <li>• Modelos organizativos.</li> <li>• Normativas y estándares europeos. <ul style="list-style-type: none"> <li>○ Familia ISO 2700X y su aplicación práctica.</li> <li>○ GDPR, casos de incumplimiento y sanciones.</li> <li>○ Directiva NIS2</li> </ul> </li> <li>• Normativas y estándares nacionales <ul style="list-style-type: none"> <li>○ Esquema Nacional de Seguridad, implementación en el sector público y privado.</li> <li>○ RGPD</li> </ul> </li> </ul>	
<b>Resultados de aprendizaje TÍTULO</b>	<b>Conocimientos y contenidos</b>	CC01 Interpretar de manera crítica los estándares y las normativas de ciberseguridad de mayor relevancia a nivel nacional, europeo e internacional. en contextos complejos, garantizando el cumplimiento y la eficacia de estos.
	<b>Competencias</b>	<p>CP02 Elaborar un informes técnicos, legales o ejecutivos, adecuados al público objetivo detallando las causas y consecuencias de un incidente informático haciendo uso de las evidencias obtenidas en la realización de un análisis forense.</p> <p>CP03 Implementar medidas y mecanismos de protección de datos personales conforme a la normativa de protección de datos vigente.</p> <p>CP05 Elaborar un plan integral de ciberseguridad para organizaciones, proponiendo mejoras a sus mecanismos de seguridad informática que atiendan a su naturaleza, recursos, fortalezas, debilidades y necesidades.</p>
<b>Resultados de aprendizaje ASIGNATURA</b>		
<ul style="list-style-type: none"> <li>• Preparar a una empresa para afrontar las pruebas de certificación de diferentes estándares o normativas, tanto nacionales como a nivel europeo.</li> <li>• Garantizar la seguridad de la información en entornos organizativos diversos, demostrando entendimiento de las implicaciones éticas y legales de la ciberseguridad</li> <li>• Monitorizar el cumplimiento de las políticas de seguridad informática definidas en una organización.</li> </ul>		

Actividades formativas	Horas totales
Clases expositivas síncronas	14
Recursos didácticos audiovisuales	8
Seminarios síncronos	2
Clases prácticas síncronas	6
Resolución de ejercicios, casos y proyectos	12
Prácticas de laboratorio asíncronas	4
<b>Trabajo autónomo</b>	<b>102</b>
<b>Prueba de evaluación final</b>	<b>2</b>
<b>Total</b>	<b>150</b>

Sistemas de evaluación	MÍNIMO	MÁXIMO
Evaluación final: prueba o examen virtual	60	60
Resolución problemas	10	30
Estudio casos / Proyectos	10	30
Otras actividades de evaluación continua	0	10
<b>Total</b>	<b>80</b>	<b>130</b>