

**ESTUDIO PROPIO: Máster en Ciberdefensa**

**CÓDIGO DEL PLAN DE ESTUDIOS: EH70**

**ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:**

CURSO	Obligatorios		Optativos		Prácticas Externas	Memoria/ Proyecto	Créditos
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	54	17				6	60
2º							
3º							
<b>ECTS TOTALES</b>	<b>54</b>	<b>17</b>				<b>6</b>	<b>60</b>

**PROGRAMA TEMÁTICO**

**ASIGNATURAS OBLIGATORIAS**

Curso	Código Asignatura	Denominación	Carácter OB/OP	Créditos totales	Breve descripción del contenido
1º	702210	BASES DE CIBERSEGURIDAD	OB	3	Principios básicos de la criptografía clásica y moderna y su aplicación a la seguridad de la información y de las comunicaciones.
1º	702211	INTRODUCCIÓN A LA CIBERDEFENSA	OB	3	Conceptos relacionados con la Ciberdefensa como antecedentes, ciberespacio, ciberterrorismo y ciberguerra, concepto operativo, capacidades Ciberdefensa y estrategias.
1º	702212	ASPECTOS LEGALES, POLÍTICOS Y ÉTICOS DEL CIBERESPACIO	OB	3	Aspectos Legales, Políticos y Éticos del Ciberespacio relacionados con las operaciones en el citado dominio.
1º	702213	ASPECTOS DOCTRINALES. PLANEAMIENTO DE OPERACIONES	OB	3	Aplicación de la doctrina militar a Ciberdefensa y su adaptación al ciberespacio y el planeamiento de operaciones en el ciberespacio.
1º	702214	CIBERAMENAZAS A LA INFRAESTRUCTURAS CRÍTICAS	OB	3	Estudio de las Ciberamenazas a las infraestructuras críticas y los sistemas de control industrial que las controlan.
1º	702215	EXPERIMENTACIÓN EN CIBERDEFENSA (CD&E)	OB	3	Estudio metodología experimentación: Desarrollo de Conceptos y Experimentación (CD&E) aplicada a la Ciberdefensa
1º	702216	ANÁLISIS DE RIESGOS ESTÁTICO Y DINÁMICO	OB	3	Estudio de metodologías de análisis de riesgo de una organización y evaluación del mismo de una forma dinámica.
1º	702217	DETECCIÓN Y DEFENSA FRENTE A AMENAZAS CIBERNÉTICAS	OB	3	Capacidades de carácter defensivo que comprende la Ciberdefensa: detección y correlación de eventos y protección.
1º	702218	RESPUESTA A INCIDENTES. ANÁLISIS FORENSE	OB	3	Conceptos relacionados con los modelos organizativos, misión, competencias y catálogo de servicios de un CSIRT y el análisis forense de los incidentes de seguridad.
1º	702219	ANÁLISIS DE MALWARE	OB	3	Estudio de los diferentes tipos de malware, sistemas de obtención del mismo y una metodología de análisis de malware.
1º	702220	RECUPERACIÓN Y ANÁLISIS DE DATOS	OB	3	Estudio diferentes técnicas de recuperación frente a ciberataques, el concepto de sistemas resilientes y técnicas de fusión y análisis de datos aplicadas a Ciberdefensa.
1º	702221	CONCIENCIA DE LA SITUACIÓN Y COMPARTICIÓN INFORMACIÓN	OB	3	Aspectos relacionados con las siguientes actividades de inteligencia: conciencia de la situación y colaboración y compartición de información de Ciberdefensa
1º	702222	CIBERINTELIGENCIA Y FUENTES ABIERTAS	OB	3	Conceptos relacionados con las actividades de inteligencia aplicada a la Ciberdefensa, su integración en el proceso de planeamiento operacional y OSINT.

1º	702223	AMENAZAS AVANZADAS PERSISTENTES (APT'S)	OB	3	Estudio de los aspectos relacionados con la actividad de obtención de información a través de ciberarmas como las APT.
1º	702224	HACKING ÉTICO	OB	6	Estudio metodología de test de penetración y el uso de plataformas de explotación y uso automatizado de ataques cibernéticos.
1º	702225	ATAQUES DE DENEGACIÓN DE SERVICIO	OB	3	Estudio de los ataques de denegación de servicio destinados a eliminar total o parcialmente un ordenador o servicio.
1º	702226	INGENIERÍA SOCIAL	OB	3	Estudio de los aspectos fundamentales en los que se basa la ingeniería social y su aplicación a Ciberdefensa.
<b>MEMORIA/PROYECTO</b>					
Curso	Código Asignatura	Denominación	Carácter OB/OP	Créditos totales	Breve descripción del contenido
1º	702227	TRABAJO FIN DE MÁSTER	OB	6	Trabajo Final para poner en práctica las competencias adquiridas en las asignaturas.

Carácter: OB – Obligatoria; OP - Optativa