DOBLE GRADO EN DERECHO Y ESTUDIOS JURÍDICO MILITARES
CURSO 2026-2027

Asignatura	**Inteligencia, ciberdefensa y seguridad de la información en el ámbito militar**	**Código**	902414
		Versión	Mayo 2025
Módulo	Derecho Militar	**Materia**	
Créditos	6 ECTS	**Presenciales**	2,5
		No presenciales	3,5
Curso	Cuarto	**Semestre**	Primero

PROFESORADO, GRUPOS Y HORARIOS

Departamento Responsable	Derecho Internacional, Eclesiástico y Filosofía del Derecho	
Profesor Coordinador	**E-mail**	**Despacho**
José Antonio Perea Unceta	japereau@ucm.es	119

Grupo	Horario	Aula	Profesor	E-mail	Tutoría/ Despacho

Los grupos, horario, aula y profesor pueden consultarse a través de la página Web de la Facultad de Derecho, en la sección correspondiente a Alumnos, Información Académica y en el enlace Horarios del curso Académico:
https://derecho.ucm.es/informacion-academica.

EXÁMENES

Convocatoria	Fecha

Ordinarias y Extraordinaria	Las que determine el Decanato en cada convocatoria conforme al calendario oficial de exámenes. Se publican en la WEB de la Facultad de Derecho (Alumnos-Información académica): https://derecho.ucm.es/informacion-academica.

SINOPSIS

BREVE DESCRIPTOR

Esta asignatura de "INTELIGENCIA, CIBERDEFENSA Y SEGURIDAD DE LA INFORMACIÓN EN ELÁMBITO MILITAR" contempla la regulación y organización de la seguridad militar de las nuevas tecnologías, en las comunicaciones, en los datos, en las redes sociales y en relación con las infraestructuras esenciales, con la detección de as amenazas para la seguridad nacional y la determinación de los organismos públicos de ciberseguridad en el ámbito del Ministerio de Defensa, la UE y la OTAN.

CONOCIMIENTOS PREVIOS RECOMENDADOS

Se recomienda para cursar esta asignatura haber estudiado Derecho Internacional Público, Instituciones Internacionales para la Seguridad, la Defensa y el Mantenimiento de la Paz y también Régimen de la Acción Exterior de Seguridad, Defensa y Mantenimiento de la Paz.

OBJETIVOS FORMATIVOS

OBJETIVOS (Resultados de Aprendizaje)

El objetivo general de la asignatura es conseguir que el alumnado conozca el marco jurídico en el cual se desenvuelve la seguridad de las TICS, así como que perciba la transformación social y jurídica de la seguridad en las redes, sistemas inalámbricos y de telefonía móvil; que comprenda la relación entre seguridad informática y seguridad de la información; que conozca las técnicas para la protección de documentos y datos a través de cifras y códigos; que obtenga una visión general del catálogo de delitos relacionados con la ciberdelincuencia; que domine el lenguaje técnico en materia de ciberseguridad e inteligencia tanto en la redacción de escritos como en expresiones orales; que analice los problemas que conlleva la seguridad de la información, de manera que permita la aplicación de medidas de seguridad en el tratamiento de datos; que conozca las medidas de seguridad en equipos informáticos, redes sociales y sistemas de comunicación por redes

inalámbricas; y que identifique las infraestructuras del Estado y de los Organismos que velan por su seguridad.

COMPETENCIAS

Básicas:

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Generales:

CG1 - Conocer y comprender los elementos, estructura, recursos, interpretación y aplicación del ordenamiento jurídico miliar e interpretar las fuentes y los conceptos jurídicos fundamentales de cada uno de los distintos órdenes jurídicos y su aplicación en el ámbito militar.

CG2 - Conocer y comprender los mecanismos y procedimientos de resolución de los conflictos jurídicos, así como la posición jurídica de las personas en sus relaciones con la Administración y en general con los poderes públicos. Especialmente en su relación con las Fuerzas Armadas.

CG3 - Conocer y saber aplicar los criterios de prelación de las fuentes para determinar las normas aplicables en cada caso, y en especial el de la conformidad con las reglas, los principios y los valores constitucionales en el seno de la actividad desarrollada por las Fuerzas Armadas.

CG4 - Interpretar textos jurídicos desde una perspectiva interdisciplinar utilizando los principios jurídicos y los valores y principios sociales, éticos y deontológicos como herramientas de análisis.

CG5 - Pronunciarse con una argumentación jurídica convincente sobre una cuestión teórica relativa a las diversas materias jurídicas.

CG6 - Resolver casos prácticos conforme al Derecho positivo vigente, lo que implica la elaboración previa de material, la identificación de cuestiones

problemáticas, la selección e interpretación del dato de Derecho positivo aplicable y la exposición argumentada de la subsunción.

CG7 - Manejar con destreza y precisión el lenguaje jurídico y la terminología propia de las distintas ramas del derecho: Redactar de forma ordenada y comprensible documentos jurídicos. Comunicar oralmente y por escrito ideas, argumentaciones y razonamientos jurídicos usando los registros adecuados en cada contexto.

CG8 - Utilizar las tecnologías de la información y las comunicaciones para la búsqueda y obtención de información jurídica (bases de datos de legislación, jurisprudencia, bibliografía, etc.), así como herramientas de trabajo y comunicación.

CG9 - Comprender las distintas formas de creación del Derecho en su evolución histórica y en su realidad actual, con especial referencia al ámbito militar.

Transversales:

CT1 - Capacidad de análisis y síntesis.

CT2 - Capacidad de análisis crítico, pudiendo sostener puntos de vista personales sobre la información y criterios de validación de argumentos procedentes de un ámbito especializado.

CT3 - Capacidad de planificación, organización y trabajo autónomo.

CT4 - Capacidad de transmisión de información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CT5 - Capacidad de comunicación oral y escrita en castellano como un usuario competente.

CT6 - Aplicación de los conocimientos adquiridos a la formulación y defensa de argumentos y a la resolución de problemas.

CT7 - Capacidad de buscar, seleccionar y aprovechar la información disponible sobre una cuestión objeto de estudio, con la ayuda de todos los recursos disponibles.

CT8 - Capacidad de jerarquizar la información y en general, reconocer los argumentos de autoridad científica.

CT9 – Capacidad de organizar un grupo de trabajo, distribuir las tareas y poner en común los resultados, desde el respeto y el espíritu cooperativo.

Específicas:

CE40 - Capacidad para resolver problemas relacionados con seguridad de las TICS en atención a las funciones encomendadas a las

Fuerzas Armadas

CONTENIDOS TEMÁTICOS

(Programa de la asignatura)

1. Conceptos básicos y marco jurídico en el que se desenvuelve la seguridad de la información.

· Concepto de inteligencia en las FAS. La inteligencia en redes digitales. Ámbito normativo.

· La seguridad informática y la seguridad de la información.

· La ciberdefensa, ataques y amenazas cibernéticas, mecanismos y protocolos de seguridad.

2. Criptografía y sistemas de autenticación en las FAS.

· Criptografía, autenticación de sistemas informáticos, uso de claves, firma digital y certificado digital.

· Protección de datos personales.

3. La ciberdelincuencia.

· Gobernanza del ciberespacio. Amenazas y desafíos.

· Ciberdelitos, ciberataques y contramedidas.

· Nuevas amenazas tecnológicas.

· Amenazas informáticas a la Seguridad Nacional.

4. Seguridad en las redes, sistemas inalámbricos de telefonía móvil y sistemas de información.

· Seguridad en redes inalámbricas.

· Política de seguridad en las FAS.

· Auditorías de seguridad.

· Amenazas de seguridad del software: copia de seguridad.

5. Organismos públicos de ciberseguridad en el ámbito del Ministerio de Defensa, la UE y la OTAN.

· Red de emergencias.

· Agencia Europea de Seguridad de las redes y de la información.

· Mando Conjunto de Ciberdefensa.

· Centro de Ciberdefensa de la OTAN.

· Centro Nacional de Protección de Infraestructuras críticas.

ACTIVIDADES FORMATIVAS

Clases Teóricas	Dedicación	65%
Las clases teóricas pueden exigir preparación previa por parte del alumno		
Clases Prácticas	Dedicación	30%
Otras Actividades	Dedicación	5%
EVALUACIÓN		
Exámenes	Participación en la Nota Final	70%
Otra actividad	Participación en la Nota Final	30%
Participación activa en las clases teóricas, actividades prácticas, seminarios y trabajos		
CRITERIOS DE EVALUACIÓN		
La adquisición de conocimientos por el estudiante será evaluada en un 70% mediante la realización de una o varias pruebas de examen de carácter teórico (oral o escrito). El restante 30% de la calificación global corresponderá a las calificaciones obtenidas en las actividades prácticas, así como a la valoración de su participación activa en las clases teóricas y en su caso de la asistencia y aprovechamiento de conferencias y seminarios y la realización de trabajos. En las actividades prácticas, seminarios y trabajos se tendrá en cuenta especialmente la capacidad de argumentación jurídica, el dominio de la comunicación oral y escrita, el manejo de los conocimientos normativos y jurisprudenciales y su aplicación a la resolución de las concretas cuestiones planteadas, y en su caso el trabajo en equipo. El sistema de calificación será numérico, siguiendo al efecto lo previsto en el Real Decreto 1125/2003 y, en consecuencia, aplicando la siguiente escala: de 0 a 4,9, suspenso; de 5 a 6,9, aprobado; de 7 a 8,9, notable; de 9 a 10 sobresaliente. La mención “Matrícula de Honor” podrá ser otorgada por el profesor entre los alumnos que hayan obtenido una calificación igual o superior a 9 en los porcentajes previstos en la normativa en vigor.		

CRONOGRAMA

Conforme a la programación docente aprobada para cada curso académico, se imparten cuatro horas a la semana de clases durante quince semanas, a razón de dos días a la semana, entre los meses de septiembre y enero, en turno de mañana o de tarde. En ese calendario se programan por cada profesor las actividades prácticas y, en su caso, uno o varios exámenes parciales, y, en cualquier caso, tras la finalización de este período docente -en la fecha designada por Decanato- el examen ordinario y el extraordinario.

RECURSOS

BIBLIOGRAFÍA BÁSICA

Sobre la base de esta bibliografía cada profesor recomendará las obras que estime oportunas, en sus últimas ediciones:

- Bermejo García, R. y Díaz López-Jacoiste, E.,*La ciberseguridad a la luz del Jus ad bellum y del Jus in bello*, Universidad de Navarra.
- Martínez Atienza, G., *Ataques en el Ciberespacio: conflictos armados y seguridad nacional*, Ed. Experiencia
- Robles Carrillo, M., *El modelo digital europeo*, Tirant Lo Blanch
- Segura Serrano, A., *El desafío de la ciberseguridad global: análisis desde el Derecho internacional y europeo*, Tirant Lo Blanch
- VV.AA., Normativa de ciberseguridad, Paraninfo
- VV.AA., *Ciberataques y ciberseguridad en la escena internacional*, Aranzadi

BIBLIOGRAFÍA COMPLEMENTARIA

En función de la materia a estudiar, cada profesor especificará, en su caso, para cada lección del programa aquella bibliografía complementaria que resulte de interés para el alumno.

OTROS RECURSOS

Cada profesor detallará, en su caso, la posible utilización, entre otros, de los siguientes recursos: Campus Virtual, bases de datos formativos y jurisprudenciales, páginas web y revistas y publicaciones periódicas de especial interés para la asignatura.