24-25

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO

CÓDIGO 3110910-

UNED

24-25

MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO

CÓDIGO 3110910-

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN
REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA
EQUIPO DOCENTE
HORARIO DE ATENCIÓN AL ESTUDIANTE
COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE
RESULTADOS DE APRENDIZAJE
CONTENIDOS
METODOLOGÍA
SISTEMA DE EVALUACIÓN
BIBLIOGRAFÍA BÁSICA
BIBLIOGRAFÍA COMPLEMENTARIA
RECURSOS DE APOYO Y WEBGRAFÍA
IGUALDAD DE GÉNERO

Nombre de la asignatura	MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO
Código	3110910-
Curso académico	2024/2025
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Esta asignatura optativa se imparte en el segundo cuatrimestre del Master. En ella, a partir de la configuración legal de la Defensa Nacional como un componente fundamental de la más amplia Seguridad Nacional y de la consideración que, como ámbito de especial interés, se ha atribuido a la ciberseguridad, se abordará el régimen jurídico a que se encuentra sometida la actuación de los Estados en el ciberespacio, con especial énfasis en lo que respecta a la aplicación de las normas internacionales atinentes al uso de la fuerza armada en el ciberespacio y a la conducción de las ciberhostilidades.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Los necesarios para cursar el Master.

EQUIPO DOCENTE

Nombre y Apellidos	LAURA DELGADO CARRILLO
Correo Electrónico	laura.delg@der.uned.es
Teléfono	91398-6146
Facultad	FACULTAD DE DERECHO
Departamento	DERECHO PENAL Y CRIMINOLOGÍA

COLABORADORES DOCENTES EXTERNOS

Nombre y Apellidos	JERONIMO DOMINGUEZ BASCOY
Correo Electrónico	

HORARIO DE ATENCIÓN AL ESTUDIANTE

Prof. Laura Delgado Carrillo:

•Correo electrónico: laura.delg@der.uned.es

•Teléfono: 91398-6146

•Horario de tutoría: Despacho 3.48 (martes de 15'00h a 19'00h o cita previa).

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS BÁSICAS

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades. sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

COMPETENCIAS TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

COMPETENCIAS ESPECÍFICAS

CE9 - Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.

CE10 - Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

RESULTADOS DE APRENDIZAJE

·Conocer la regulación básica de la ciberseguridad dentro del marco normativo del sistema español de Seguridad Nacional.
·Conocer la específica regulación y organización de la ciberdefensa militar.
·Conocer las singularidades de la aplicación en el ciberespacio de los principios generales del Derecho internacional público.
·Conocer las diferentes posiciones mantenidas en torno a cómo se aplican en el ciberespacio las normas internacionales relativas al uso de la fuerza armada.
·Conocer los aspectos fundamentales que presenta la aplicación del Derecho Internacional de los Conflictos Armados a las operaciones conducidas en y a través del ciberespacio.

CONTENIDOS

I. La ciberseguridad dentro del Sistema de Seguridad Nacional: normativa, documentos estratégicos y organización.

II. El componente militar de la ciberseguridad en España: el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas

III. Aplicación de los principios de soberanía, diligencia debida, jurisdicción y responsabilidad internacional en el ciberespacio. IV. Ciberespionaje y Derecho internacional público:

V. El "ius ad bellum" en el ciberespacio. Uso de la fuerza armada en el ciberespacio: prohibición general y excepciones. VI. El "ius in bello" en el ciberespacio: aplicación del Derecho Internacional de los Conflictos Armados a las operaciones conducidas en y a través del ciberespacio.

VII. Procesos en el marco de las Naciones Unidas en relación con el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional: últimos informes del Group of Governmental Experts (GGE) y del Open-Ended Working Group (OEWG).

METODOLOGÍA

La docencia de esta asignatura se desarrollará de octubre a febrero. El estudiante debe estudiar los materiales básicos de la asignatura y consultar sus dudas, comentarios, etc con el profesorado a través de la plataforma aLF de la UNED, así como mediante contacto personal individualizado cuando así se considere necesario, en los horarios de tutoría.
El tiempo de las actividades formativas, siguiendo la anterior metodología, se han distribuido de forma orientativa de la siguiente manera:

•Estudio de los contenidos teóricos-prácticos utilizando la bibliografía y los materiales complementarios: 100 horas.

•Tutorías: 14 horas.

•Otras actividades y consulta de dudas en la plataforma virtual: 14 horas.

•Trabajos: 20 horas

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen tipo test
Preguntas test	20
Duración del examen	120 (minutos)

Material permitido en el examen

Ninguno.

Criterios de evaluación

La prueba presencial consistirá en la realización de un test de 20 preguntas. Cada una de las preguntas tendrá 3 posibles respuestas, de las que solo una será correcta. Cada pregunta respondida correctamente puntuará 0,5; cada respuesta errónea descontará 0,2; las preguntas que no se contesten no descontarán puntuación.

% del examen sobre la nota final	60
Nota del examen para aprobar sin PEC	5
Nota máxima que aporta el examen a la calificación final sin PEC	10
Nota mínima en el examen para sumar la PEC	5

Comentarios y observaciones

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	Si

Descripción

La prueba presencial consistirá en la realización de un test de 20 preguntas. Cada una de las preguntas tendrá 3 posibles respuestas, de las que solo una será correcta. Cada pregunta respondida correctamente puntuará 0,5; cada respuesta errónea descontará 0,2; las preguntas que no se contesten no descontarán puntuación.

La prueba tendrá una duración de 120 minutos.

Para superar la asignatura es necesario obtener un mínimo de 5 en la prueba presencial.

Criterios de evaluación

La prueba presencial consistirá en la realización de un test de 20 preguntas. Cada una de las preguntas tendrá 3 posibles respuestas, de las que solo una será correcta. Cada pregunta respondida correctamente puntuará 0,5; cada respuesta errónea descontará 0,2; las preguntas que no se contesten no descontarán puntuación.

Ponderación de la prueba presencial y/o los trabajos en la nota final: 60% de la nota final

Fecha aproximada de entrega

Comentarios y observaciones

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?: Si,PEC no presencial

Descripción

La pruebas de evaluación continua (PEC) forma parte de la actividad formativa del estudiante. Su realización permitirá que éste evalúe el avance de su proceso de aprendizaje y podrá incidir en la calificación final.

La prueba consistirá en la realización de varias preguntas tipo test, propuestas a partir de un supuesto práctico, texto, fragmento de resolución, etc. Se comunicará oportunamente su contenido a través de la plataforma, que versará sobe la materia de la asignatura.

La realización de esta actividad es voluntaria.

La PEC es una prueba no presencial. Se realizará en la plataforma el día y hora que el equipo docente de la asignatura determinará. Fuera de la plataforma virtual no es posible realizar las PEC.

Criterios de evaluación

La PEC será valorada con un máximo de 4 puntos: los aciertos sumarán 0'4 puntos y los fallos descontarán 0'1 puntos; las preguntas que no se contesten no descontarán puntuación.

Ponderación de la PEC en la nota final: La PEC serviá SOLO para subir la nota del examen final correspondiente siempre que se den los siguientes requisitos: · Calificación de la PEC: Se debe aprobar la PEC, esto es, se debe obtener un mínimo de 2 puntos sobre los 4 posibles; y · Nota de corte en la prueba presencial: Es preciso alcanzar en la prueba presencial correspondiente al menos 5 puntos de los 10 posibles.

Fecha aproximada de entrega: Mediados de mayo

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s? No

Descripción

Criterios de evaluación

Ponderación en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

La calificación final de la asignatura se realizará teniendo en cuenta las siguientes posibilidades:

A) Si únicamente se realiza la prueba presencial:

Si el estudiante decide no realizar la evaluación continua, la calificación final de la asignatura será la nota la prueba presencial.

B) Si se opta por la realización de la PEC:

Si el estudiante opta por la evaluación continua y realiza la PEC, la calificación final de la asignatura será la suma de la PEC y la nota de la prueba presencial (máximo 10).

BIBLIOGRAFÍA BÁSICA

Atendiendo a los diversos contenidos en que se encuentra organizada la asignatura, la bibliografía será la que a continuación se indica para cada uno de ellos.

I. La ciberseguridad dentro del Sistema de Seguridad Nacional: normativa, documentos estratégicos y organización: Se preparará sobre los siguientes textos normativos y documentos oficiales de carácter estratégico:

a) La Estrategia de Ciberseguridad de la UE para la Década Digital (2020), accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020JC0018&from=EN

b) Estrategia de Seguridad Nacional 2021 (apartados sobre “Transformación digital” del Capítulo 1; sobre “Amenazas a las infraestructuras críticas”, “Espionaje e injerencias desde el exterior”, “Campañas de desinformación” y “Vulnerabilidad del ciberespacio” del Capítulo 3; “Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior” y “Seguridad de los espacios comunes globales –Ciberespacio” del Capítulo 4), accesible en: https://www.boe.es/boe/dias/2021/12/31/pdfs/BOE-A-2021-21884.pdf

c) Estrategia Nacional de Ciberseguridad 2019, accesible en: https://www.boe.es/eli/es/o/2019/04/26/pci487/dof/spa/pdf

d) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2), accesible en:
https://www.boe.es/doue/2022/333/L00080-00152.pdf
e) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (por el que se traspone la Directiva (UE) 2016/1148 al ordenamiento jurídico español), accesible en:
https://www.boe.es/boe/dias/2018/09/08/pdfs/BOE-A-2018-12257.pdf
f) Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, accesible en:
https://www.boe.es/buscar/act.php?id=BOE-A-2021-1192
g) Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, accesible en:
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389
h) Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad, accesible en:
https://www.boe.es/buscar/act.php?id=BOE-A-2018-799

II. El componente militar de la ciberseguridad en España: el Mando Conjunto del Ciberespacio: Se preparará a partir de la información contenida en su página web (https://emad.defensa.gob.es/unidades/mcce/) y de la lectura de los siguientes textos:
a) La Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa [preámbulo y artículos 9 y 11 (solo en lo que respecta al Mando Operativo Ciberespacial)]:
https://www.boe.es/buscar/act.php?id=BOE-A-2020-8638
b) Concepto de Ciberdefensa del JEMAD, de 28 de septiembre de 2018 (resumen ejecutivo), accesible a través del siguiente enlace:
https://emad.defensa.gob.es/prensa/noticias/2018/10/listado/181023_Concepto_de_Ciberdefensa.html
c) Allied Joint Publication 3.20: “Allied Joint Doctrine for Cyberspace Operations”, publicación de la OTAN que hemos incorporado como doctrina nacional:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

III. Aplicación de los principios de soberanía, diligencia debida, jurisdicción y responsabilidad internacional en el ciberespacio (comparte enlaces con el apartado IV).

IV. Ciberespionaje y Derecho internacional público:

Aunque la obra de referencia sobre los contenidos a que se refieren estos dos apartados III y IV la constituye la Parte I del *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"* (Cambridge University Press, 2017), los mismos pueden prepararse mediante la lectura de los siguientes artículos, accesibles a través de los enlaces que se indican:

a) THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS (Eric Talbot Jensen), publicado en el Vol. 48 del GEORGETOWN JOURNAL OF INTERNATIONAL LAW: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

b) THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS (Harriet Moynihan), Research Paper de la Chatham House: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

c) REVISITING PAST CYBER OPERATIONS IN LIGHT OF NEW CYBER NORMS AND INTERPRETATIONS OF INTERNATIONAL LAW: INCHING TOWARDS LINES IN THE SAND? (Dennis Broeders, Els de Busser, Fabio Cristiano &Tatiana Tropina), publicado en el vol. 7.1 del Journal of Cyber Policy: https://www.tandfonline.com/doi/epdf/10.1080/23738871.2022.2041061?needAccess=true&role=button

d) THE INTERNATIONAL LEGAL REGULATION OF STATE-SPONSORED CYBER ESPIONAGE (Russell Buchan), publicado en White Rose Research Online: http://eprints.whiterose.ac.uk/98791/10/Russell_The%20International%20Legal%20Regulation%20of%20Cyber%20Espionage%20_comments%20combined.pdf

V. El "ius ad bellum" en el ciberespacio. Uso de la fuerza armada en el ciberespacio: prohibición general y excepciones (comparte enlaces con el apartado VI).

VI. El "ius in bello" en el ciberespacio: aplicación del Derecho Internacional de los Conflictos Armados a las operaciones conducidas en y a través del ciberespacio:

Las Partes III y IV del citado *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"* constituyen la obra de referencia para quienes deseen adentrarse en profundidad en estas materias. No obstante, a los fines de preparación de asignatura, bastará con la información contenida en los siguientes artículos:

a) THE LAW OF CYBER WARFARE: QUO VADIS? (Michael N. Schmitt), publicado en el Vol. 25 de la STANFORD LAW &POLICY REVIEW: Accesible a través de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320755

b) PEACETIME CYBER RESPONSES AND WARTIME CYBER OPERATIONS UNDER INTERNATIONAL LAW: AN ANALYTICAL VADE MECUM (Michael N. Schmitt), publicado en el Vol. 8 del HARVARD NATIONAL SECURITY JOURNAL:

https://ore.exeter.ac.uk/repository/bitstream/handle/10871/28179/Schmitt-NSJ-Vol-8.pdf?sequence=5&isAllowed=y

c) TWENTY YEARS ON: INTERNATIONAL HUMANITARIAN LAW AND THE PROTECTION OF CIVILIANS AGAINST THE EFFECTS OF CYBER OPERATIONS DURING ARMED CONFLICTS (Laurent Gisel, Tilman Rodenhäuser y Knut Dörmann), publicado en el número de septiembre de 2020 de la INTERNATIONAL REVIEW OF THE RED CROSS:
https://international-review.icrc.org/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts

d) DIRECT PARTICIPATION IN HOSTILITIES IN THE AGE OF CYBER: EXPLORING THE FAULT LINES (David Wallace, Shane Reeves &Trent Powell), publicado en el vol. 12 del Harvard National Security Journal:
https://harvardnsj.org/wp-content/uploads/2021/02/HNSJ-Vol-12-Wallace-Reeves-and-Powell-Direct-Participation-in-Hostilities-in-the-Age-of-Cyber.pdf

VII. Procesos en el marco de las Naciones Unidas en relación con el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional: últimos informes del Group of Governmental Experts (GGE) y del Open-Ended Working Group (OEWG).

a) Los textos de los informes pueden obtenerse en:
https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/gge/documents/gge-report-adopted.pdf

b) Puede, además, alcanzarse un conocimiento más profundo sobre el tema con la lectura de los siguientes artículos:
https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/
https://journals.muni.cz/mujlt/article/view/20668/16944

BIBLIOGRAFÍA COMPLEMENTARIA

RECURSOS DE APOYO Y WEBGRAFÍA

Se recomiendan las siguientes web, cuya visita proporcionará información de indudable utilidad para la mejor comprensión de los contenidos de la asignatura:

•CCN- CERT: https://www.ccn-cert.cni.es/

•INCIBE CERT: https://www.incibe-cert.es/

•CNPIC: https://cnpic.interior.gob.es/opencms/es/inicio/

•ENISA: https://www.enisa.europa.eu/

•NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): https://ccdcoe.org/

•Cyber Operations Tracker: https://www.cfr.org/interactive/cyber-operations

•European Repository of Cyber Incidents (EuRepoC): https://eurepoc.eu/

Los materiales que se recomiendan para la preparación del curso han sido seleccionados en función de los objetivos específicos del curso y teniendo presente en todo momento la metodología propia de la educación a distancia.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.