

21-22

MÁSTER UNIVERSITARIO EN  
CIBERSEGURIDAD

# GUÍA DE ESTUDIO PÚBLICA



## MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO

CÓDIGO 3110910-

UNED

21-22

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

Nombre de la asignatura	MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO
Código	3110910-
Curso académico	2021/2022
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
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. Dr. D. Sergio Cámara Arroyo. Despacho 3.52 (miércoles de 10:00 a 14:00 horas)  
guardia del departamento martes de 16:00 a 20:00 horas. Tef.: 913988054.

## 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 capaz 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: el Group of Governmental Experts (GGE) y el Open-Ended Working Group (OEWG), antecedentes y estado actual de los trabajos

## 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 4 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 4 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 4 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% nota final.

Fecha aproximada de entrega 20/01/2020

Comentarios y observaciones

#### PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC? Si, PEC no presencial

#### Descripción

Las 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 sobre 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 2,5 puntos. Para hacer el cómputo de la nota, las 10 respuestas se valoran sobre 10, de manera que se asigna a cada acierto una puntuación de 1 y a cada fallo un descuento de 0,2, y el resultado final se divide por 4 para ajustarlo al valor final de 2,5.

Ponderación de la PEC en la nota final

La PEC servirá 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 1,25 puntos sobre los 2,5 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 14/01/2020  
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.

***1. 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) Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, accesible en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001&from=es>

b) Estrategia de Seguridad Nacional 2017 (apartados relativos a las amenazas en el ciberespacio y a la ciberseguridad de los Capítulos 4 y 5, así como el Capítulo 6), accesible en:

[http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824\\_Estrategia\\_de\\_Seguridad\\_Nacional\\_ESN\\_doble\\_pag.pdf](http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf)

c) Estrategia Nacional de Ciberseguridad 2019: Aprobada por el Consejo de Seguridad Nacional en su reunión del 12 de abril de 2019, su texto está disponible en:

<https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf>



d) DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, accesible en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES>

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 anterior Directiva al ordenamiento jurídico español), accesible en:

<https://www.boe.es/boe/dias/2018/09/08/pdfs/BOE-A-2018-12257.pdf>

f) 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](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389)

g) 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/pdf/2018/BOE-A-2018-799-consolidado.pdf>

**II. El componente militar de la ciberseguridad en España: el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas:** Se preparará con la lectura de los siguientes textos normativos:

a) La Orden Ministerial 10/2013, de 19 de febrero (ya derogada), por la que se creó el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, accesible en:

[http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226\\_CIBERDEFENSA.pdf](http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226_CIBERDEFENSA.pdf)

b) Instrucción 65/2015, de 30 de diciembre, del Jefe de Estado Mayor de la Defensa, por la que se desarrolla la organización del Estado Mayor de la Defensa (solo el Capítulo IV, relativo al Mando Conjunto de Ciberdefensa), accesible en:

[http://intra.mdef.es/intradef/contenido\\_INET\\_Active/Contenidos/Estado\\_Mayor\\_de\\_la\\_Defensa/Documentacion/s090047/Documentos/INSTRUCCION%20N%2065%20-%2015%20DEL%20JEMAD\\_09003a99807ce8be.pdf](http://intra.mdef.es/intradef/contenido_INET_Active/Contenidos/Estado_Mayor_de_la_Defensa/Documentacion/s090047/Documentos/INSTRUCCION%20N%2065%20-%2015%20DEL%20JEMAD_09003a99807ce8be.pdf)

c) Concepto de Ciberdefensa del JEMAD, de 28 de septiembre de 2018 (resumen ejecutivo), accesible en:

[http://www.emad.mde.es/Galerias/EMAD/files/Concepto\\_CIBER\\_Resumen\\_Ejecutivo.pdf](http://www.emad.mde.es/Galerias/EMAD/files/Concepto_CIBER_Resumen_Ejecutivo.pdf)

**III. Aplicación de los principios de soberanía, diligencia debida, jurisdicción y responsabilidad internacional en el ciberespacio.**

a) *The Application of International Law to State Cyberattacks*, de Harriet Moynihan:

<https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf>

b) *Grey Zones in the International Law of Cyberspace*, de Michael N. Schmitt:

<https://cpb-us->

[w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt\\_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf](https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf)

c) *Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace*, de Gary P. Corn (obviar toda la parte relativa al “*Domestic Legal Framework*”):

<https://poseidon01.ssrn.com/delivery.php?ID=666112089118089013103088093105104066019041046044086035108099066122066097025084098113031012096001011007032119005123095098065114121055070011022074030111113012068093019046039010121029031066112064001075017027113016093026019109024084113028015067008119086105&EXT=pdf>

#### **IV. Ciberespionaje y Derecho internacional público:**

Aunque la obra de referencia sobre estos aspectos la constituye la Parte I del “*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*” (Cambridge University Press, 2017), estos contenidos 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 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](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.**

a) *The Law of Cyber Warfare: Quo Vadis?*, de Michael N. Schmitt:

<https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf>

b) *World Wide Warfare - 'Jus Ad Bellum' and the Use of Cyber Force*, de Marco Roscini:

<https://poseidon01.ssrn.com/delivery.php?ID=572020111031084067018084092125007108006045091065063000028096099064102114089023086103045011120033106120053098125017002105109114047040027013023094068068121110113116026009081056095085025019115116095092007119095068092126079028021108117029117124069021008117&EXT=pdf>

#### **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 un trabajo del Profesor Jerónimo Domínguez Bascoy, que oportunamente se proporcionará a los alumnos, o 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:

<https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf>

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://harvardnsj.org/wp-content/uploads/sites/13/2017/02/Schmitt-NSJ-Vol-8.pdf>

## 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:

a) CCN- CERT: <https://www.ccn-cert.cni.es/>

b) INCIBE CERT: <https://www.incibe-cert.es/>

c) CNPIC: <http://www.cnpic.es/index.html>

d) ENISA: <https://www.enisa.europa.eu/>

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

f) Cyber Operations Tracker: <https://www.cfr.org/interactive/cyber-operations>

A través de la Plataforma virtual aLF de la UNED el profesor proporcionará presentaciones, textos, artículos y materiales que sirvan de apoyo a los alumnos.

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.

Los alumnos recibirán una Guía Didáctica en la que encontrarán una orientación previa al curso así como respuestas a muchas de las cuestiones que se le irán planteando a medida que vaya avanzando en el estudio.

---

## 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.