Guía docente de la asignatura

El Ámbito Ciberespacial

Fecha última actualización: 14/07/2021
Fecha de aprobación por la Comisión Académica: 23/07/2021

Máster	Máster Universitario en Pensamiento Estratégico y Seguridad Global
MÓDULO	El Ámbito Ciberespacial
RAMA	Ciencias Sociales y Jurídicas
CENTRO RESPONSABLE DEL TÍTULO	Escuela Internacional de Posgrado

Semestre	Segundo	**Créditos**	6	**Tipo**	Optativa	**Tipo de enseñanza**	Enseñanza Virtual

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Máster)

1. Introducción al ciberespacio.

2. Amenazas y riesgos

3. La ciberseguridad: paradigma de seguridad.

4. Cibercriminalidad.

5. Ciberterrorismo.

6. Ciberdefensa y ciberguerra.

COMPETENCIAS

COMPETENCIAS BÁSICAS

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en 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

- CG01 - Formular los procesos de análisis, síntesis, organización y planificación asociados a la investigación
- CG02 - Argumentar, describir y comparar de forma crítica, original y creativa
- CG03 - Reconocer la importancia de la motivación por la calidad en el proceso y en los resultados
- CG05 - Planificar y aplicar información diversa y compleja
- CG06 - Argumentar de forma oral y escrita y utilizar conceptos y términos de manera adecuada
- CG07 - Adquirir habilidades de aprendizaje para el trabajo autónomo

COMPETENCIAS ESPECÍFICAS

- CE07 - Comparar y evaluar las principales amenazas contemporáneas y emergentes, así como los actores e instituciones que intervienen en las políticas de seguridad y defensa
- CE11 - Valorar el papel de las Fuerzas Armadas en el espectro de las operaciones militares nacionales e internacionales

COMPETENCIAS TRANSVERSALES

- CT01 - Comprender y defender la importancia que la diversidad de culturas y costumbres tienen en la investigación o práctica profesional
- CT02 - Tener un compromiso ético y social en la aplicación de los conocimientos adquiridos
- CT03 - Ser capaz de trabajar en equipos interdisciplinarios para alcanzar objetivos comunes desde campos expertos diferenciados
- CT04 - Incorporar los principios del Diseño Universal en el desempeño de su profesión

RESULTADOS DE APRENDIZAJE (Objetivos)

RESULTADOS GENERALES DEL APRENDIZAJE:
1. Obtención de conocimientos básicos conceptuales, teóricos y metodológicos necesarios para la comprensión del ámbito ciberespacial.
2. Obtención de conocimientos básicos sobre amenazas y riesgos en el ciberespacio.

3. Obtención de conocimientos sobre la ciberseguridad como paradigma de seguridad.
4. Obtención de conocimientos básicos sobre el marco normativo de lucha contra la cibercriminalidad.
5. Obtención de conocimientos básicos sobre el fenómeno del ciberterrorismo.
6. Obtención de conocimientos básicos sobre ciberdefensa y ciberguerra.
RESULTADOS ESPECÍFICOS
Cognitivos:
· El alumnado dominará los enfoques teóricos y metodológicos sobre el ciberespacio y la ciberseguridad.
· El alumnado asimilará los conceptos, instrumentos jurídicos y compromisos internacionales que explican y regulan la actividad de los Estados y de los agentes
no estatales en el ciberespacio y el paradigma de la ciberseguridad.
· El alumnado asimilará los conceptos, categorías, sistemas y características que permiten entender la cibercriminalidad, el ciberterrorismo, la ciberdefensa y la ciberguerra.
Procedimentales/Instrumentales:
· El alumnado será capaz de asimilar los conocimientos sobre las materias antes descritas
· El alumnado será capaz de aplicar los conceptos básicos estudiados al análisis de la seguridad internacional.
Actitudinales y transversales:
· El alumnado desarrollará la capacidad crítica a la hora analizar los diferentes estudios de caso y de materias que puedan plantearse.
· El alumnado desarrollará la capacidad de búsqueda de soluciones y argumentaciones sobre la materia.
· El alumnado desarrollará la visión interdisciplinar de la temática.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

1. Introducción al ciberespacio.

1.1. Evolución, concepto y naturaleza.

1.2. Caracteres, componentes y principios.

2. Amenazas y riesgos

2.1. Actores y riesgos en el ciberespacio.

2.2. El fenómeno de deslocalización de las amenazas.

2.3. Actividades ilícitas y maliciosas en el ciberespacio

2.4. Desinformación y manipulación informativa

3. La ciberseguridad: paradigma de seguridad.

3.1. Naturaleza y caracteres del modelo de seguridad

3.2. Principios y reglas

3.3.Ciberinteligencia

3.4. Ciberespionaje

4. Cibercriminalidad.

4.1.El fenoḿeno criminal en el ciberespacio

4.2. Normativa en materia de cibercriminalidad

4.3. Mecanismos de lucha contra la cibercriminalidad

5. Ciberterrorismo.

5.1. Concepto y caracteres.

5.2. Modalidades de ciberterrorismo.

5.3. Normativa y mecanismos de lucha contra el ciberterrorismo.

6. Ciberdefensa y ciberguerra.

6.1.Concepto y modalidades.

6.2. Normativa internacional en materia de ciberdefensa.

6.3. Marco doctrinal de la ciberdefensa

6.4. Aplicación del Derecho Internacional de los Conflictos Armados al ciberespacio.

- Uso del ciberespacio en operaciones militares

PRÁCTICO

1. Introducción al ciberespacio.

2. Amenazas y riesgos

3. La ciberseguridad: paradigma de seguridad.

4. Cibercriminalidad.

5. Ciberterrorismo

6. Ciberdefensa y ciberguerra.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

• Acton, James: “Cyber Warfare & Inadvertent Escalation”, Daedalus, 149(2): 133-149

- AJP 3.20 Allied Joint Doctrine for Cyberoperations. NATO.
- Brantly, Aaron (ed.): The cyber deterrence problem. Lanhman: Rowman & Littlefield, 2020.
- Ciberseguridad Global. Oportunidades y compromisos del uso del Ciberespacio. Universidad de Granada. Spain
- Clarke, Richard & Robert Knake: Cyber War. The next threat to national security and what to do about it. Nueva York: Harper Collins, 2011.
- Concept of Cyber Defence. EMAD. Spain
- Doctrine Note Information Manoeuvre. British Army. UK
- Federated Mission Networking Swimlane Planning Perspective Federated Cyberspace Command and Control. NATO
- Jasper, Scott: Strategic cyber deterrence: the active cyber defense option. Lanham: Rowman & Littlefield, 2017.
- Jasper, Scott: Securing freedom in the global commons. Stanford: Stanford University Press, 2010.
- Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities. UK
- Mazanec, Brian & Thayer, Bradley: Deterring cyber warfare: bolstering strategic stability in cyberspace. Londres: Palgrave, 2014.
- PDC-1 (A) Doctrine of Employment of the Armed Forces. EMAD. Spain
- Rid, Thomas: Cyber War will not take place. Nueva York: Oxford University Press, 2013.
- Robles Carrillo, M., "Amenaza y uso de la fuerza a través del ciberespacio", Revista Latinoamericana de Derecho Internacional /Latin American Journal of International Law, No 4, 2016 (http://www.revistaladi.com.ar/numero4-robles/).
- Robles Carrillo, M., "Los principios rectores de la cooperación internacional en el ciberespacio. Alcance y contenido del consenso entre los Estados", Revista Iberoamericana de Derecho Internacional y de la Integración - Número 5 - Noviembre 2016. http://www.ijeditores.com.ar/pop.php?option=articulo&Hash=a61dd25b9bddee46ea8cb43eb63376 cc
- Robles Carrillo, M., "El concepto de arma cibernética en el marco internacional: una aproximación funcional", Boletín del Instituto Español de Estudios Estratégicos. Documento de opinión, No 101/2016, http://www.ieee.es/contenido/noticias/2016/10/DIEEEO101-2016.html
- Robles Carrillo, M., "La reforma de la Corporación para la Asignación de Nombres y Números de Internet (ICANN): Un análisis en términos de legitimidad", Revista Española de Derecho Internacional, Vol. 70. No 2, 2018, pp. 155-181. http://dx.doi.org/10.17103/redi.70.2.2018.1.06
- Robles Carrillo, M., "Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral?", Revista de Derecho Comunitario Europeo, Vol. 60, 2018. https://doi.org/10.18042/cepc/rdce.60.03
- Robles Carrillo, M., "El régimen jurídico de las operaciones en el ciberespacio: estado del debate". Boletín del Instituto Español de Estudios Estratégicos. Documento de opinión 101/2019. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO101_2019MARROB_legalciber.pdf
- Robles Carrillo, M., "Sanciones contra ciberataques: la acción de la Unión Europea". Boletín del Instituto Español de Estudios Estratégicos. Documento de opinión 143/2020. http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO143_2020MARROB_ciberUE.pdf
- Robles Carrillo, M., "Seguridad en Redes 5G: la acción de la Unión Europea". Actas de las XVI RECSI. Universidad de Lleida. http://www.recsi2020.udl.cat/static/site/files/Robles-XVI-RECSI.pdf
- Robles Carrillo, M. y Almeida Ros , M., "Email Spoofing: un enfoque técnico-jurídico". Actas de las XVI RECSI. Universidad de Lleida. http://www.recsi2020.udl.cat/static/site/files/RoblesAlmeida-XVI-RECSI.pdf
- Robles Carrillo, M., "Análisis de la Normativa sobre Seguridad de Redes y Sistemas de Información: el Real Decreto 43/2021". Actas de las VI Jornadas Nacionales (JNIC2021 LIVE). https://ruidera.uclm.es/xmlui/bitstream/handle/10578/28654/44 INVESTIGACIÓN EN CIBERSEGURIDAD.pdf?sequence=1&isAllowed=y

BIBLIOGRAFÍA COMPLEMENTARIA

- Collins, A., Contemporary Security Studies, 4º Ed., Oxford University Press, 2016.
- Fierke, K.M., Critical Approach to International Security, 2º Ed., Politu Press, 2015.
- Fuentes Torrijo, X., "La prohibición de la amenaza y del uso de la fuerza por el derecho internacional", Araucaria: Revista Iberoamericana de filosofía, política y humanidades, Vol. 16, Nº 32, 2014 (doi: 10.12795/araucaria.2014.i32.13).
- Gayoso Rey, J., "Las estrategias y la lucha contra el terrorismo", Cuadernos de la Guardia Civil, Nº 58, 2019, pp. 55-70.
- Robles Carrillo, M., "El modelo de neutralidad de la red en la Unión Europea: alcance y contenido". Revista de Derecho Comunitario Europeo, Vol. 63, 2019. https://recyt.fecyt.es/index.php/RDCE/article/view/73760
- Robles Carrillo, M., "La posición de Francia sobre el régimen jurídico de las operaciones en el ciberespacio". Boletín del Instituto Español de Estudios Estratégicos. Documento de opinión 51/2020. http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO51_2020MARROB_digiFrance.pdf
- Sadat, L.N., Seeking Accountability for the Unlawful Use of Force, Cambridge Univ. Press 2018.
- Sartori, G., La carrera hacia ninguna parte. Diez lecciones sobre nuestra sociedad en peligro, Ed. Taurus, Madrid, 2016.

ENLACES RECOMENDADOS

- Center for Strategic & International Studies (CSIS)/ www.csis.org
- https://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional
- Mando Conjunto del Ciberespacio
- RAND Corporation/ www.rand.org
- The National Cyber Security Centre
- UNITED NATIONS INTERIM FORCE IN LEBANON
- UK National Cyber Force
- The NATO Cooperative Cyber Defence Centre of Excellence

METODOLOGÍA DOCENTE

- MD01 Lección puntual magistral/expositiva on-line
- MD02 Sesiones de discusión y debate mediante foros on-line
- MD03 Desarrollo de foros on-line de información y de consultas

- MD04 Resolución de problemas y estudio de casos prácticos
- MD06 Material audiovisual editado por el profesor (presentaciones con audio, páginas web, podcasts, guías, lecturas) Análisis de fuentes y documentos
- MD07 Realización de trabajos individuales (análisis de fuentes y documentos)
- MD09 Cuestionarios online

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

1) Aportaciones de los estudiantes en los foros de discusión: 40%
2) Entrega de trabajos informes, trabajos, proyectos a través de la plataforma docente: 30%
3) Cuestionarios on-line: 30%

EVALUACIÓN EXTRAORDINARIA

Para los estudiantes que han seguido la evaluación continua, pero no superaron la materia en la convocatoria ordinaria, la evaluación en la convocatoria extraordinaria se realizará mediante una prueba escrita que podrá consistir en pruebas objetivas, resolución de problemas, casos o supuestos, pruebas de respuesta breve, test, análisis de textos. Dicha prueba supondrá el 100% de la calificación final.

EVALUACIÓN ÚNICA FINAL

El artículo 8 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que podrá acogerse a la evaluación única final el estudiante que no pueda cumplir con el método de evaluación continua por causas justificadas. Para ello, el estudiante, en las dos primeras semanas de impartición de la asignatura o en las dos semanas siguientes a su matriculación si esta se ha producido con posterioridad al inicio de las clases o por causa sobrevenidas, lo solicitará, a través del procedimiento electrónico, a la Coordinación del Máster, quien dará traslado al profesorado correspondiente, alegando y acreditando las razones que le asisten para no poder seguir el sistema de evaluación continua. La evaluación de aquellos estudiantes acogidos al sistema de Evaluación Única Final consistirá en un examen escrito sobre el programa teórico y práctico de la asignatura (100% de la calificación final).

INFORMACIÓN ADICIONAL

Diseño para todos: Necesidades Específicas de Apoyo Educativo (NEAE): Siguiendo las recomendaciones de la CRUE y del Secretariado de Inclusión y Diversidad de la UGR, los sistemas de adquisición y de evaluación de competencias recogidos en esta Guía Docente se aplicarán conforme al principio de diseño para todas las personas, facilitando el aprendizaje y la demostración de conocimientos de acuerdo a las necesidades y la diversidad funcional del alumnado. Información sobre el Plagio: La Universidad de Granada fomentará el respeto a la propiedad intelectual y transmitirá a los estudiantes que el plagio es una práctica contraria a los principios que rigen la formación universitaria. Para ello procederá a reconocer la autoría de los trabajos y su protección de acuerdo con la propiedad intelectual según establezca la legislación vigente. El plagio, entendido como la presentación de un trabajo u obra hecho por otra persona como propio o la copia de textos sin citar su procedencia y dándolos como de elaboración propia,

conllevará automáticamente la calificación numérica de cero en la asignatura en la que se hubiera detectado, independientemente del resto de las calificaciones que el estudiante hubiera obtenido. Esta consecuencia debe entenderse sin perjuicio de las responsabilidades disciplinarias en las que pudieran incurrir los estudiantes que plagien. Los trabajos y materiales entregados por parte de los estudiantes tendrán que ir firmados con una declaración explícita en la que se asume la originalidad del trabajo, entendida en el sentido de que no ha utilizado fuentes sin citarlas debidamente.