Guía Docente: Análisis y gestión del ámbito ciberespacial

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Máster en Seguridad, Defensa y Liderazgo
Plan de estudios	2022
Materia	Seguridad y Defensa
Carácter	Obligatorio
Período de impartición	Segundo Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se precisa

DATOS DEL PROFESORADO			
Profesor Responsable	Roger Sanz Gonzalez	**Correo electrónico**	roger.sanz@ui1.es
Área	Ciencia de la Computación e Inteligencia Artificial	**Facultad**	Facultad de Criminología
Perfil Profesional 2.0	Manager de Gobierno, Riesgo y Cumplimiento (GRC) . Consultor Senior con especialización en la gestión de riesgos digitales, seguridad e inteligencia para los negocios para disciplinas disruptivas como el uso de la inteligencia artificial aplicada. Ha desempeñado puestos directivos en los ámbitos de operaciones, tecnología, gestión de riesgos, seguridad, auditoría interna y compliance. https://www.linkedin.com/in/rogersanz		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Geoestrategia: amenazas y desafíos • La Seguridad como fenómeno global • La Defensa como fenómeno global • Fundamentos de Inteligencia y contrainteligencia • Análisis y gestión del ámbito cognitivo • Análisis y gestión del ámbito ciberespacial
Contexto y sentido de la asignatura en la titulación y perfil profesional	El mundo globalizado se caracteriza, entre otras cosas, por la omnipresente utilización de nuevas tecnologías (Internet, manipulación de la información, difusión de noticias sin control, inteligencia artificial, procesamiento masivo de datos, robótica…) y por el casi infinito grado de interconexión entre todo tipo de agentes (gobiernos, instituciones, empresas, organizaciones, personas…). En este contexto cobra una especial importancia conocer los fundamentos para el análisis y gestión de un nuevo espacio de operaciones que la “Doctrina para el Empleo de las Fuerzas Armadas” denomina “ámbito ciberespacial” y que queda definido en los siguientes términos: *El ámbito ciberespacial es el ámbito artificial compuesto por infraestructuras, redes, sistemas de información y telecomunicaciones y otros sistemas electrónicos, por su interacción a través de las líneas de comunicación sobre las que se propaga y el espectro electromagnético (EEM), así como por la información que es almacenada o transmitida a través de ellos. Es transversal a los demás ámbitos y no está sujeto a un determinado espacio geográfico. Le caracterizan su extensión, el anonimato, la inmediatez y su fácil acceso.* *Finalmente, su carácter artificial y su rápida evolución generan continuas vulnerabilidades y oportunidades.*

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	Generales y básicas • CG1: Trabajar en equipos multidisciplinares y específicamente de Seguridad y Defensa. • CG2: Coordinar y dirigir equipos de trabajo en el ámbito de la seguridad y defensa. • CG5: Aumentar la sensibilidad e interés respecto a los temas de interés social y políticas públicas referidas a seguridad y defensa. • CG6: Adquirir una conciencia crítica para la promoción del respeto y los Derechos Humanos. • CG7: Desarrollar habilidades para el aprendizaje autónomo en el ámbito de la seguridad y defensa. • CG8: Potenciar la capacidad de iniciativa, creatividad, liderazgo y superación en el desarrollo de la vida profesional. • CG9: Potenciar la visión estratégica en el desarrollo de la profesión. • CG10: Desenvolverse con eficacia en un entorno de presión. • 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. • 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. Específicas • CE1: Conocer los instrumentos jurídicos y marcos institucionales en el ámbito de la seguridad y defensa. • CE21: Adquirir habilidades para analizar y documentar situaciones de crisis, catástrofes humanitarias y conflictos. • CE23: Conocer cómo se gestionan las empresas de seguridad y los departamentos de seguridad de las grandes empresas, en la consecución de objetivos organizativos.
Resultados de aprendizaje de la asignatura	• Configurar de manera segura la plataforma necesaria para el soporte de aplicaciones y servicios web. • Adquirir conocimientos adecuados de las diferentes tecnologías empleadas para desarrollar servicios seguros en Internet. • Conocer los ciberataques fundamentales y la forma de responder y protegerse. • Conocer las principales formas de ataque a infraestructuras sociales (IoT) e industriales avanzadas. • Desarrollar métodos de seguridad en sistemas tecnológicos sociales (IoT) e industriales. • Desarrollar conocimientos adecuados de gestión de seguridad en sistemas e infraestructuras críticas.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Las tecnologías de la información aplicadas al ciberespionaje y el ciberterrorismo se identifican hoy como un factor esencial para la Seguridad a nivel nacional, internacional y global, como a su vez constituyen un elemento esencial para la vigilancia y la ofensiva en beneficio de la Seguridad en dichos tres ámbitos. En la asignatura Mundo cibernético, seguridad y defensa el estudiante se enfrentará al análisis y profundización avanzada de los retos que la sociedad de la información supone para el mundo de la seguridad, y en particular a la detección y protección frente amenazas tales como virus, troyanos, ataques de denegación de servicio, espionaje, intercepción de telecomunicaciones, etc. La protección de infraestructuras críticas frente ataques informáticos, la organización española del mando conjunto de ciberdefensa y la revisión de los aspectos legales asociados a la supervisión de sistemas informáticos en el ámbito de la empresa son algunos de los temas que igualmente recibirán tratamiento en dicha asignatura. • Tema 1. Introducción a la Ciberdefensa. • Tema 2. Ciberamenazas a las infraestructuras críticas. • Tema 3. Herramientas de las ciberamenazas Web profunda. • Tema 4. Las APT (Amenazas Avanzadas Persistentes). • Tema 5. Detección y defensa frente a la amenaza ciber. • Tema 6. Respuestas ante incidentes ciber y análisis forense.
Contenidos	• Unidad Didáctica 1. Introducción a la Ciberdefensa. • Unidad Didáctica 2. Ciberamenazas a las infraestructuras críticas. • Unidad Didáctica 3. Herramientas de las ciberamenazas y web profunda. • Unidad Didáctica 4. Actores no estatales y APTs (Amenazas persistentes avanzadas) • Unidad Didáctica 5. Gestión de capacidades de detección de amenazas en el ciberespacio • Unidad Didáctica 6. Respuesta ante ciberincidentes y análisis forense digital

METODOLOGÍA	
Actividades formativas	• **Contenidos teóricos:** contenidos de aprendizaje de cada unidad didáctica, lecciones para trabajar con memorizaciones significativas y habilidades aplicativas. • **Estudios de caso individual:** como motivación y conducción del pensamiento reflexivo personal. • **Foros de debate:** formados por una serie de temas, relacionados con el contenido teórico de la asignatura, que la docente propondrá para discusión conjunta. • **Actividad colaborativa:** orientado a fomentar el trabajo colectivo. • **Cuestionarios de evaluación:** en formato tipo test que sirvan de repaso al alumno y además le permitan prepararse para la realización del examen final.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del*

alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.

El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*.

El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera:

Sistema de evaluación convocatoria ordinaria

Opción 1. Evaluación continua

Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los

porcentajes correspondientes se alcance una calificación mínima de un 5.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el resultado total, se establece una relación de proporcionalidad en una escala de 10.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior.

En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado.

En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura.

Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Clarke, R. & Knake, R. (2011). *Guerra en la red, los nuevos campos de batalla*. Barcelona. Editorial Planeta. Ministerio de Defensa (EMAD) 2018. “Concepto de Ciberdefensa. Resúmen Ejecutivo”, Madrid.
BibliografÍa complementaria	Toffler, Alvin (1995). “*Onward Cyber-Soldiers*”, en Time Magazine, agosto, Nº 146 Torres Soriano, Manuel Ricardo (2007). *La dimensión propagandística del terrorismo yihadista global*. Granada: Tesis Doctoral de la Universidad de Granada.
Otros recursos	CESEDEN, Monografía “El ciberespacio, nuevo escenario de confrontación”. 2012. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf UIT, “Guía para la elaboración de una Estrategia Nacional de Ciberseguridad” https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf