1. Identificación

1.1. De la Asignatura

Curso Académico	2020/2021
Titulación	GRADO EN SEGURIDAD
Nombre de la Asignatura	CIBERSEGURIDAD
Código	5145
Curso	CUARTO
Carácter	OPTATIVA
N.º Grupos	1
Créditos ECTS	4.5
Estimación del volumen de trabajo del alumno	112.5
Organización Temporal/Temporalidad	1 Cuatrimestre
Idiomas en que se imparte	ESPAÑOL

1.2. Del profesorado: Equipo Docente

Coordinación de la asignatura ANDRES SORIANO GUILLAMON Grupo de Docencia: 1 Coordinación de los grupos:1	Correo Electrónico / Página web / Tutoría electrónica	andres.soriano@um.es Tutoría Electrónica: SÍ				
	Teléfono, Horario y Lugar de atención al alumnado	Duración	Día	Horario	Lugar	Observaciones
		Anual	Martes	19:30- 20:30		Presencial
		Anual	Miércoles	16:30- 18:00		Presencial
		Anual	Jueves	15:00- 20:00		Tutoría online

2. Presentación

Los peligros aparejados a las nuevas tecnologías y al ciberespacio, pueden afectar la seguridad, estabilidad y desarrollo de un país y sus habitantes, por ello, se requiere de una capacidad analítica que permita anticiparse a las posibles amenazas y vulnerabilidades, otorgando medidas capaces de contrarrestarlas, a través de la implementación de mecanismos de seguridad. Para ello a lo largo de esta asignatura, se profundizará sobre las siguientes cuestiones:

- Identificar las vulnerabilidades existentes en los entornos cibernéticos.
- Analizar las motivaciones y características que conforman las diferentes formas de criminalidad asociadas a los entornos virtuales, así como su respuesta penal.
- Establecer un sistema de análisis y gestión de riesgos.
- Estudiar las características y beneficios que aportan las diferentes auditorias de seguridad.
- Evaluar las consecuencias que se derivarían de cada amenaza en caso de que se lleven a cabo con éxito.
- Estimar el coste que repercutiría cada ataque, así como el de su medida de respuesta.
- Análisis en ciberinteligencia como factor de protección en ciberseguridad, etc.

3. Condiciones de acceso a la asignatura

3.1 Incompatibilidades

No consta

3.2 Recomendaciones

Esta asignatura, se dirige hacia aquellos alumnos que deseen profundizar sus conocimientos en la gestión de riesgos y vulnerabilidades en todas sus esferas, siendo de especial interés para aquellas personas que deseen desempeñar una actividad laboral relacionada con la seguridad y defensa (FCSE, Fuerzas Armadas, Policías, Protección civil, Seguridad privada,etc.), así como estudiantes de otras materias, criminólogos, peritos informáticos, analistas, etc.

4. Competencias

4.1 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

· 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

4.2 Competencias de la titulación

· G2. Adquirir los conocimientos teórico-prácticos, métodos, técnicas y herramientas de investigación que proporcionan criterios de actuación eficientes para desempeñar las profesiones relacionadas con la seguridad pública y privada
· G3. Ser capaz de gestionar la información y el conocimiento en el ámbito de los estudios de la seguridad y la prevención de riesgos, incluyendo saber utilizar como usuario las herramientas básicas en TIC en estos ámbitos.
· G4. Conocer los valores esenciales de la ética y la integridad intelectual en la práctica del profesional de la seguridad pública o privada.
· G6. Ser capaz de trabajar en equipos interdisciplinares que trabajan en el ámbito de la seguridad y la prevención de riesgos.
· G12. Ser capaz de explicar y razonar sobre la base de argumentos de índole jurídica, psicológica, sociológica y científica referidos al ámbito de la seguridad
· G15. Capacidad de comprensión y análisis de la información y documentación de las distintas áreas científicas objeto de estudio en el Grado en Seguridad.
· CE8. Conocer el ordenamiento jurídico y demostrar ser capaz de interpretarlo y utilizarlo de manera crítica.
· CE10. Saber usar conceptos y teorías criminológicas para entender y explicar el delito, al delincuente, la victimización y las respuestas ante el delito y la desviación.
· CE18. Capacidad para identificar los nuevos retos de la criminalidad organizada, así como las nuevas amenazas internacionales en el campo de la ciberseguridad.

4.3 Competencias transversales y de materia

· Competencia 1. Obtener la capacidad de análisis y respuesta ante un incidente de ciberseguridad, pudiendo identificar el tipo de ataque y la forma de desarrollarse el mismo.

5. Contenidos

TEMA 1. Tema 1: Fundamentos de ciberseguridad. Conceptos básicos: Ciberespacio, Ciberseguridad,

Ciberguerra, Ciberinteligencia Metodologías ciberinteligencia OSINT…

TEMA 2. Marco normativo y estándares de ciberseguridad.

Marco normativo y estándares de ciberseguridad.

ISO 27001

Marco de referencia NIST

Certificaciones en ciberseguridad

Common Criteria

TEMA 3. Análisis de malware y componentes de un ciberataque.

TEMA 4. Auditorías de ciberseguridad.

TEMA 5. Análisis y gestión de riesgos en ciberseguridad

TEMA 6. Hacking ético

TEMA 7. Marco legislativo internacional

TEMA 8. Estrategia nacional de ciberseguridad

TEMA 9. Ciberamenazas con potencial desestabilizador: hacktivismo, ciberterrorismo y campañas de desinformación (fake news)

TEMA 10. Cibercriminalidad en España

PRÁCTICAS

Práctica 1. Práctica 1: Metodologías de análisis en ciberinteligencia: Global

Práctica 2. Práctica 2: Preparación de un laboratorio de investigación de entornos ciber: Global

Práctica 3. Práctica 3: Ciberinteligencia IMINT: Global

Práctica 4. Práctica 4: Ciberinteligencia OSINT: Global

Práctica 5. Práctica 5: Hacking ético : Global

6. Metodología Docente

Actividad Formativa	Metodología	Horas Presenciales	Horas en Semipresencialidad	Horas No Presenciales	Trabajo Autónomo	Volumen de trabajo
CLASE MAGISTRAL	Clases expositivas en las que se abordará la parte teórica de la asignatura a través de clases magistrales o proyección dirigida sobre las diferentes amenazas que conforman el ciberespacio, así como en al evaluación de riesgos y vulnerabilidades.	30	0	30		30.00
CLASES PRÁCTICAS	Realización de supuestos prácticos enmarcados en el aprendizaje de herramientas para la obtención de ciberinteligencia, así como prácticas de hacking ético.	7,5	0	7,5		7.50
	Total	37.5		37.5	0	37.5

7. Horario de la asignatura

https://www.um.es/web/estudios/grados/seguridad /2020-21#horarios

8. Sistema de Evaluación

Métodos / Instrumentos	Exámenes escritos u orales: En el caso de los exámenes escritos, podrán ser pruebas objetivas, de desarrollo, de respuesta corta, de ejecución de tareas, de escala de actitudes, realizadas por los estudiantes para mostrar los conocimientos teóricos y prácticos adquiridos. Los exámenes orales pueden consistir en entrevistas de evaluación, preguntas individualizadas planteadas para valorar los resultados de aprendizaje previstos en la materia.
Criterios de Valoración	
Ponderación	70
Métodos / Instrumentos	Informes escritos, trabajos y proyectos: presentación por escrito de prácticas y trabajos resueltos, informes, proyectos, portafolios, con independencia de que se realicen individual o grupalmente.
Criterios de Valoración	
Ponderación	20
Métodos / Instrumentos	Presentación pública de trabajos: exposición de los resultados obtenidos y procedimientos necesarios para la realización de un trabajo, así como respuestas razonadas a las posibles cuestiones que se plantee sobre el mismo.
Criterios de Valoración	
Ponderación	0
Métodos / Instrumentos	Procedimientos de observación del trabajo del estudiante: registros de participación, de realización de actividades, cumplimiento de plazos, participación en foros
Criterios de Valoración	
Ponderación	10
Métodos / Instrumentos	Evaluación en semipresencialidad
Criterios de Valoración	No establecida
Métodos / Instrumentos	Evaluación en no presencialidad
Criterios de Valoración	Se establecerá el sistema de evaluación no presencial, como medida excepcional, en caso de que las autoridades sanitarias competentes lo estimen oportuno, derivado de la crisis sanitaria ocasionada por la pandemia derivada del Covid-19

Fechas de exámenes

https://www.um.es/web/estudios/grados/seguridad /2020-21#examenes

9. Resultados del Aprendizaje

10. Bibliografía

Bibliografía Básica

- ISO 27001, de Sistemas de gestión.- ISO 19011, Directrices para la auditoría de los sistemas de gestión.- Estrategia nacional de ciberseguridad, año 2019- OWASP. Análisis y gestión de riesgos.

Nueva Referencia Electrónica

Nueva Referencia Electrónica

Nueva Referencia Electrónica

11. Observaciones y recomendaciones