UNIVERSIDAD DE MURCIA

1. Identificación

1.1. De la asignatura

Curso Académico	2024/2025
Titulación	GRADO EN SEGURIDAD
Nombre de la asignatura	CIBERSEGURIDAD
Código	5145
Curso	CUARTO
Carácter	OPTATIVA
Número de grupos	2
Créditos ECTS	4.5
Estimación del volumen de trabajo	112.5
Organización temporal	1º Cuatrimestre
Idiomas en que se imparte	Español

1.2. Del profesorado: Equipo docente

CASTILLO FELIPE, RAFAEL

Docente: **GRUPO 1, GRUPO 1**

Coordinación de los grupos:

Coordinador de la asignatura

Categoría
CA

Área
DERECHO PROCESAL

Departamento
DERECHO FINANCIERO, INTERNACIONAL Y PROCESAL

Correo electrónico / Página web / Tutoría electrónica
rafael.castillo@um.es rafael.castillo@um.es Tutoría electrónica: **Sí**

Teléfono, horario y lugar de atención al alumnado

Duración:	Día:	Horario:	Lugar:
A	Jueves	17:30-18:30	No consta

Observaciones:
Previa cita

Duración:	Día:	Horario:	Lugar:
A	Viernes	08:00-11:00	(Sin Extensión), Paraninfo y Edificio Rector Loustau B1.0A.019

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
A	Martes	18:30-20:30	No consta

Observaciones:
No consta

CASTILLO FELIPE, RAFAEL

Docente: **GRUPO 1, GRUPO 1**

Coordinación de los grupos:

Coordinador de la asignatura

Categoría
CA

Área
DERECHO PROCESAL

Departamento
DERECHO FINANCIERO, INTERNACIONAL Y PROCESAL

Correo electrónico / Página web / Tutoría electrónica
rafael.castillo@um.es rafael.castillo@um.es Tutoría electrónica: **Sí**

Teléfono, horario y lugar de atención al alumnado

Duración:	Día:	Horario:	Lugar:
A	Jueves	17:30-18:30	No consta

Observaciones:
Previa cita

Duración:	Día:	Horario:	Lugar:
A	Viernes	08:00-11:00	(Sin Extensión), Paraninfo y Edificio Rector Loustau B1.0A.019

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
A	Martes	18:30-20:30	No consta

Observaciones:
No consta

DIAZ CARRILLO, JUAN MANUEL

Docente: **GRUPO 1, GRUPO ONLINE**

Coordinación de los grupos: **GRUPO 1, GRUPO ONLINE**

Coordinador de la asignatura

Categoría
CA

Área
No consta

Departamento
No consta

Correo electrónico / Página web / Tutoría electrónica
juanmanuel.diaz1@um.es Tutoría electrónica: **No**

Teléfono, horario y lugar de atención al alumnado

2. Presentación

La ciberseguridad es una disciplina esencial en el mundo moderno, ya que protege los sistemas, redes y datos contra ataques digitales. En un entorno cada vez más globalizado y digital, comprender los fundamentos de la ciberseguridad es crucial para cualquier organización o individuo que maneje información sensible. La ciberseguridad se centra en proteger la confidencialidad, integridad y disponibilidad de la información. A su vez, la cibercriminalidad abarca actividades delictivas que utilizan las tecnologías de la información para perpetrar delitos, como el robo de datos, fraude y sabotaje.

Para abordar eficazmente estos desafíos, es necesario implementar estándares de ciberseguridad que proporcionen un marco para medidas de prevención efectivas. Ejemplos de estos estándares incluyen ISO/IEC 27001 y NIST, que establecen directrices para gestionar la seguridad de la información, las cuales son esenciales para proteger contra vulnerabilidades y amenazas en constante evolución.

El análisis de malware desempeña un papel fundamental en la comprensión de cómo operan los ciberataques. Los cibercriminales emplean diversas técnicas y herramientas, como virus, gusanos, troyanos, ransomware y spyware, para comprometer sistemas y datos. Además, los ciberataques pueden involucrar técnicas sofisticadas como el phishing, ataques de denegación de servicio (DDoS) y exploits de día cero, que explotan vulnerabilidades no conocidas previamente por los desarrolladores de software.

Los cibercriminales varían en perfiles, desde individuos que operan solos hasta grupos organizados y insiders con acceso privilegiado a los sistemas de una organización. Por otro lado, las cibervíctimas incluyen desde individuos y pequeñas empresas hasta grandes corporaciones y gobiernos, cada uno enfrentando diferentes tipos de amenazas y riesgos que pueden tener graves repercusiones económicas, de reputación y operativas.

En este contexto, la cibercriminalidad no solo afecta a las organizaciones a nivel económico, sino que también puede comprometer la seguridad nacional y la infraestructura crítica. El ciberespacio, el entorno virtual en el que se desarrollan las interacciones digitales, ha visto surgir nuevas amenazas internacionales como el ciberterrorismo, el espionaje cibernético y los ataques a infraestructuras críticas, lo que requiere una vigilancia constante y una colaboración internacional efectiva para ser mitigadas.

El hacking ético emerge como una práctica vital en la ciberseguridad, donde expertos autorizados evalúan la seguridad de los sistemas mediante pruebas controladas. Estas prácticas de prevención incluyen pruebas de penetración (pentesting), auditorías de seguridad y programas de recompensas por la identificación de vulnerabilidades (bug bounty), todas dirigidas a fortalecer las defensas cibernéticas.

Diversos organismos internacionales y nacionales están dedicados a combatir la cibercriminalidad. Organizaciones como INTERPOL, Europol y el FBI juegan roles cruciales en la identificación, persecución y prevención de delitos cibernéticos. Además, iniciativas de cooperación internacional y conferencias de ciberseguridad facilitan el intercambio de información y la colaboración en la lucha contra estas amenazas globales.

3. Condiciones de acceso a la asignatura

3.1. Incompatibilidades

No constan

3.2. Requisitos

No constan

3.3. 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

- CM1-Capacidad para analizar y valorar el ámbito de la seguridad en el espacio virtual o cibernético (CE10, CE18)
- CM2- Capacidad para conocer las principales medidas de prevención en ciberseguridad en el ciberespacio (CE10, CE18)
- CM3- Comprensión de las principales tipologías criminales en el campo de la cibercriminalidad, así como las nuevas amenazas internacionales que surgen a raíz de las mismas (CE8, CE10, CE18)
- CM4- Conocer los principales ámbitos y procedimientos de la evaluación psicológica (CE10, CE18)
- CM5- Comprensión de los principales instrumentos y organismos internacionales en la erradicación de la cibercriminalidad (CE8, CE10, CE18)

5. Contenidos

5.1. Teoría

Tema 1: Fundamentos Ciberseguridad (Concepto de Ciberseguridad)

Tema 2: Estándares de Ciberseguridad (Medidas de Prevención de la Ciberseguridad).

Tema 3: Hacking Ético (Medidas de Prevención de la Ciberseguridad)

Tema 4: Componentes de un ciberataque.

Tema 5: Cibercriminalidad: Respuesta a una cibercrisis

Tema 6: Ciberespacio, cibercriminales y nuevas amenazas Internacionales

Tema 7: Organismos en la lucha contra la cibercriminalidad.

5.2. Prácticas

- **Práctica 1: Práctica 1: Metodologías de análisis en ciberinteligencia**
- **Práctica 2: Práctica 2: Preparación de un laboratorio de investigación de entornos ciber**
- **Práctica 3: Práctica 3: Ciberinteligencia IMINT**
- **Práctica 4: Práctica 4: Ciberinteligencia OSINT**
- **Práctica 5: Práctica 5: Hacking ético**

6. Actividades Formativas

Actividad Formativa	Metodología	Horas	Presencialidad
AF1: Exposición teórica: clase magistral.		33.8	100.0
AF2: Tutorías o trabajos dirigidos.		2.2	100.0
AF3: Resolución de problemas, simulaciones y estudios de casos; seminarios especializados; aprendizaje orientado a proyectos; exposición y discusión de trabajos.		9.0	100.0
AF5: Trabajo autónomo del estudiante		67.5	0.0
	Totales	112,50	

7. Horario de la asignatura

https://www.um.es/web/estudios/grados/seguridad /2024-25#horarios

8. Sistemas de Evaluación

GRUPO 1

	Criterios

Identificador	Denominación del instrumento de evaluación	de Valoración	Ponderación
SE1	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.		60.0
SE2	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.		20.0
SE3	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.		10.0
SE4	Procedimientos de observación del trabajo del estudiante: registros de participación, de realización de actividades, cumplimiento de plazos, participación en foros		10.0

GRUPO ONLINE

Identificador	Denominación del instrumento de evaluación	Criterios de Valoración	Ponderación
SE1	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.		60.0
SE2	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.		20.0
SE3	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.		10.0
SE4	Procedimientos de observación del trabajo del estudiante: registros de participación, de realización de actividades, cumplimiento de plazos, participación en foros		10.0

9. Fechas de exámenes

https://www.um.es/web/estudios/grados/seguridad /2024-25#examenes

10. Resultados del Aprendizaje

- RA1- Conocer la evolución del comportamiento criminal a través del ciberespacio
- RA2- Capacidad para identificar las medidas de ciberseguridad más eficaces en la lucha contra la cibercriminalidad dependiendo de la oportunidad criminal y de la tipología delictiva
- RA3- Saber apreciar y reflexionar sobre los nuevos perfiles de ciberdelincuentes, así como de las cibervíctimas

- RA4- Ser capaz de identificar los componentes de equipos informáticos, así como la metodología de análisis forense, evidencia digital, cadena de custodia u otras herramientas forenses
- RA5- Conocimiento de los organismos nacionales e internacionales en la lucha contra la cibercriminalidad e implicados en la actualización de los sistemas de ciberseguridad

11. Bibliografía

Bibliografía básica

- - ISO 27001, de Sistemas de gestión. AENOR.
- Instituto Nacional de Ciberseguridad.

Bibliografía complementaria

- - ISO 19011, Directrices para la auditoría de los sistemas de gestión. AENOR.
- Barrio Andrés, M., Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos, Wolters Kluwer, Las Rozas (Madrid), 2018.
- Memento Experto en Ciberseguridad, Francis Lefebvre, Madrid, 2021.
- - Estrategia nacional de ciberseguridad, año 2019.
- - OWASP. Análisis y gestión de riesgos.

12. Observaciones

NECESIDADES EDUCATIVAS ESPECIALES Aquellos estudiantes con discapacidad o necesidades educativas especiales podrán dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV; http://wwwumes/adyv/) para recibir orientación sobre un mejor aprovechamiento de su proceso formativo y, en su caso, la adopción de medidas de equiparación y de mejora para la inclusión, en virtud de la Resolución Rectoral R-358/2016 El tratamiento de la información sobre este alumnado, en cumplimiento con la LOPD, es de estricta confidencialidad

Esta asignatura se encuentra vinculada de forma directa con el Objetivo de Desarrollo Sostenible número 16: "Paz, justicia e instituciones sólidas"

NECESIDADES EDUCATIVAS ESPECIALES

Aquellos estudiantes con discapacidad o necesidades educativas especiales podrán dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV - https://www.um.es/adyv) para recibir orientación sobre un mejor aprovechamiento de su proceso formativo y, en su caso, la adopción de medidas de equiparación y de mejora para la inclusión, en virtud de la Resolución Rectoral R-358/2016. El tratamiento de la información sobre este alumnado, en cumplimiento con la LOPD, es de estricta confidencialidad.

REGLAMENTO DE EVALUACIÓN DE ESTUDIANTES

El artículo 8.6 del Reglamento de Evaluación de Estudiantes (REVA) prevé que "salvo en el caso de actividades definidas como obligatorias en la guía docente, si el o la estudiante no puede seguir el proceso de evaluación continua por circunstancias sobrevenidas debidamente justificadas, tendrá derecho a realizar una prueba global".

Se recuerda asimismo que el artículo 22.1 del Reglamento de Evaluación de Estudiantes (REVA) estipula que "el o la estudiante que se valga de conductas fraudulentas, incluida la indebida atribución de identidad o autoría, o esté en posesión de medios o instrumentos que faciliten dichas conductas, obtendrá la calificación de cero en el procedimiento de evaluación y, en su caso, podrá ser objeto de sanción, previa apertura de expediente disciplinario".