1. DATOS BÁSICOS

Asignatura	Dimensiones de la Seguridad
Titulación	Grado en Ingeniería de la Ciberseguridad
Escuela/ Facultad	Escuela de Arquitectura, Ingeniería y Diseño
Curso	Primero
ECTS	6 ECTS
Carácter	Básico
Idioma/s	Castellano/inglés
Modalidad	Online/Presencial
Semestre	Segundo semestre
Curso académico	2024-2025
Docente coordinador	Ramón Rizo Gómez
Docente	Ramón Rizo Gómez

2. PRESENTACIÓN

La seguridad constituye uno de los anhelos del ser humano, cualquiera que sea el ámbito en el que se desenvuelva. La aparición y espectacular desarrollo de un nuevo contexto ausente de corporeidad como es el ciberespacio, no se ha producido en ausencia de la aparición de amenazas y, por ende, de una exacerbación de esos deseos de sentirse a salvo de amenazas, máxime ante un hábitat que de la mano del desconocimiento de este y la sofisticación tecnológica todavía se percibe como más incontrolable.

Difícilmente podemos defendernos de lo desconocido, puesto que la ignorancia de sus cualidades hace que no podamos establecer contramedidas adecuadas. Por ello, quien debe acometer la misión de asegurar un sistema de gestión de la información debe conocer no solo las posibles amenazas, sino también los actores que las ponen en práctica y la motivación que subyace a sus conductas.

Debemos, por tanto, tener una idea clara de contexto en el que está inscrita nuestra organización, empresa, organismo público o cualquier otro ente en el que desarrollaremos nuestro cometido, para ser conscientes de las amenazas a las que nos enfrentamos y la forma de blindar nuestros activos.

Esta asignatura está incluida dentro del módulo “Ciberseguridad” formado por las siguientes asignaturas:

- Dimensiones de la seguridad (6 ECTS)
- Criptografía (6 ECTS)
- Técnicas de Hacking (6 ECTS)
- Metodologías de desarrollo seguro (6 ECTS)
- Diseño y análisis de algoritmos (6 ECTS)

- Seguridad en base de datos (6 ECTS)
- Seguridad en redes (6 ECTS)
- Desarrollo seguro de web y apps (6 ECTS)
- Malware y amenazas dirigidas (6 ECTS)
- Auditoría (6 ECTS)
- Pentesting (6 ECTS)

Security is one of the desires of human beings, regardless of the environment in which they operate. The appearance and spectacular development of a new context devoid of corporeality such as cyberspace, has not occurred in the absence of the appearance of threats and, therefore, of an exacerbation of those desires to feel safe from threats, especially in the face of a habitat that, hand in hand with ignorance of it and technological sophistication, is still perceived as more uncontrollable.

We can hardly defend ourselves from the unknown, since ignorance of its qualities means that we cannot establish adequate countermeasures. Therefore, whoever must undertake the mission of securing an information management system must know not only the possible threats, but also the actors who put them into practice and the motivation underlying their behavior.

We must therefore have a clear idea of the context in which our organization, company, public body or any other entity in which we will carry out our work is registered, in order to be aware of the threats we face and how to protect our assets.

This subject is included in the "Cybersecurity" module, which is made up of the following subjects:

• Dimensions of security (6 ECTS)
• Cryptography (6 ECTS)
• Hacking techniques (6 ECTS)
• Secure development methodologies (6 ECTS)
• Design and analysis of algorithms (6 ECTS)
• Database security (6 ECTS)
• Network security (6 ECTS)
• Secure web and app development (6 ECTS)
• Malware and targeted threats (6 ECTS)
• Auditing (6 ECTS)
• Pentesting (6 ECTS)

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Conocimientos

CON06. Describir el concepto de ciberseguridad y sus pilares fundamentales e implicaciones en un contexto globalizado, tecnológico y conectado como el actual.

- Describir el concepto, evolución histórica y transformación de la seguridad en el ámbito internacional
- Definir el concepto de ciberseguridad
- Diferenciar las estrategias de seguridad de las diferentes organizaciones globales

CON08. Enumerar las etapas o pasos que los atacantes siguen para construir sus ataques, así como los patrones de ataque más graves e importantes y los entornos de seguridad ofensiva.

- Describir el concepto de terrorismo y criminalidad organizada en el ámbito de la ciberseguridad

- Diferenciar los sistemas de protección aplicados a infraestructuras críticas, energéticas, aeroespaciales, marítimas y civiles.
- Describir la estrategia de Seguridad Nacional Española

CON06. Describing the concept of cybersecurity and its fundamental pillars and implications in a globalized, technological, and connected context like the current one:

- Describing the concept, historical evolution, and transformation of security in the international arena.
- Defining the concept of cybersecurity.
- Differentiating security strategies of various global organizations.

CON08. Enumerating the stages or steps that attackers follow to construct their attacks, as well as the most severe and important attack patterns and offensive security environments:

- Describing the concept of terrorism and organized crime in the realm of cybersecurity.
- Differentiating protection systems applied to critical infrastructure, energy, aerospace, maritime, and civilian sectors.
- Describing the Spanish National Security strategy.

Habilidades

Competencias

CP09. Escoger el tipo de auditoría más adecuado para cada contexto, ejecutar dichas auditorías con las herramientas más adecuadas, y analizar los resultados obteniendo conclusiones relevantes.

CP11. Identificar y evaluar los riesgos y amenazas en una organización en todos los aspectos relacionados con la ciberseguridad.

CP13. Transmitir mensajes (ideas, conceptos, sentimientos, argumentos), tanto de forma oral como escrita, alineando de manera estratégica los intereses de los distintos agentes implicados en la comunicación.

CP14. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.

CP19. Mostrar comportamientos éticos y compromiso social en el desempeño de las actividades de una profesión, así como sensibilidad a la desigualdad y a la diversidad.

CP09. Selecting the most appropriate type of audit for each context, executing these audits with the most suitable tools, and analyzing the results to draw relevant conclusions.

CP11. Identifying and evaluating risks and threats within an organization in all aspects related to cybersecurity.

CP13. Communicating messages (ideas, concepts, feelings, arguments) both orally and in writing, strategically aligning the interests of the various stakeholders involved in the communication.

CP14. Utilizing information and communication technologies for data search and analysis, research, communication, and learning.

CP19. Demonstrating ethical behavior and social commitment in the performance of professional activities, as well as sensitivity to inequality and diversity.

Resultados de aprendizaje:

RA1. Describir el concepto, evolución histórica y transformación de la seguridad en el ámbito internacional
RA2. Definir el concepto de ciberseguridad
RA3. Diferenciar las estrategias de seguridad de las diferentes organizaciones globales
RA4. Describir el concepto de terrorismo y criminalidad organizada en el ámbito de la ciberseguridad
RA5. Diferenciar los sistemas de protección aplicados a infraestructuras críticas, energéticas, aeroespaciales, marítimas y civiles.
RA6. Describir la estrategia de Seguridad Nacional Española

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CP09	Escoger el tipo de auditoría más adecuado para cada contexto, ejecutar dichas auditorías con las herramientas más adecuadas, y analizar los resultados obteniendo conclusiones relevantes
CP11	Identificar y evaluar los riesgos y amenazas en una organización en todos los aspectos relacionados con la ciberseguridad
CP13	Transmitir mensajes (ideas, conceptos, sentimientos, argumentos), tanto de forma oral como escrita, alineando de manera estratégica los intereses de los distintos agentes implicados en la comunicación
CP14	Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje
CP19	Mostrar comportamientos éticos y compromiso social en el desempeño de las actividades de una profesión, así como la sensibilidad a la desigualdad y a la diversidad

Skills	Learning outcome
CP09	Selecting the most appropiate type of audit for each context, executing these audits with the most suitable tools, and analyzing the results to draw relevant conclusions
CP11	Identifying and evaluating risks and threats within an organization in all aspects related to cybersecurity
CP13	Communicating messages (ideas, concepts, feelings, arguments) both orally and in writing, strategically, aligning the interest of the various stakeolders involved in the communication
CP14	Utilizing information and communication technologies for data search and analysis, research, communication, and learning
CP19	Demostrating ethical behavior and social commitment in the performance of professional activities, as well as sensitivity to inequality and diversity

4. CONTENIDOS

- Seguridad y globalización
- Los riesgos y amenazas de seguridad en el siglo XXI
- El concepto de seguridad: evolución e implicaciones
- El concepto de seguridad: evolución e implicaciones.
- Nuevos paradigmas de seguridad
- Las respuestas institucionales: las estrategias de seguridad nacional.
- La política común de seguridad y defensa de la UE. La estrategia europea de seguridad
- Estrategia de Seguridad Nacional Española

- Security and globalization.
- Security risks and threats in the 21st century.
- The Concept of Security: Evolution and Implications.
- New Security Paradigms
- Institutional Responses: National Security Strategies.
- The EU's Common Security and Defence Policy. The European Security Strateg
- Spanish National Security Strategy

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:

- Clase magistral / web conference
- Método del caso
- Aprendizaje cooperativo

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad presencial:

Actividad formativa	Número de horas
Clases magistrales	8
Seminarios de aplicación práctica	26
Análisis de casos	32
Resolución problemas	0
Exposiciones orales de trabajos	6
Elaboración de informes y escritos	22
Trabajo autónomo	50
Debates y coloquios	4

Pruebas presenciales de conocimiento	2
TOTAL	**150**

Modalidad virtual:

Actividad formativa	Número de horas
Clases magistrales	8
Clases virtuales síncronas	26
Análisis de casos	32
Exposiciones orales síncronas de trabajos	6
Elaboración de informes y escritos	22
Estudio de contenidos y documentación complementaria (trabajo autónomo)	50
Foro virtual	4
Pruebas virtuales de conocimiento	2
TOTAL	**150**

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad presencial:

Sistema de evaluación	Peso

Modalidad virtual:

Sistema de evaluación	Peso
Pruebas de evaluación virtuales	60 %
Casos/problema	30 %
Exposiciones orales síncronas	5 %
Observación del desempeño	5 %
Total	100 %

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de las actividades.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria extraordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de las actividades.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

Quien se presente a la convocatoria ordinaria y obtenga una puntuación global igual o superior a 5, superará la asignatura en dicha convocatoria, independientemente de los ejercicios presentados y calificados. En ningún caso será posible presentar con posterioridad trabajos no entregados en tiempo y forma, en convocatoria ordinaria, con el objetivo de mejorar la nota final obtenida en la convocatoria extraordinaria.

Igualmente, la entrega de los trabajos con posterioridad a que en la clase se haya efectuado la corrección y feedback de los mismos por parte del profesor, supondrá que la calificación obtenida sufrirá una reducción del 25 %.

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

Los exámenes de esta asignatura en la modalidad de impartición online, serán pruebas de evaluación virtuales, realizadas a través de la plataforma, no siendo en ningún caso exámenes presenciales.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Actividades evaluables	Fecha
1.- CIBERGUERRA	marzo 2025
2.- PREDICCIONES	abril 2025
3.- INTELIGENCIA APT	mayo 2025
4.- INFRAESTRUCTURAS CRÍTICAS	junio 2025

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

La obra de referencia para el seguimiento de la asignatura es:

- A Brief Guide to the History of the Internet. Invest Intech (n.d.), Archieved 2014, April 27. http://bit.ly/3URylB7
- A brief history of the internet. ScienceNote, 2017- http://bit.ly/3O28Smh
- ARPANET. (2022, 10 de octubre). Wikipedia, La enciclopedia libre. http://bit.ly/3hIfwCo
- Comprehensive Study on Cybercrime (2013), UNODC. http://bit.ly/3hItpAw
- Historia de la computación. (2022, 11 de noviembre). Wikipedia, La enciclopedia libre. http://bit.ly/3Ab4FHw
- History of Internet (nd.). N.D. Blog. Archieved 2022. http://bit.ly/3URAkFz
- History of Internet (nd). Dave.Marshall. Archieved 2022. https://bit.ly/3E357Zi
- Hobbes' Internet Timeline (nd). Hobbes. Archieved 2022. http://bit.ly/3g344AI
- Revolución Digital. (2022, 9 de noviembre). Wikipedia, La enciclopedia libre. http://bit.ly/3TwHwWO

10. UNIDAD DE ORIENTACIÓN EDUCATIVA, DIVERSIDAD E INCLUSIÓN

Desde la Unidad de Orientación Educativa, Diversidad e Inclusión (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades

específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.
Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

11. ENCUESTAS DE SATISFACCIÓN

¡Tu opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.

PLAN DE TRABAJO DE LA ASIGNATURA

CÓMO COMUNICARTE CON TU DOCENTE

Cuando tengas una duda sobre los contenidos o actividades, no olvides escribirla en los foros de tu asignatura para que todos tus compañeros y compañeras puedan leerla.

¡Es posible que alguien tenga tu misma duda!

Si tienes alguna consulta exclusivamente dirigida al docente puedes enviarle un mensaje privado desde el Campus Virtual. Además, en caso de que necesites profundizar en algún tema, puedes acordar una tutoría.

Es conveniente que leas con regularidad los mensajes enviados por estudiantes y docentes, pues constituyen una vía más de aprendizaje.

CRONOGRAMA DE ACTIVIDADES

En este apartado se indica el cronograma de actividades formativas, así como las fechas de entrega de las actividades evaluables de la asignatura:

Semana	Contenidos	Actividades formativas/evaluables	Peso en la evaluación de la actividad evaluable
1,2 y 3	Unidad UNO		
4,5 Y 6	Unidad DOS	Actividad UNO	5%
7,8 Y 9	Unidad TRES	Actividad DOS	5 %
10, 11 Y 12	Unidad CUATRO	Actividad TRES	10 %
13 Y 14	Unidad CINCO		
15 Y 16	Unidad SEIS	Actividad CUATRO	10%

Este cronograma podrá sufrir modificaciones que serán notificadas al estudiante en tiempo y forma.

DESCRIPCIÓN DE LAS ACTIVIDADES DE EVALUACIÓN

Actividad 1. Realizar un juicio crítico sobre la utilización de medios en la ciberguerra, en relación con la amenaza que constituye para las infraestructuras críticas

Actividad 2. Estudiar un informe predictivo sobre la evolución de la actividad delictiva y ciberamenazas y realizar una comparación con la realidad acontecida

Actividad 3. Realizar una búsqueda de información en relación con un objetivo determinado y elaborar un informe al respecto

Actividad 4. Estudiar un documento con información sobre un medio tecnológico y elaborar un informe en relación con su implicación como amenaza para las infraestructuras críticas

RÚBRICAS DE LAS ACTIVIDADES EVALUABLES

	No realizado/ Inadecuado	Poco adecuado	Adecuado	Muy adecuado
Habilidades de comunicación	Lenguaje confuso, errores gramaticales y ortográficos, nula argumentación	La redacción tiene errores de sintaxis, vocabulario poco profesional	Buena redacción, estilo adecuado, con algún error sintáctico	La redacción es ágil y de estilo profesional, la sintaxis correcta y el vocabulario variado
Fundamentación Y motivación	No hace referencia a documentos, normas o autores que respalden su trabajo	El número de normas y autores citados es limitado, en ocasiones hay errores	La fundamentación y motivación están adecuadamente referenciadas a textos y normativas	La fundamentación y motivación están perfectamente referenciadas a textos y normativas
Resultado final correcto Argumentación	No se da respuesta al problema planteado	Se da respuesta parcial al problema planteado	Se responden la mayoría de las cuestiones planteadas	Se da respuesta a todas las cuestiones planteadas
Planificación y estructuración	El ejercicio no sigue una línea argumental	Existe una línea argumental, pero la estructura no está definida	Existe una línea argumental y estructura clara y adecuada	La argumentación y estructuración es destacable

REGLAMENTO PLAGIO

Atendiendo al Reglamento disciplinario de los estudiantes de la Universidad Europea:

- El plagio, en todo o en parte, de obras intelectuales de cualquier tipo se considera falta muy grave.
- Las faltas muy graves relativas a plagios y al uso de medios fraudulentos para superar las pruebas de evaluación, tendrán como consecuencia la pérdida de la convocatoria correspondiente, así como el reflejo de la falta y su motivo, en el expediente académico.

REGLAMENTO USO DE IA

El estudiante debe ser el autor o autora de sus trabajos/actividades.

El uso de herramientas de Inteligencia Artificial (IA) debe ser autorizado por el docente en cada trabajo/actividad, indicando de qué manera está permitido su uso. El docente informará previamente en qué situaciones se podrá usar herramientas de IA para mejorar la ortografía, gramática y edición en general. El estudiante es responsable de precisar la información dada por la herramienta y declarar

debidamente el uso de cualquier herramienta de IA, en función de las directrices que marque el docente. La decisión final sobre la autoría del trabajo y la idoneidad del uso reportado de una herramienta de IA recae en el docente y en los responsables de la titulación.