1. DATOS BÁSICOS

Asignatura	Principios Jurídicos básicos aplicados a la ciberseguridad
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 ciberseguridad, al igual que cualquier otro aspecto de nuestra vida diaria en sociedad, está regulada por un conjunto de normas jurídicas que determinan derechos, obligaciones y prohibiciones que deberán tomar en consideración todos los actores que participen en alguna actividad relacionada con la misma.
El Ingeniero en ciberseguridad no está al margen de lo anterior, al contrario, precisamente él, asumirá en algunos casos el papel de CISO encargado, por tanto, de que la organización en la que desempeña tal papel no solo cumpla con la normativa, sino que esté en disposición de demostrarlo, manteniendo las evidencias documentales necesarias para ello.

Por tanto, es imprescindible que, junto complemente su competencia tecnológica con unos conocimientos legales básicos que le permitan conocer la estructura jurídica y la normativa nacional, europea e internacional, aplicable al ámbito de la ciberseguridad tanto en el contexto público como en el privado.

Esta asignatura está incluida dentro del módulo “Empresa y regulación” formado por las siguientes asignaturas:

- Empresa y legislación 6 ECTS (Curso 1º)
- Principios jurídicos básicos aplicados a la ciberseguridad 6 ECTS (Curso 1º)
- Análisis y gestión del riesgo 6 ECTS (Curso 4º)
- Regulación y gobernanza de la seguridad 6 ECTS (Curso 4º)

Cybersecurity, like any other aspect of our daily life in society, is regulated by a set of legal rules that determine rights, obligations and prohibitions that must be taken into consideration by all actors who participate in any activity related to it.
The cybersecurity engineer is not exempt from the above, on the contrary, he will in some cases assume the role of CISO, therefore, in charge of ensuring that the organization in which he plays such a role not only complies with the regulations, but is also able to demonstrate it, maintaining the necessary documentary evidence for this.

Therefore, it is essential that, together with his technological competence, he complements his basic legal knowledge that allows him to know the legal structure and national, European and international regulations, applicable to the field of cybersecurity in both the public and private context.

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

- Business and legislation 6 ECTS (1st year)
- Basic legal principles applied to cybersecurity 6 ECTS (1st year)
- Risk analysis and management 6 ECTS (4th year)
- Security regulation and governance 6 ECTS (4th year)

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Conocimientos
CON09. Examinar la legislación nacional e internacional que se aplica a la ciberseguridad y a sus profesionales, así como el concepto de ciberdelito, su modelo de negocio y sus implicaciones.

- Identificar la legislación y código ético necesario para la labor profesional en el sector de la ciberseguridad
- Reconocer la legislación nacional e internacional que se aplica a la ciberseguridad y a sus profesionales
- Identificar la legislación nacional e internacional que se aplica a la protección de datos

CON09. Examining the national and international legislation applied to cybersecurity and its professionals, as well as the concept of cybercrime, its business model, and its implications.

- Identifying the legislation and ethical code necessary for professional work in the cybersecurity sector.
- Recognizing the national and international legislation applied to cybersecurity and its professionals.
- Identifying the national and international legislation applied to data protection.

Habilidades

HAB03. Analizar concepto de empresa, su marco institucional y jurídico, reconociendo los sistemas básicos de organización y gestión de empresas.

- Describir el concepto de ciberdelito, su modelo de negocio y sus implicaciones
- Describir el factor ético del profesional de la ciberseguridad
- Detallar el concepto de hacking ético

HAB03. Analyzing the concept of a company, its institutional and legal framework, recognizing the basic systems of organization and management of companies.

- Describing the concept of cybercrime, its business model, and its implications.
- Describing the ethical factor of cybersecurity professionals.
- Detailing the concept of ethical hacking.

Competencias

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.
CP16. Cooperar con otros en la consecución de un objetivo compartido, participando de manera activa, empática y ejerciendo la escucha activa y el respeto a todos los integrantes.
CP19. Mostrar comportamientos éticos y compromiso social en el desem-peño de las actividades de una profesión, así como sensibilidad a la desigualdad y a la diversidad.

CP11. Identifying and assessing risks and threats in an organization in all aspects related to cybersecurity.
CP13. Transmitting messages (ideas, concepts, feelings, arguments), both orally and in writing, strategically aligning the interests of the various parties involved in communication.
CP16. Cooperating with others in achieving a shared objective, participating actively, empathetically, and practicing active listening and respect for all members.
CP19. Demonstrating ethical behavior and social commitment in the performance of professional activities, as well as sensitivity to inequality and diversity.

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
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
CP16	Cooperar con otros en la consecución de un objetivo compartido, participando de manera activa, empática y ejerciendo la escucha activa y el respeto a todos los integrantes

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

Competencias	Resultados de aprendizaje
CP11	Identifying and assessing risks and threats in an organization in all aspects retaled to cybersecurity
CP13	Transmitting messages (ideas, concepts, feelings, arguments), both orally and in writing, strategically aligning the interest of the various
CP16	Cooperating with others in achieving a shared objective, participating actively, empathetically, and practicing active listening and respect for all members
CP19	Demonstrating ethical behavior and social commitment in the performance of professional activities, as well as sensitivity to inequality and diversity

4. CONTENIDOS

- Marco jurídico del Derecho de la ciberseguridad.
- La regulación legal de los servicios de información.
- La protección de datos personales
- Introducción al Derecho Penal de la Ciberseguridad
- La importancia de la ética profesional
- Hacking Ético

- Legal Framework of Cybersecurity Law
- Legal Regulation of Information Services.
- Protection of Personal Data.
- Introduction to Cybersecurity Criminal Law.
- The Importance of Professional Ethics.
- Ethical Hacking.

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 basado en problemas.

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	40
Exposiciones orales de trabajos	2
Elaboración de informes y escritos	18
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	40
Exposiciones orales síncronas de trabajos	2
Elaboración de informes y escritos	18
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 %

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.

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.

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
EJERCICIO 1 DERECHO DERIVADO DE LA UNIÓN EUROPEA	MARZO 2025
EJERCICIO 2 PROTOCOLOS DE CIBERSEGURIDAD	ABRIL 2025
EJERCICIO 3 PROTECCIÓN DE DATOS PERSONALES	MAYO 2025
EJERCICIO 4 ENCRIPTACIÓN EXTREMO A EXTREMO	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:

- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

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. Estudiar un documento elaborado por un organismo de la Unión Europea con el objetivo de comprender la importancia que tiene la normativa Europea mediante su aplicación o proyección en el marco jurídico nacional que regula los aspectos normativos de la ciberseguridad

Actividad 2. Leer y analizar algunas Sentencias Judiciales relativas a delitos informáticos, para a continuación y en base a las lecciones aprendidas realizar una traslación de estas a la elaboración de una política de seguridad tendente a evitar las brechas de seguridad

Actividad 3. Leer y analizar un informe elaborado por la Agencia Española de Protección de Datos y de órganos judiciales en relación con la cesión y uso por empresas de datos biométricos

Actividad 4. Estudiar un documento de la Unión Europea y una sentencia del Tribunal Europeo de Derechos Humanos y redactar un documento donde se analice lo sucedido, incorporando finalmente la propia opinión en relación con el equilibrio entre privacidad y seguridad, así como las consecuencias que esto tiene para la ciberseguridad.

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.