1. DATOS BÁSICOS

Asignatura	Seguridad de la información y programas de cumplimiento
Titulación	Máster Universitario en Protección de Datos por la Universidad Europea de Madrid.
Escuela/ Facultad	Facultad de Ciencias Sociales y de la Comunicación
Curso	1
ECTS	6
Carácter	Obligatorio
Idioma/s	Español
Modalidad	Online
Semestre	1er semestre
Curso académico	2024/2025
Docente coordinador	Ramón Rizo

2. PRESENTACIÓN

La programación curricular de este máster se ha articulado con el objetivo de hacer referencia, durante el primer semestre, a las cuestiones más esenciales relativas a la protección de datos. En este módulo se estudiarán cuestiones relacionadas con la seguridad de la información y los programas de cumplimiento desde la óptica de protección de datos.

En concreto, en este módulo, el estudio de la normativa de protección de datos se centrará en abordarlo desde la óptica de la ciberseguridad, de manera que será un análisis más técnico de cuestiones relacionadas con la seguridad, el análisis de riesgos, la evaluación de impacto y otras cuestiones de interés en este sentido.

El contenido principal que se abordará estará compuesto por los siguientes puntos:

1. Ciberseguridad y responsabilidad por activa.

2. Marco normativo de la seguridad de la información.

3. Las violaciones de la seguridad. Notificación de violaciones de seguridad.

4. Ciberseguridad y gobierno de la seguridad de la información

5. Programa de cumplimiento de Protección de Datos y Seguridad en una organización

6. Evaluación de Impacto de Protección de Datos “EIPD”.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

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.

CB7. Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB10. Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Competencias transversales:

CT1. Creatividad. Crear ideas nuevas y conceptos a partir de ideas y conceptos conocidos, llegando a conclusiones o resolviendo problemas, retos y situaciones de una forma original.CT2. Comunicación estratégica. 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.

CT3. Competencia digital. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.

CT4. Liderazgo influyente. Influir en otros para guiarles y dirigirles hacía unos objetivos y metas concretos, tomando en consideración sus puntos de vista, especialmente en situaciones derivadas de entornos volátiles, inciertos, complejos y ambiguos (VUCA) del mundo actual.

CT5. Trabajo en equipo. 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.

Competencias específicas:

CE1. Analizar el marco normativo de la protección de datos en España y la Unión Europea para la implementación en el mercado de tecnologías disruptivas.

CE2. Innovar en la interpretación del marco legal, organizativo y contractual que regula las actividades profesionales en el área de la protección de datos en diferentes sectores económicos.

CE4. Justificar, hipotetizar y razonar sobre la ampliación de los principios de seguridad y ciberseguridad para contribuir en el mejoramiento continuo del entorno de protección de datos.

CE6. Valorar y contrastar la normativa de protección de datos para su aplicación profesional en los principales sectores empresariales, tanto públicos como privados.

CE 11. Planificar y diseñar técnicas de cumplimiento normativo y políticas o guías en el ámbito de la protección de datos y la seguridad de la información en el marco de la prevención de posibles conductas antijuridicas.

CE 12. Desarrollar una visión crítica sobre los problemas contemporáneos asociados al marco de la protección de datos determinando medidas preventivas o alternativas para solucionar eficazmente las problemáticas detectadas.

CE 14. Aplicar de forma práctica e integradora los conocimientos, habilidades y competencias adquiridos en entornos profesionales relacionados con la protección de datos.

Resultados de aprendizaje:

1.- Proponer soluciones óptimas para articular los conceptos de ciberseguridad y responsabilidad activa.

2.- Interpretar de manera crítica el marco normativo de seguridad de la información.

3.- Desglosar la manera en la que ha evolucionado el principio de justicia universal.

4.- Investigar acerca de los procedimientos judiciales o administrativos que han tenido lugar con ocasión de violaciones a la seguridad de la información.

5.- Evaluar la eficacia de los programas de cumplimiento de protección de datos en organizaciones o empresas.

6.- Valorar los resultados de la aplicación de Evaluaciones de Impacto de Protección de Datos "EIPD".

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
CB1 y CB3 CT4, CT6, y CT8 CE7, CE9, CE10, y CE11	1.- Proponer soluciones óptimas para articular los conceptos de ciberseguridad y responsabilidad activa. 2.- Interpretar de manera crítica el marco normativo de seguridad de la información. 3.- Desglosar la manera en la que ha evolucionado el principio de justicia universal. 4.- Investigar acerca de los procedimientos judiciales o administrativos que han tenido lugar con ocasión de violaciones a la seguridad de la información. 5.- Evaluar la eficacia de los programas de cumplimiento de protección de datos en organizaciones o empresas. 6.- Valorar los resultados de la aplicación de Evaluaciones de Impacto de Protección de Datos "EIPD".

4. CONTENIDOS

1. Ciberseguridad y responsabilidad por activa.

2. Marco normativo de la seguridad de la información.

3. Las violaciones de la seguridad. Notificación de violaciones de seguridad.

4. Ciberseguridad y gobierno de la seguridad de la información

5. Programa de cumplimiento de Protección de Datos y Seguridad en una organización

6. Evaluación de Impacto de Protección de Datos "EIPD".

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

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

- Clase magistral/ web conference
- Aprendizaje cooperativo
- Aprendizaje basado en retos

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 online:

Actividad formativa	Número de horas
ACTIVIDADES FORMATIVAS DE LA MODALIDAD A DISTANCIA*	Nº de horas
Clases magistrales	10
Clases virtuales	20
Análisis de casos	12
Resolución de problemas	10
Elaboración de informes y escritos	10
Investigaciones y proyectos	10
Estudios de contenidos y documentación complementaria	50
Tutoría Virtual	18
Foro Virtual	8
Pruebas presenciales de conocimiento	2
Nº TOTAL	**150**

7. EVALUACIÓN

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

Modalidad online:

Sistema de evaluación	Peso
Casos/problemas	40
Pruebas **presenciales** de conocimiento	60

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 4,0 en la prueba final, para que la misma pueda hacer media con el resto de 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 4,0 en la prueba final, para que la misma pueda hacer media con el resto de 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.

8. CRONOGRAMA

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

Actividades evaluables	Fecha
Ciberseguridad y responsabilidad proactiva	24/02/2025
Violaciones de seguridad	14/03/2025

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

9. BIBLIOGRAFÍA

A continuación, se indica bibliografía recomendada:

- Álvarez Hernando, J. “Practicum de Protección de datos”. Editorial Aranzadi, Pamplona, 2021

- Davara Fernández de Marcos E. y L. "“Memento de Protección de Datos y derechos digitales”. Lefebvre, Madrid, 2023.

- Davara Fernández de Marcos E. y L. “Protección de datos: lo que nunca le han contado”, Wolters Kluwer- La Ley, 2022.

- Davara Fernández de Marcos E. y L. (Coords) “Análisis práctico de sanciones en materia de protección de datos divididas por conceptos y sectores”, Thomson Reuters Aranzadi, Pamplona, 2021.

- Davara Fernández de Marcos E. y L. “12ª ed. Manual de Derecho Informático”, Thompson Reuters-Aranzadi, Pamplona, 2020

- Davara Fernández de Marcos E. y L. “El Reglamento Europeo de protección de datos y la LOPDGDD: todo lo que necesitas saber”, Editorial WKE, Madrid, 2020.

- López-Calvo, J. “La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD (2.ª ed.), España, Editorial BOSCH, 2019.

- Ortega, A.: “Problemas que el Covid-19 plantea en el binomio transparencia y protección de datos. Aportación de soluciones prácticas desde la ciencia jurídica”. Thomson Reuters Aranzadi, Pamplona, 2022

- Simón, P. y Bacaria, J. (Coords.) “Las funciones del Delegado de Protección de Datos en los distintos sectores de actividad” - Sello Bosch- Editorial Wolters Kluwer. 2020

- Troncoso Reigada, A. (Coord.) “Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos y garantía de los derechos digitales”. Civitas- Thomson Reuters Aranzadi, 2021.

10. UNIDAD DE ATENCIÓN A LA DIVERSIDAD

Estudiantes con necesidades específicas de apoyo educativo:

Las adaptaciones o ajustes curriculares para estudiantes con necesidades específicas de apoyo educativo, a fin de garantizar la equidad de oportunidades, serán pautadas por la Unidad de Atención a la Diversidad (UAD).

Será requisito imprescindible la emisión de un informe de adaptaciones/ajustes curriculares por parte de dicha Unidad, por lo que los estudiantes con necesidades específicas de apoyo educativo deberán contactar a través de: unidad.diversidad@universidadeuropea.es al comienzo de cada semestre.

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.