GUÍA DOCENTE
2025 - 2026

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura

Nombre completo	Marco Normativo y Legislativo. Privacidad de los datos
Código	DTC-MCS-523
Impartido en	Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [Primer Curso] Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	3,0 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Telemática y Computación
Responsable	Marta Cañas
Horario	Segundo semestre

Datos del profesorado

Profesor

Nombre	Marta Concepción Cañas Miralles
Departamento / Área	Departamento de Telemática y Computación
Despacho	No se dispone de despacho, pero si es necesario se puede hacer uso de un aula
Correo electrónico	mccanas@icai.comillas.edu

Profesor

Nombre	Ofelia Tejerina Rodríguez
Departamento / Área	Facultad de Derecho (ICADE)
Correo electrónico	otejerina@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Aportación al perfil profesional de la titulación

Conocimiento teórico y práctico de la normativa y legislación existente en materia de ciberseguridad, privacidad, e inteligencia artificial. Independientemente del camino que se elija en la carrea profesional, es necesario conocer los que se debe cumplir para el correcto desarrollo de los proyectos. La normativa que se revisará es de ámbito nacional, europeo e internacional. Es importante tener este conocimiento para complementar el desarrollo de los conocimientos prácticos de ciberseguridad, privacidad e inteligencia artificial que se adopten en el resto de asignaturas.

Prerrequisitos

No hay prerrequisitos mínimos, es una asignatura transversal, que tiene explicaciones claras sobre la normativa y legislación en materia de ciberseguridad, privacidad y cualquier otro marco normativo que les afecte.

Competencias - Objetivos

Competencias

Conocer la legislación y normativa ligada a la ciberseguridad, privacidad e inteligencia artificial, para aplicarla en el día a día, ya sea en el entorno laboral aplicado directamente a privacidad, o bien en todos los trabajos relacionados con ciberseguridad

Resultados de Aprendizaje

Conocimiento de los aspectos normativos y legislación existente en la materia para aplicarlos en el mundo laboral, en los proyectos e incluso en nuestra vida diaria como usuarios de plataformas, aplicaciones, redes sociales, etc.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

BLOQUE I (9 sesiones)**: Protección de Datos Personales y Privacidad**

1. Contexto general:

- Tendencias, principios transversales (accountability, privacy by design & by default).
- Principios generales (consentimiento, licitud, lealtad, transparencia, limitación, minimización, exactitud, integridad, conservación).

2. Legislación de protección de datos

- **GDPR (UE)**: derechos de los individuos. Ejercicio de derechos, registros de decisiones automatizadas, revisión humana. Roles y gobernanza (responsable, encargado, DPO, DPIA, registros).
- **LOPDGDD (España)**: derechos digitales, particularidades nacionales.

3. Tratamientos de datos personales

- Definición y tipologías.
- Bases jurídicas, legitimación y categorías especiales.

4. Medidas de seguridad

- Medidas técnico-organizativas proporcionales.
- Control de accesos, cifrado, seudonimización, registros, continuidad, auditoría.

5. Brechas de seguridad (art. 33-34 GDPR)

- Notificación a autoridades (≤72h).
- Comunicación a interesados (alto riesgo).
- Registro y lecciones aprendidas.
- Aspectos procesales y garantías

6. Secretos empresariales (Ley 1/2019)

- Definición, protección, uso lícito/ilícito.

- Acciones legales, cláusulas contractuales, medidas organizativas y técnicas.

7. Auditorías de protección de datos

- Alcance, modelo y plan de acción.
- Qué se audita: registros, contratos, DPIA, medidas, brechas, derechos.

8. Autoridades y agencias (AEPD, EDPB, EDPS).

BLOQUE II (2 sesiones)**: Directiva NIS2 y Ciberseguridad**

1. Contexto general

- Relación entre ciberseguridad y privacidad.
- Principios de CIA (confidencialidad, integridad, disponibilidad).

2. Directiva NIS2

- Ámbito y sujetos obligados (sectores esenciales e importantes).
- Obligaciones principales: gestión de riesgos, cadena de suministro, seguridad operativa y del software.
- Informes de incidentes: aviso temprano (~24h), notificación (~72h), informe final (~1 mes).
- Supervisión, sanciones y responsabilidades directivas.
- Autoridades competentes: ENISA, CSIRTs, INCIBE, CCN-CERT.

3.Cumplimiento práctico y brechas de seguridad:

- Seguimiento, planes de remediación, pruebas y evidencias.
- Criterios de severidad (incidente significativo).
- Notificación y coordinación con CSIRTs.

4. Seguridad en la cadena de suministro

- Due diligence, contratos, evaluaciones periódicas.
- Evidencias, certificaciones, planes de continuidad.

5. Gestión de proyectos de ciberseguridad

- Seguridad desde el diseño y por defecto.
- DPO y CISO involucrados, trazabilidad, cumplimiento.

6. Esquema Nacional de Seguridad (ENS)

BLOQUE II (4 sesiones)**: Inteligencia Artificial (IA)**

1. Reglamento de IA (AI Act)

- Enfoque basado en riesgos.

- Aplicación directa y plazos graduales.

2. Clasificación de sistemas de IA

- Prácticas prohibidas.
- Sistemas de alto riesgo: requisitos de gobernanza, trazabilidad, transparencia, supervisión humana.
- Sistemas de riesgo limitado: obligaciones de transparencia.
- IA de propósito general y modelos fundacionales.

3. Aspectos técnicos y de cumplimiento

- Ciclo de vida de IA.
- Gestión de datos, sesgos, pruebas de robustez, red-teaming.
- Documentación técnica, fichas de modelo, registro en la UE.
- Trazabilidad y explicabilidad proporcional.
- Códigos de conducta.

4. Gobernanza y obligaciones prácticas

- Designación de responsables y canales de incidentes.
- Evaluaciones de impacto (DPIA/IA impact assessment).
- Supervisión post-despliegue y reporting.

5. Garantías de derechos

- Transparencia, consentimiento informado.
- Información clara a usuarios.
- Prevención de discriminación, explicabilidad, revisión humana.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Metodología Presencial: Actividades

Las clases son presenciales y obligatorias

Metodología No presencial: Actividades

En algunos casos se pueden enviar casos prácticos para revisar offline

RESUMEN HORAS DE TRABAJO DEL ALUMNO

2h a la semana en el segundo semestre + tiempo de dedicación fuera de las clases que dependerá de la asistencia y gestión de cada uno de los alumnos

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Trabajo continuo	El alumno deberá participar en todos los trabajos, individuales o colectivos que, con un carácter eminentemente práctico, indique el profesor.
Asistencia a clase	El alumno deberá asistir, como mínimo a un 80 % de las clases para poder valorar este ítem.
EXAMEN	El alumno deberá realizar el examen final de la asignatura, que podrá ser tipo test, desarrollo o mixto.

Calificaciones

1. La asistencia del alumno a clase (10% de la nota).
2. Preparación y participación activa en debates en las clases y actividades prácticas (20% de la nota).
3. Prueba final (70% de la nota)

Normas de uso de la IA

Se permite usar la IA para la parte de documentación, estudio y presentación de los temas elegidos por los alumnos, así como para el trabajo de laboratorio, en la medida prevista en los niveles 2 y 3 de la guía https://aiassessmentscale.com/ :

"La IA puede utilizarse para actividades previas a la tarea, como la lluvia de ideas, la descripción y la investigación inicial. Este nivel se centra en el uso de la IA para la planificación, las síntesis y la generación de ideas, pero las evaluaciones deben hacer hincapié en la capacidad de desarrollar y refinar estas ideas de forma independiente." y "La IA puede utilizarse para ayudar a completar la tarea, incluida la generación de ideas, la redacción, la retroalimentación y la evaluación. Los estudiantes deben evaluar y modificar críticamente los resultados sugeridos por la IA, demostrando su comprensión." En todo caso, el uso de la IA tiene que estar citado y las fuentes verificadas de forma independiente por el alumno. No se permite el uso de la IA en ninguna de las pruebas de examen, ni en los tests de evaluación del rendimiento."

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Reglamento general de protección de datos: Hacia un nuevo modelo europeo de protección de datos (Derecho administrativo). Ed. REUS. 2016. Dir. Jose Luís Piñar Mañas. Autores: Borja Adsuara Varela, Carlos Alonso Martínez, María Álvarez Caro, & 33 más.

El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Ed. WOLTERS KLUWER. 2018.Coord.: José López Calvo. Autores: Ana Aperribai Ulacia, Román Intxaurtieta Madariaga, Juan Antonio Toro Peña, Javier Puyol Montero , entre otros.

La figura del responsable en el derecho a la protección de datos. Ed. LA LEY. Autor: Belén Durán Cardo.

Cómo sobrevivir al GDPR. Ed. BOSCH. 2018. Autor: Wolters Kluwer.

Guías de ayuda de la Agencia Española de Protección de Datos: https://www.aepd.es/es/guias-y-herramientas/guias

Guías del Information Commissioner's Office (UK): https://ico.org.uk/for-organisations/guide-to-data-protection/

Ciberseguridad Ahora: Conceptos clave para gestionar el riesgo y asegurar los activos empresariales. Ed. Independently published. 2019. Autor: Víctor M Ruiz Lara.

El cisne negro: el impacto de lo altamente improbable. Ed. Planeta 2012. Autor: Nassim Nicholas Taleb.

Ingeniería social. El arte del hacking personal. Ed. ANAYA. 2011. Autor: Christopher Hadnagy.

The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Ed. Wiley Publishing, Inc. 2007. Autores: Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan Eren, Neel Mehta, and Riley Hassell.

Ethical Hacking. Un enfoque metodológico para profesionales. Ed. ALFAOMEGA. 2010. Autores: Ezequiel Sallis, Claudio Caracciolo y Marcelo Rodríguez.

Ciberseguridad y transformación digital: Cloud, Identidad Digital, Blockchain, Agile, Inteligencia Artificial. Ed. ANAYA. 2019. Autores: María Ángeles Caballero Velasco, Diego Cilleros Serrano.

How to Measure Anything in Cybersecurity Risk. Ed. WILEY. 2016. Autores: Douglas W. Hubbard, Richard Seiersen.