UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Memoria verificada del título oficial de

MÁSTER UNIVERSITARIO EN PROTECCIÓN DE DATOS

(Aprobado por ANECA el 31 de julio de 2014)

INDICE

1. DESCRIPCIÓN DEL TÍTULO

1.1. Datos básicos

Denominación	**Máster Universitario en Protección de Datos por la Universidad Internacional de La Rioja**
Tipo de Enseñanza	A distancia
Rama de conocimiento	Ciencias Sociales y Jurídicas
ISCED 1	380 - Derecho
ISCED 2	---
Profesión regulada	NO[1]
Lengua	Castellano
Facultad	Facultad de Derecho

1.2. Distribución de créditos en el título

Materias	Créditos ECTS
Obligatorias	50
Prácticas Externas	4
Trabajo Fin de Máster	6
Créditos totales	**60**

1.3. Plazas de nuevo ingreso ofertadas

Año de implantación	
Primer Año	100
Segundo Año	150

1.4. Número de créditos de matrícula por estudiante y período lectivo

	TIEMPO COMPLETO		TIEMPO PARCIAL	
	ECTS Matrícula Min	ECTS Matrícula Max	ECTS Matrícula Min	ECTS Matrícula Max
PRIMER AÑO	60	60	30	42
RESTO AÑOS	42	52	30	38

http://gestor.unir.net/userFiles/file/documentos/normativa/permanencia.pdf

[1] Pendiente de la Aprobación de la Propuesta de Reglamento General de Protección de Datos de la Unión Europea cuya Sección 4ª regula el Delegado de Protección de Datos.

2. JUSTIFICACIÓN, ADECUACIÓN Y PROCEDIMIENTOS

2.1. Interés académico, científico y profesional del título.

Vivimos en lo que el profesor Castells definió como "Galaxia Internet" o en la sociedad de la información, una sociedad cuyo valor principal reside en nuestra capacidad para procesar información y el conocimiento. En prácticamente todos los sectores productivos, y sin ninguna duda en el conjunto de la Administración, la información y el conocimiento poseen un valor estratégico. El camino de innovación tecnológica y social que nos ha traído hasta este punto vino marcada por distintos hitos que han definido un complejo marco regulador y han determinado la necesidad de contar con una categoría de profesional altamente especializado para su gestión y cumplimiento: *el data protection officer (DPO).*

La razón para la necesidad de esta figura es doble. En primer lugar, disciplinar el modo en el que se recoge y trata la información personal resulta fundamental para garantizar el adecuado funcionamiento de los sistemas de cualquier organización pública o privada, trate o no datos de carácter personal. Además, resulta esencial disponer de criterios claros en cualquier proceso de gestión que requiera uso de tecnologías de la información que se proyecten sobre el modo de ordenar la actividad de las organizaciones garantizando su funcionamiento.

En segundo lugar, el DPO se ocupa esencialmente del cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y toda la normativa conexa. El objetivo primario no es otro que la garantía del derecho fundamental a la protección de datos. Sin embargo, esta normativa es un instrumento que facilita la gestión de información y sus flujos de circulación ofreciendo un marco de seguridad jurídica indispensable para el desarrollo económico y social.

El desarrollo de políticas de implementación de la LOPD no puede resultar ni meramente formal ni epidérmico. No puede consistir en una decisión resignada, requiere de un compromiso activo de la organización. Una organización que se someta a un proceso de implantación de la LOPD debe transmitir verticalmente, desde el equipo directivo, al último de los trabajadores una idea de compromiso. La complejidad de la sociedad de la información determina en este ámbito promover un profundo cambio cultural. Diseñar una arquitectura de cumplimiento normativo que funcione sin fisuras obliga a comprometerse con un análisis riguroso y transparente del modelo de gestión y su incidencia en el tratamiento de información personal. Los resultados de una auditoría de cumplimiento normativo no tienen por qué afectar estructuralmente al modelo de gestión pero puede requerir adaptaciones que, sin el compromiso del que aquí se habla, podrían resultar traumáticas.

2.1.1 Interés académico y científico.

El ejercicio profesional del DPO sirve a la garantía del derecho fundamental a la protección de datos personales. El nacimiento de este derecho y su proyección futura poseen una relevancia académica y científica de primer nivel que, lejos de erigirse en un objeto de conocimiento sectorial propio de las ciencias jurídicas, se proyecta de manera instrumental sobre otras áreas de conocimiento lo que le confiere un rasgo multidisciplinar particularmente significativo.

El derecho fundamental a la protección de datos personales, y su marco regulador afectará a cualquier realidad de la vida en cualquiera de sus dimensiones, -económica, política, social, cultural, etc., a condición de que se requiera el tratamiento de datos personales. Baste con citar algunos ejemplos relevantes de este interés en las distintas áreas de conocimiento:

● Ciencias sociales.

Es imposible el desempeño de labores de investigación en ámbitos como la sociología, la economía, la sociología, el marketing y estudios de mercado, las ciencias actuariales, o el trabajo social sin recurrir a tratamientos de información personal. Pero además el análisis de datos personales puede ser en sí mismo un objeto primario de investigación en ámbitos como por ejemplo el del análisis comportamental.

● Ciencias de la salud.

El tratamiento de información personal en el ámbito de la salud no es sólo necesario desde el punto de vista asistencial. El despliegue de actividades investigadoras en esta materia obliga a adoptar estrategias de anonimización. Sin embargo, en muchas ocasiones la relación de identidad es relevante para los estudios cuando no existe la obligación de ser capaz de reconstruirla en el caso de las pruebas farmacológicas. Por otra parte, los estudios sobre condiciones de privacidad y seguridad de los ficheros y tratamientos con datos de salud desde enfoques éticos, jurídicos, técnicos e incluso puramente médicos poseen relevancia por sí mismos como condición indispensable para el desarrollo de la ciencia en éste ámbito.

● Humanidades.

La Historia de la Vida Privada escrita por George Duby, o las nucleares reflexiones de Benjamín Constant sobre la vida privada como soporte indispensable para garantizar la libertad política en las modernas democracias ponen de manifiesto que también en este ámbito el objeto del máster posee relevancia. Puede afirmarse, y para ello basta con leer las últimas noticias sobre el espionaje norteamericano para entender hasta qué punto en las futuras investigaciones sobre el periodo que arranca con la criptografía de ENIAC en la Segunda Guerra Mundial hasta nuestros días no podrán entenderse sin un análisis que abarque la conformación de la vida privada, sus instrumentos de garantía y sus violaciones.

● Ciencias Básicas.

La investigación básica en ámbitos como las redes neuronales y la neurobiología, la inteligencia artificial o la computación cuántica están sentando las bases para el desarrollo de la próxima generación de herramientas ordenadas al procesado masivo de información. Por otra parte, algunas áreas como la biotecnología-ingeniería genética guardan una relación directa material, ética y jurídica con la vida privada y el derecho fundamental a la protección de datos personales.

● Ciencias aplicadas y tecnológicas.

Biga Data, Etiquetas de Identificación por Radiofrecuencia-RFID, Cloud Computing, Wireless-Wimax, geolocalización, domótica, biónica, biometría, internet de las cosas… Todos estos conceptos expresan hasta qué punto existe una relación directa entre el conjunto de desarrollo que en el ámbito de la informática y de las telecomunicaciones y el objeto del máster que aquí se presente. Pero esta relación se convierte en objeto de estudio cuando nos referimos al conjunto de herramientas y técnicas cuyo objetivo es garantizar la seguridad de los datos.

● Ciencias jurídicas.

Finalmente y como es obvio es en el ámbito del estudio del Derecho donde los derecho relacionados con la vida privada y en particular el derecho fundamental a la protección de datos personales adquiere un carácter central. Especialmente en un momento de transición en el que realidades como las redes sociales, o las aplicaciones móviles desbordan las costuras de los ordenamientos tradicionales obligando a resolver

cuestiones esenciales como la determinación del Derecho aplicable en un mundo sin fronteras espacio-temporales o el desarrollo de instrumentos jurídicos que siendo capaces de garantizar las libertades individuales permitan el desarrollo del modelo económico emergente.

Prueba del interés académico e investigador lo ofrece una simple mirada a uno de los recursos más usuales a la hora de buscar bibliografía:

- Dialnet Publicaciones (http://dialnet.unirioja.es/).

Término de búsqueda: "protección de datos". Resultados directos 3054.

Búsquedas relacionadas:

- "Privacidad". Resultados directos: 830.
- "Datos personales". Resultados directos: 4396.

- Dialnet tesis doctorales (http://dialnet.unirioja.es/).

Término de búsqueda: "protección de datos". Resultados directos 106.

Este último término aunque parezca apuntar a un cierto volumen de producción demuestra, cuando a la búsqueda se le añaden aspectos sectoriales, la existencia de un amplio margen al esfuerzo investigador. Así:

Búsqueda	Núm. Tesis	Ciencias jurídicas
Protección de datos + redes sociales	3	0
Protección de datos + consentimiento	5	2
Protección de datos + Bigdata	0	0
Protección de datos+ cloud computing	0	0
Protección de datos + videovigilancia	0	0
Protección de datos + geolocalización	1	1
Protección de datos+ transparencia	1	0
Protección de datos open data	2	0
Búsqueda	**Núm. Tesis**	**Ciencias jurídicas**
Protección de datos+cookies	0	0
Protección de dato + análisis comportamental	0	0
Protección de datos + publicidad	26	2
Protección de datos + menores	19	1
Protección de datos + relaciones laborales	3	1
Protección de datos + salud	16	1
Protección de datos + Investigación biomédica	1	0
Protección de datos + Hacienda Pública	0	0
Protección de datos + Internet	8	3
Protección de datos + Internet de las cosas	0	0

Protección de datos + Aplicaciones Móviles	4	0
Encargado del tratamiento	2	0
Protección de datos + seguridad	22	4
Protección de datos + secreto	3	2
Protección de datos + Comunicaciones de datos	30	4
Protección de datos + Derechos de acceso, rectificación, cancelación y oposición.	0	0

Por su parte, una consulta al repositorio de información sobre tesis doctorales TESEO (https://www.educacion.gob.es/teseo/listarBusqueda.do) ofrece un resultado de veinticinco tesis con la búsqueda del término "protección de datos" en el título.

2.1.2 Interés profesional.

Es precisamente en este plano en el que se pone de manifiesto cómo el cumplimiento de la LOPD reviste una enorme dificultad desde el punto de vista del asesoramiento y exige profesionales altamente cualificados. Ello se debe a tres tipos de razones:

- No existe un cumplimiento "teórico" de la LOPD. Debe ajustarse a la realidad concreta del sector y a las características concretas de la organización. La empresa requiere saber "cómo cumplir" desde su concreta circunstancia. Las recetas genéricas, generalmente, son de imposible aplicación o imponen costes inasumibles.

- El carácter instrumental del derecho a la protección de datos comporta un alto grado de conocimiento jurídico de las normas sectoriales. Es imposible asesorar a una clínica médica a un hospital sin conocer cómo se regula la historia clínica, los análisis clínicos o la investigación biomédica. Existe una protección de datos personales en la salud, en los servicios financieros, en los seguros, en la seguridad privada etc.

- El jurista debe realizar un esfuerzo de adquisición de conocimientos complementarios que le permitan interactuar con otros profesionales. No es posible asesorar en protección de datos personales sin un mínimo de cultura informática. No se trata de reivindicar al jurista con perfil de informático, pero sí de partir de un conocimiento mínimo que permita un diálogo productivo. Y a la inversa sucede exactamente lo mismo, un experto en seguridad, negocio o marketing debe ser capaz de entender la trascendencia que para su actividad posee el cumplimiento de la legislación sobre protección de datos personales.

Por ello, el asesoramiento respecto del derecho de las tecnologías de la información y de las comunicaciones se está convirtiendo en un sector de alta especialización y el rigor de estos profesionales resulta estratégico en los procesos de implementación de la LOPD y en la garantía de las obligaciones jurídicas de las organizaciones en la sociedad de la información.

2.1.3 Datos adicionales.

Si bien no existen estudios empíricos que permitan establecer con precisión el escenario de mercado para los expertos en protección de datos, existen datos que permiten deducir de modo muy claro el interés académico de una titulación de esta naturaleza:

A. Va a ser un perfil profesional obligatorio.

La tramitación de Propuesta de Reglamento del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos) ha culminado con la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura). De aprobarse aquello que disponen su art 35 y ss.

Artículo 35
Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
a) el tratamiento sea llevado a cabo por una autoridad u organismo públicos; o
b) el tratamiento sea llevado a cabo por una persona jurídica con respecto a más de 5000 interesados durante un periodo consecutivo de 12 meses; o
c) las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados; o
d) las actividades principales del responsable o del encargado del tratamiento consistan en el tratamiento de categorías especiales de datos con arreglo al artículo 9, apartado 1, datos de localización o datos relativos a niños o a empleados en ficheros a gran escala.
2. Un grupo de empresas podrá nombrar un delegado principal de protección de datos responsable, siempre que se garantice que resulte fácil acceder a un delegado de protección de datos desde cualquier emplazamiento.
3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo públicos, el delegado de protección de datos podrá ser designado para varias de sus entidades, teniendo en cuenta la estructura organizativa de la autoridad u organismo públicos.
4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen categorías de responsables o encargados podrán designar un delegado de protección de datos.
5. El responsable o el encargado del tratamiento designarán el delegado de protección de datos atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar las tareas contempladas en el artículo 37. El nivel de conocimientos especializados requerido se determinará, en particular, en función del tratamiento de datos llevado a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado del tratamiento.
6. El responsable o el encargado del tratamiento velarán por que cualesquiera otras funciones profesionales del delegado de protección de datos sean compatibles con sus tareas y funciones en calidad de delegado de protección de datos y no planteen conflictos
7. El responsable o el encargado del tratamiento designarán un delegado de protección de datos para un mandato mínimo de cuatro años en el caso de un empleado o de dos años en el caso de un proveedor de servicios externos. El delegado de protección de datos podrá ser nombrado para nuevos mandatos. Durante su mandato, el delegado de protección de datos solo podrá ser destituido si deja de cumplir las condiciones requeridas para el ejercicio de sus funciones.
8. El delegado de protección de datos podrá ser empleado por el responsable o el encargado del tratamiento o desempeñar sus tareas sobre la base de un contrato de servicios.

9. El responsable o el encargado del tratamiento comunicarán el nombre y los datos de contacto del delegado de protección de datos a la autoridad de control y al público.
10. Los interesados tendrán derecho a entrar en contacto con el delegado de protección de datos para tratar todas las cuestiones relativas al tratamiento de datos que les conciernan y a solicitar el ejercicio de los derechos que les confiere el presente Reglamento.

En la práctica esta previsión normativa supone una necesidad de formación para proveer los oportunos perfiles funcionales:

● en las administraciones públicas españolas ya sea para formar personal preexistente ya sea con motivo de la convocatoria de procesos de selección de personal, ya sea con motivo de la externalización de estas funciones en el sector profesional;

● en personas jurídicas con más de 5000 empleados o clientes,

● en entidades que realicen operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados, como por ejemplo las de selección de personal, marketing comportamental y servicios asociados al asesoramiento personal o profesional (coaching);

● en entidades que traten datos especialmente protegidos (ideología, religión, creencias, salud, aspectos raciales o vida sexual);

● en organizaciones que traten datos datos de localización a gran escala (servicios de teletaxi, marketing o servicios basados en geolocalización etc.);

● en organizaciones que traten datos de menores a gran escala, lo que sucederá en el entero sector educativo;

● en organizaciones que traten datos de empleados a gran escala, lo que no sólo incluye empresas con un gran volumen de trabajadores sino también al entero sector de servicios de asesoramiento fiscal y laboral.

En la propuesta aprobada se subraya que «el responsable o el encargado del tratamiento designarán el delegado de protección de datos atendiendo **a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos**». Desde este punto de vista queda demostrado de modo muy preciso el interés del estudio ofrecido.

B. El grado de cumplimiento de las organizaciones españolas ofrece un amplio margen de negocio al sector, capaz de generar puestos de trabajo.

La Asociación Profesional Española de Privacidad, mediante nota de prensa emitida con motivo del Día Europeo de la Protección de Datos[2], señalaba cómo comparando las cifras de la última Memoria de la Agencia Española de Protección de Datos (2012) con el número de empresas que ofrecía el INE a 1 de enero de 2013, dos millones de organizaciones podrían no cumplir con los dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Comunidad Autónoma	Responsables[3]	Empresas[4]	Ficheros inscritos	Empresas que no habrían inscrito ningún fichero

[2] http://www.apep.es/28-de-enero-da-de-la-proteccin-de-datos-en-europa/
[3] Datos obtenidos sobre la distribución de ficheros de la Sección 4 de la Memoria 2012 de la Agencia Española de Protección de Datos. Pag.92.
[4] Fuente. Nota de prensa de 1 de Agosto del INE. Estructura y dinamismo del tejido empresarial en España. Directorio Central de Empresas (DIRCE) a 1 de enero de 2013. Tabla «Empresas activas según sector económico, por comunidades y ciudades autónomas. Datos a 1 de enero de 2013» pag. 6.

Andalucía	149.268	471.521	438.948	322.253
Aragón	36.827	88.067	90.192	51.240
Principado de Asturias	31.906	66.869	95.915	34.963
Canarias	30.781	129.566	103.683	98.785
Cantabria	12.053	37.190	29.628	25.137
Castilla y León	52.594	162.153	139.068	109.559
Castilla-La Mancha	37.032	124.405	108.200	87.373
Cataluña	200.925	580.804	512.221	379.879
Comunitat Valenciana	124.050	337.161	317.890	213.111
Extremadura	17.677	63.353	51.033	45.676
Galicia	74.408	192.998	214.871	118.590
Illes Balears	22.673	85.044	76.504	62.731
Comunidad Foral de Navarra	11.936	40.860	33.909	28.924
Madrid	172.341	496.003	428.021	323.662
Región de Murcia	32.476	87.146	84.280	54.670
País Vasco	42.515	153.709	112.352	111.194
La Rioja	9.718	22.316	24.502	12.598
Ceuta	530	3.610	1.238	3.080
Melilla	661	3.795	3.127	3.134
Total	**1.060.371**	**3.146.570**	**2.865.582**	**2.086.199**

En la misma línea apunta el Estudio sobre la protección de datos en las empresas españolas elaborado por INTECO en 2012[5]. Entre las conclusiones del Estudio merece la pena destacar dos:

● La mitad de las pequeñas y medianas empresas manifiesta cumplir con todas las obligaciones que contempla la normativa española sobre protección de datos.

● El 57,5% de las empresas afirma haber inscrito los registros en la AEPD. **La estimación de INTECO es que solo el 31,8% los han inscrito**.

C. La privacidad como motor de confianza en la economía digital.

En el marco de la Agenda digital para España el Plan de confianza en el ámbito digital (Ministerio de Industria, Energía y Turismo-Junio 2013)[6]

«En cuestiones de privacidad, la encuesta del Eurobarómetro muestra que, en relación con el resto de países de la Unión Europea, España ocupa la primera posición en cuanto a preocupación de los ciudadanos sobre la protección de la información de datos personales, tanto en el ámbito público como en el privado. Según un reciente Barómetro del CIS3, entre las preocupaciones destacan las dificultades para hacer un buen uso de las políticas de privacidad y la percepción que de ellas tiene la ciudadanía. Esta afirmación se pone de manifiesto en:

[5] https://www.inteco.es/guias_estudios/Estudios/Estudio_empresas_LOPD_2012
[6] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-confianza-ambito-digital.aspx

• El 31,2% reconoce que nunca lee las políticas de privacidad de las páginas de Internet que visita y un 28% lo hace raramente.
● El 34,2% indica que más que informar correctamente, lo que buscan es evitar problemas legales y un 42,3% está bastante de acuerdo con dicha afirmación.
● El 70,3% considera que las políticas de privacidad y la información que se ofrece en los sitios de Internet sobre el tratamiento de datos son poco o nada claras.
● Finalmente el 65,5% señala que los sitios web intentan que no se sepa qué van a hacer con los datos personales de los que disponen».

El documento sitúa la privacidad como elemento esencial para confianza digital ya desde su introducción:

«La construcción de un clima de confianza requiere actuar sobre diferentes ámbitos, entre ellos la ciberseguridad, el respeto y la **protección de la privacidad**, el uso responsable y seguro de servicios y contenidos, la protección de colectivos especialmente vulnerables, la resistencia y fortaleza de las infraestructuras tecnológicas de las que somos especialmente dependientes, la gobernanza, la seguridad jurídica de las relaciones personales y económicas en dicho entorno, así como la protección del consumidor en Internet».

Y finalmente lo enmarca en su primer eje de actuación:

«Eje I: Experiencia digital segura
La ADpE, la EUCS y la ESN y las estrategias para la protección de la infancia y la adolescencia, consideran esencial la sensibilización y la concienciación de los usuarios para aumentar la confianza y el buen uso de Internet.
En este ámbito, se han realizado numerosas actuaciones públicas y privadas en los últimos años con el objetivo de incrementar la confianza en Internet, especialmente en aspectos relacionados con la seguridad de la información, **la protección de la privacidad**, el comercio electrónico seguro y el uso responsable y seguro de la tecnología por la infancia y la adolescencia, entre otros».

Que la aplicación de normas sobre protección de datos personales será esencial para el desarrollo de la economía digital es una afirmación subyacente a múltiples estudios de INTECO, ya sea autónomamente considerada, ya sea vinculada a la seguridad[7]:

● Estudio sobre seguridad en dispositivos móviles y smartphones (1er cuatrimestre 2012).

● Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles, 1er cuatrimestre de 2012 (18ª oleada).

● Estudio sobre la percepción de los usuarios acerca de su privacidad en Internet.

● Estudio sobre seguridad en dispositivos móviles y smartphones, informe anual 2011.

● Estudio sobre cloud computing en el sector público en España.

● Guía para empresas: identidad digital y reputación online.

● Guía para usuarios: identidad digital y reputación online.

[7] https://www.inteco.es/guias_estudios/Estudios/

● Guía para empresas: seguridad y privacidad del cloud computing.

Por último la propia Unión Europea destaca el papel central de la privacidad para la Agenda Digital Europea como parte integrante del binomio confianza y seguridad[8].

Por tanto un estudio de máster sobre protección de datos resulta plenamente justificado por cuanto:

● Constituye un ámbito de interés académico e investigador de primera magnitud con multitud de campos abiertos a la innovación.

● En un futuro cercano el delegado de protección de datos será una figura obligatoria y necesaria en virtud de la regulación europea.

● Incluso con la normativa vigente las carencias en el cumplimiento evidencian la existencia de un mercado emergente para este tipo de profesionales.

● Los distintos estudios y los planes de la UE y el Gobierno de España para el impulso de una Agenda Digital erigen la privacidad como uno de los motores de confianza para la economía digital.

CUADRO RESUMEN DE EVIDENCIAS QUE JUSTIFICAN EL INTERÉS DEL MÁSTER	
Tipo	**Evidencia**
Bibliografía	Referencias a trabajos publicados indexadas en Dialnet
Tesis doctorales	Referencias a tesis doctorales indexadas en Dialnet
Normativa	Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura).
Asociación profesional	Dos millones de empresas en España no han registrado sus ficheros en la Agencia Española de Protección de Datos. http://www.apep.es/28-de-enero-da-de-la-proteccin-de-datos-en-europa/
AEPD	Memoria 2012 de la Agencia Española de Protección de Datos
INE	Estructura y dinamismo del tejido empresarial en España. Directorio Central de Empresas (DIRCE) a 1 de enero de 2013. Tabla «Empresas activas según sector económico, por comunidades y ciudades autónomas. Datos a 1 de enero de 2013»
INTECO	● Estudio sobre la protección de datos en las empresas españolas. ● Estudio sobre seguridad en dispositivos móviles y smartphones (1er cuatrimestre 2012). ● Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles, 1er cuatrimestre de 2012 (18ª oleada). ● Estudio sobre la percepción de los usuarios acerca de su privacidad en Internet. ● Estudio sobre seguridad en dispositivos móviles y smartphones, informe anual 2011. ● Estudio sobre cloud computing en el sector público en España. ● Guía para empresas: identidad digital y reputación online.

[8] Online privacy. http://ec.europa.eu/digital-agenda/en/online-privacy.

	● Guía para usuarios: identidad digital y reputación online. ● Guía para empresas: seguridad y privacidad del cloud computing.
Ministerio de Industria, Energía y Turismo-Junio 2013	Agenda digital para España el Plan de confianza en el ámbito digital

2.2. Normas reguladoras

No existe propiamente una norma reguladora del ejercicio profesional. No obstante deben citarse los artículos 35 y ss., de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Estas normas definen la categoría profesional y sus funciones de modo muy preciso:

Artículo 35
Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
a) el tratamiento sea llevado a cabo por una autoridad u organismo públicos; o
b) el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más; o
c) las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados.
2. En el caso contemplado en el apartado 1, letra b), un grupo de empresas podrá nombrar un delegado de protección de datos único.
3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo públicos, el delegado de protección de datos podrá ser designado para varias de sus entidades, teniendo en cuenta la estructura organizativa de la autoridad u organismo públicos.
4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen categorías de responsables o encargados podrán designar un delegado de protección
de datos.
5. El responsable o el encargado del tratamiento designarán el delegado de protección de datos atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar las tareas contempladas en el artículo 37. El nivel de conocimientos especializados requerido se determinará, en particular, en función del tratamiento de datos llevado a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado del tratamiento.
6. El responsable o el encargado del tratamiento velarán por que cualesquiera otras funciones profesionales del delegado de protección de datos sean compatibles con sus tareas y funciones en calidad de delegado de protección de datos y no planteen conflictos de intereses.
7. El responsable o el encargado del tratamiento designarán un delegado de protección de datos para un mandato mínimo de dos años. El delegado de protección de datos podrá ser nombrado para nuevos mandatos. Durante su mandato, el delegado de protección de datos solo podrá ser destituido si deja de cumplir las condiciones requeridas para el ejercicio de sus funciones.
8. El delegado de protección de datos podrá ser empleado por el responsable o el encargado del tratamiento o desempeñar sus tareas sobre la base de un contrato de servicios.
9. El responsable o el encargado del tratamiento comunicarán el nombre y los datos de contacto del delegado de protección de datos a la autoridad de control y al público.

10. Los interesados tendrán derecho a entrar en contacto con el delegado de protección de datos para tratar todas las cuestiones relativas al tratamiento de datos que les conciernan y a solicitar el ejercicio de los derechos que les confiere el presente Reglamento.
11. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a las actividades principales del responsable o del encargado del tratamiento contempladas en el apartado 1, letra c), así como los criterios aplicables a las cualidades profesionales del delegado de protección de datos contempladas en el apartado 5.

Artículo 36

Función de delegado de protección de datos

1. El responsable o el encargado del tratamiento velarán por que el delegado de protección de datos se implique adecuadamente y en su debido momento en todas las cuestiones relativas a la protección de datos personales.
2. El responsable o el encargado del tratamiento velarán por que el delegado de protección de datos desempeñe sus funciones y tareas con independencia y no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones. El delegado de protección de datos informará directamente a la dirección del responsable o del encargado del tratamiento.
3. El responsable o el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de sus tareas y facilitarán el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de las funciones y tareas contempladas en el artículo 37.

Artículo 37

Tareas del delegado de protección de datos

1. El responsable o el encargado del tratamiento encomendarán al delegado de protección de datos, como mínimo, las siguientes tareas:
a) informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y documentar esta actividad y las respuestas recibidas;
b) supervisar la implementación y aplicación de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) supervisar la implementación y aplicación del presente Reglamento, en particular por lo que hace a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos, así como a la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos en virtud del presente Reglamento;
d) velar por la conservación de la documentación contemplada en el artículo 28;
e) supervisar la documentación, notificación y comunicación de las violaciones de datos personales de conformidad con lo dispuesto en los artículos 31 y 32;
f) supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte del responsable o del encargado del tratamiento y la presentación de solicitudes de autorización o consulta previas, si fueran necesarias de conformidad con lo dispuesto en los artículos 33 y 34;
g) supervisar la respuesta a las solicitudes de la autoridad de control y, en el marco de las competencias del delegado de protección de datos, cooperar con la autoridad de control a solicitud de esta o a iniciativa propia;
h) actuar como punto de contacto para la autoridad de control sobre las cuestiones relacionadas con el tratamiento y consultar con la autoridad de control, si procede, a iniciativa propia.
2. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a las

tareas, la certificación, el estatuto, las competencias y los recursos del delegado de protección de datos contemplados en el apartado 1[9].

[9] El texto incluido en la memoria original ha sido modificado por la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura).

Artículo 35

Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
a) el tratamiento sea llevado a cabo por una autoridad u organismo públicos; o
b) el tratamiento sea llevado a cabo por una persona jurídica con respecto a más de 5000 interesados durante un periodo consecutivo de 12 meses; o
c) las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados; o
d) las actividades principales del responsable o del encargado del tratamiento consistan en el tratamiento de categorías especiales de datos con arreglo al artículo 9, apartado 1, datos de localización o datos relativos a niños o a empleados en ficheros a gran escala.
2. Un grupo de empresas podrá nombrar un delegado principal de protección de datos responsable, siempre que se garantice que resulte fácil acceder a un delegado de protección de datos desde cualquier emplazamiento.
3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo públicos, el delegado de protección de datos podrá ser designado para varias de sus entidades, teniendo en cuenta la estructura organizativa de la autoridad u organismo públicos.
4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen categorías de responsables o encargados podrán designar un delegado de protección de datos.
5. El responsable o el encargado del tratamiento designarán el delegado de protección de datos atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar las tareas contempladas en el artículo 37. El nivel de conocimientos especializados requerido se determinará, en particular, en función del tratamiento de datos llevado a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado del tratamiento.
6. El responsable o el encargado del tratamiento velarán por que cualesquiera otras funciones profesionales del delegado de protección de datos sean compatibles con sus tareas y funciones en calidad de delegado de protección de datos y no planteen conflictos
7. El responsable o el encargado del tratamiento designarán un delegado de protección de datos para un mandato mínimo de cuatro años en el caso de un empleado o de dos años en el caso de un proveedor de servicios externos. El delegado de protección de datos podrá ser nombrado para nuevos mandatos. Durante su mandato, el delegado de protección de datos solo podrá ser destituido si deja de cumplir las condiciones requeridas para el ejercicio de sus funciones.
8. El delegado de protección de datos podrá ser empleado por el responsable o el encargado del tratamiento o desempeñar sus tareas sobre la base de un contrato de servicios.
9. El responsable o el encargado del tratamiento comunicarán el nombre y los datos de contacto del delegado de protección de datos a la autoridad de control y al público.
10. Los interesados tendrán derecho a entrar en contacto con el delegado de protección de datos para tratar todas las cuestiones relativas al tratamiento de datos que les conciernan y a solicitar el ejercicio de los derechos que les confiere el presente Reglamento.

Artículo 36

Función de delegado de protección de datos

1. El responsable o el encargado del tratamiento velarán por que el delegado de protección de datos se implique adecuadamente y en su debido momento en todas las cuestiones relativas a la protección de datos personales.
2. El responsable o el encargado del tratamiento velarán por que el delegado de protección de datos desempeñe sus funciones y tareas con independencia y no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones. El delegado de protección de datos informará directamente a la dirección ejecutiva del responsable o del encargado del tratamiento. El responsable o el encargado del tratamiento nombrarán, a este fin, a un miembro de la dirección ejecutiva que será responsable de cumplir con las disposiciones del presente Reglamento.
3. El responsable o el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de sus tareas y facilitarán todos los medios, incluidos el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de las funciones y tareas contempladas en el artículo 37 y para mantener sus conocimientos profesionales.
4. El delegado de protección de datos estará vinculado por el deber de secreto con respecto a la identidad de los interesados y a las circunstancias que permitan la identificación de los interesados, a menos que los propios interesados le liberen de dicho deber.

Artículo 37

Tareas del delegado de protección de datos

El responsable o el encargado del tratamiento encomendarán al delegado de protección de datos, como mínimo, las siguientes tareas:
a) sensibilizar, informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento, en particular en relación con las medidas y los procedimientos técnicos y organizativos, y documentar esta actividad y las respuestas recibidas;
b) supervisar la implementación y aplicación de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) supervisar la implementación y aplicación del presente Reglamento, en particular por lo que hace referencia a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos, así como a la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos en virtud del presente Reglamento;
d) velar por la conservación de la documentación contemplada en el artículo 28;

2.3. Referentes nacionales e internacionales.

A. Normativa

La consideración de la normativa básica y complementaria de desarrollo resulta indispensable para la formación especializada y profesionalizante por la que apuesta el presente máster. La normativa sobre protección de datos personales lejos de agitarse en su norma esencial, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, despliega sus efectos en todo el Ordenamiento. De ahí que existan referencias explícitas a la materia en múltiple legislación sectorial y que, incluso cuando éstas no existan la correspondiente norma sirva para integrar las consecuencias de la regulación sobre el derecho fundamental a la protección de datos en el sector del que se trate.

Nacional.

● Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

→ Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

→ Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

→ Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

→ Instrucción 2/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

→ Instrucción 1/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

→ Instrucción 2/1995, de 4 de mayo, de la APD, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal.

Autonómica:

● Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos (DOGC núm. 5731, de 8.10.2010)

e) supervisar la documentación, notificación y comunicación de las violaciones de datos personales de conformidad con lo dispuesto en los artículos 31 y 32;
f) supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte del responsable o del encargado del tratamiento y la presentación de solicitudes de consulta previa , si fueran necesarias de conformidad con lo dispuesto en los artículos 32 bis, 33 y 34;
g) supervisar la respuesta a las solicitudes de la autoridad de control y, en el marco de las competencias del delegado de protección de datos, cooperar con la autoridad de control a solicitud de esta o a iniciativa propia;
h) actuar como punto de contacto para la autoridad de control sobre las cuestiones relacionadas con el tratamiento y consultar con la autoridad de control, si procede, a iniciativa propia.
i) comprobar la conformidad del tratamiento con el presente Reglamento en el marco del mecanismo de consulta previa establecido en el artículo 34;
j) informar a los representantes de los trabajadores sobre el tratamiento de datos de los empleados.

→ Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos (DOGC núm. 3835, pág.4483, de 4.03.2003)

● Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos

→ Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.

→ Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.

Sectorial: (directamente relacionada)

1) Fuerzas y Cuerpos de Seguridad.

● Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos.

● Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

● Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

2) Sociedad de la información y telecomunicaciones.

● Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

→ Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.

→ Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

→ Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento que desarrolla el Título III de la Ley General de Telecomunicaciones. Título V.

→ Orden CTE 771/2002, de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.

● Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

● Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

3) Administración.

● La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

→ Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (DA.4ª)

→ Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

4) Salud.

● Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida.

● Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesionales Sanitarias.

● Ley 16/2003, de 28 de marzo, de cohesión y calidad del Sistema Nacional de Salud.

● Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

● Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.

● Ley 25/1990, de 20 de diciembre, del Medicamento.

→ Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud

→ Real Decreto 124/2007, de 2 de febrero, por el que se regula el Registro nacional de instrucciones previas y el correspondiente fichero automatizado de datos de carácter personal.

→ Real Decreto 65/2006, de 30 de enero, por el que se establecen requisitos para la importación y exportación de muestras biológicas.

→ Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

5) Otras normas.

Véase:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/index-ides-idphp.php.

6) Jurisprudencia.

SSTC: 254/1993, 11/1998, 290/2000 y 292/2000[10].

SSTS 429/2012, 585/2012.

B. Documentos.

La documentación nacional en éste ámbito resulta abundantísima y será tenida en cuenta para la formación en el máster. Como elementos de referencia central cabe situar:

AEPD.

● Memorias.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/index-ides-idphp.php

● Guías y publicaciones.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

● Informes.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/index-ides-idphp.php

● Resoluciones.

http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php

[10] Se cita únicamente la jurisprudencia constitucional, así como la dictada por el rsu en relación con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal por su relevancia. Obviamente existen decenas de sentencias en esta materia.

Inteco.

● Informe "Adecuación a la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico"

● Estudio sobre la percepción de los usuarios acerca de su privacidad en Internet

● Estudio sobre la protección de datos en las empresas españolas

● Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas

● Estudio sobre cloud computing en el sector público en España

● Riesgos y amenazas en cloud computing

● Estudio sobre la privacidad y la seguridad de los datos personales en el sector sanitario español

● Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles

● Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online

http://www.inteco.es/Estudios/

Otros.

● Agenda Digital para España

http://www.agendadigital.gob.es/agenda-digital/Paginas/agenda-digital.aspx.

→ Plan de confianza en el ámbito digital (Junio 2013).

http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-confianza-ambito-digital.aspx

C. Planes de estudio.

Se aportan un conjunto de planes de estudio de formación de posgrado relacionados con la materia objeto del máster. Únicamente dos de ellos se centran directamente en la materia lo que evidencia la existencia de una necesidad objetiva de este tipo de estudios. Por otra parte, y como más adelante se señalará el mercado necesita de un máster cuyo enfoque se plantee nuevas perspectivas en el abordaje de la materia y en la preparación de los titulados.

I. Máster en e-Learning y Redes Sociales
Entidad Organizadora: Universidad Internacional de La Rioja
Grado: Máster Oficial
Modalidad Enseñanza: Online
Duración: 60 créditos
Enlace: http://www.unir.net/master-online-e-learning.aspx#programa

II. Máster Universitario en Gestión de las Tecnologías de la Información
Entidad Organizadora: Universidad Ramón Llull
Grado: Máster Oficial
Modalidad Enseñanza: Presencial y Online
Duración: 60 créditos
Enlace: http://www.beslasalle.net/portal/masters/masters-technology-mgti-barcelonapresentation

III. Máster Universitario en Investigación e Innovación en Tecnologías de la Información y las Comunicaciones
Entidad Organizadora: Universidad Autónoma de Madrid
Grado: Máster Oficial
Modalidad Enseñanza: Presencial
Duración: 60 créditos

Enlace: http://www.uam.es/ss/Satellite/es/1242663065228/1242662165493/masteroficial/masterOficia/Master_Universitario_en_Investigacion_e_Innovacion_en_Tecnologias_de_la_Informacion_y_las_Comunicaci.htm

IV. Máster Universitario en Seguridad de Tecnologías de la Información y Comunicaciones
Entidad Organizadora: Universidad Europea de Madrid
Grado: Máster Oficial
Modalidad Enseñanza: Presencial
Duración: 60 créditos
Enlace: http://www.uem.es/postgrado/master-oficial-en-seguridad-de-las-tecnologiasde-la-informacion-y-las-comunicaciones/programa

V. Máster Universitario en Tecnologias de la Información
Entidad Organizadora: Universitat de les Illes Balears
Grado: Máster Oficial
Modalidad Enseñanza: Presencial
Duración: 60 créditos
Enlace: http://postgrau.uib.cat/es/master/MTIN/

Títulos Propios de Posgrado - Masters, Especialistas, Expertos:

I. Especialista Universitario en Consultoría ITIO (Integración de las TIC en las Organizaciones)
Entidad Organizadora: Universidad Politécnica de Valéncia
Grado: Máster y Especialista
Modalidad Enseñanza: Presencial
Duración: 22 créditos (Especialista), 60 créditos (Máster)
Enlace: http://www.itio.upv.es/~consitiocfp/programa.html

II. Experto en Protección de Datos
Entidad Organizadora: Universidad Camilo José Cela
Grado: Máster y Especialista
Modalidad Enseñanza: Presencial + Prácticas (AEPD)
Duración: 200 horas.
Enlace: http://www.ucjc.edu/index.php?section=estudios/titulaciones/mastersposgrados/experto-proteccion-datos/programa

III. Máster en ASESORÍA Y CONSULTORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIÓNES TIC
Entidad Organizadora: Universidad de Burgos
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 65,3 créditos
Enlace: http://limbo.ubu.es/campusvirtual/postgrado/cabecera_ep.asp?Curso=2008&IdPrograma

ma=64

IV. Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC
Entidad Organizadora: Universidad Autónoma de Madrid
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 60 créditos
Enlace: http://arantxa.ii.uam.es/~masgdtic/

V. Máster en Derecho de las Telecomunicaciones y Tecnologías de la Información
Entidad Organizadora: Universidad Carlos III de Madrid
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 60 créditos
Enlace: http://www.uc3m.es/portal/page/portal/postgrado_mast_doct/masters/Master_en_Derecho_de_las_Telecomunicaciones_y_TI

VI. Máster en Normativa de Protección de Datos en el Sector Sanitario
Entidad Organizadora: Universidad de Cádiz
Grado: Máster
Modalidad Enseñanza: Online
Duración: 55 créditos
Enlace: http://www2.uca.es/serv/formagest/salud/mlpd/index.htm

VII. Máster en Dirección Estratégica en Tecnologías de la Información
Entidad Organizadora: Universidad de Leon
Grado: Máster
Modalidad Enseñanza: Online
Duración: 800 horas
Enlace: http://www.funiber.org/areas-de-conocimiento/tecnologias-de-lainformacion/master-en-direccion-estrategica-en-tecnologias-de-lainformacion/programa-academico/programa-de-estudios/

VIII. Máster Dirección y gestión de sistemas y tecnologías de la información
Entidad Organizadora: UOC
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 32 créditos, 480 horas
Enlace: http://www.uoc.edu/masters/esp/web/economia_empresa/direccion_y_gestion_de_las_tic/master/direccion_y_gestion_de_sistemas_y_tecnologias_de_la_informacion/programa_academico.html

IX. Máster en Gestión de Nuevas Tecnologías para la Empresa
Entidad Organizadora: Universidad CEU San Pablo
Grado: Máster
Modalidad Enseñanza: Online
Duración: 6 cursos (Especialista), 12 cursos (Master)
Enlace: http://www.campusvirtualceu.com/cursos/master_nuevas_tecnologias.htm

X. Magister Lvcentinvs: Master en Propiedad Intelectual e Industrial y Derecho de la Sociedad de la Información
Entidad Organizadora: Universidad de Alicante
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 60 créditos
Enlace: http://www.ml.ua.es/

XI. Máster en Propiedad Intelectual y Sociedad de la Información
Entidad Organizadora: Universidad Ramón Llull
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 9 meses
Enlace: http://www.esade.edu/posderecho/esp/part_time/ip_it/contenido

XII. Máster iberoamericano en servicios de información, juventud y desarrollo comunitario en nuevas tecnologías
Entidad Organizadora: Universidad de Salamanca
Grado: Máster
Modalidad Enseñanza: Presencial
Duración: 370 horas
Enlace: http://www.usal.es/webusal/node/2355

XIII. Máster en asesoría y consultoría en tecnologías de la información y las comunicaciones (MAC-TIC)
Entidad Organizadora: Universidad de Salamanca
Grado: Máster
Modalidad Enseñanza: Semi-Presencial
Duración: 704 horas
Enlace: http://www.usal.es/webusal/node/9925

XIV. Master en Sociedade da Información e do Coñecemento
Entidad Organizadora: Universidad de Santiago de Compostela
Grado: Máster
Modalidad Enseñanza: Online
Duración: 60 créditos
Enlace: http://www.usc.es/cptf/Postgrado/CursosPostgrado/Datos2012/Cp34512012-2013g.htm

XV. Master oficial Derecho y TICs, Universidad de Valencia (extinto)
Entidad Organizadora: Universidad de Valencia
Grado: Máster (Especialidad dentro del Master "Sistemas y servicios de la sociedad de la información)
Modalidad Enseñanza: Presencial
Duración: 60 créditos
Enlace: **http://www.uv.es/mastic/especialidadDTIC.html**

XVI. Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información
Entidad Organizadora: Facultad de Derecho. Universidad S. pablo CEU
Grado: Máster oficial.

Modalidad Enseñanza: Presencial y semipresencial.
Duración: 70 créditos
Enlace:
http://www.postgrado.uspceu.es/pages/proteccion_datos/presentacion.html?ID_M=84

XV. Curso de Especialista Universitario en Protección de Datos y Privacidad
Entidad Organizadora: Facultad de Derecho de la Universidad de Murcia
Grado: Curso de posgrado
Modalidad Enseñanza: online
Duración: 30 créditos
Enlace:https://casiopea.um.es/cursospe/servlet/um.casiopea.catalogo.ControlCatalogo?accion=detalle&cu_cod=6425&aplicacion=CASIOPEA&origen=/cursospe/servlet/um.casiopea.catalogo.ControlCatalogo?accion=inicio&cbmarcar=null&marca=

2.4. Referentes internacionales

A. Normativa

Naciones Unidas.

● Declaración Universal de Derechos Humanos (1948).

● Pacto Internacional de ONU sobre derechos económicos, sociales, culturales, civiles y políticos (1966).

● Declaración Universal sobre el Genoma Humano y los derechos humanos (1999).

● Declaración de los Derechos del Niño (1959) y Declaración de los Derechos del Niño

● Convención sobre los Derechos del Niño (1989).

● Directrices para la regulación de los archivos de datos personales informatizados. Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

Consejo de Europa.

● Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Instrumento de Ratificación de 26 de septiembre de 1979.

● Convenio del Consejo de Europa, de 28 de enero 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984.

→ Protocolo Adicional del Convenio Nº 108, de 8 de noviembre de 2001.

→ Modificación del Convenio para la protección de las personas en relación con el tratamiento automatizado de sus datos personales (ETS nº 108) permitiendo el acceso de las Comunidades Europeas (aprobado por el Comité de Ministros, en Estrasburgo, el 15 de junio de 1999).

● Convenio para la protección de los Derechos Humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina. Convenio sobre los Derechos Humanos y la Biomedicina de 4 de abril de 1997.

Unión Europea.

● Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea.

● Carta de los Derechos Fundamentales de la Unión Europea.

● Carta Europea de los Derechos del Niño.

● Convenio de Schengen, de 19 de junio de 1990, de aplicación del Acuerdo de Schengen de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes. (B.O.E. de 5 de abril de 1994) y Protocolo núm. 2 por el que se integra el Acervo de Schengen en el Marco de la Unión Europea (1997).

● Convenio Europol. Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía, hecho en Bruselas el 26 de junio de 1995. (B.O.E. de 28 de septiembre de 1998).

● REGLAMENTO (CE) No 45/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

● REGLAMENTO (UE) Nº 611/2013 DE LA COMISION, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

● Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (D.O.C.E. serie L. núm. 281, de 23 de noviembre de 1995).

● Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos (DOCE, serie L, núm. 77 de 27 de abril).

● Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (DOCE, serie L, núm. 24 de 30 de enero).

● Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DOCE, serie L, núm. 178/1 de 17 de julio).

● Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas o Directiva sobre la privacidad y las comunicaciones electrónicas (DOCE, Serie L, núm. 201 de 31 de julio).

● Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

● Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación

de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

● Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores

● Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DOCE, serie L, núm. 215, de 25 de agosto).

● Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE (DOCE, Serie L núm. 181, de 4 de julio.

● Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a 'Cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. (Queda derogada a partir de 15 de mayo de 2010).

● Decisión de la Comisión de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

● Decisión de la Comisión (2010/87/UE), de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

Iberoamérica.

Pacto de San José de Costa Rica - Convención Americana sobre Derechos Humanos (1969).

ARGENTINA

Ley 25.326 de Protección de Datos (Habeas Data) del 2 de noviembre de 2000.

Decreto 1558/2001. Reglamento de la Ley de Protección de Datos (Boletín Oficial del 3 de diciembre de 2001).

CHILE.

Ley 19.628, del 28 de agosto de 1999. Protección a la Vida Privada. Modificada por la Ley 19.812, de 13 de Junio de 2002. En la actualidad, se tramita un proyecto de modificación de dicha Ley 19.628.

Decreto 779/ 2000. Reglamentación de la Ley 19.629, que regula el Registro de Bancos de Datos Personales a Cargo de los Organismos Públicos.

COLOMBIA.

Ley Estatutaria Nº 1581, de 17 de octubre de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”.

REPÚBLICA DE COSTA RICA.

● Ley nº 8968, de 7 de julio de 2011. Protección de la Persona frente al tratamiento de sus datos personales.

● Decreto Ejecutivo No.37554-JP, del 30 de octubre de 2012. Reglamento de la Ley nº 8968.

ESTADOS UNIDOS MEXICANOS

● DECRETO por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. 05/07/2010.

REPÚBLICA DE NICARAGUA

● Ley nº 787, Ley de Protección de Datos Personales.

REPÚBLICA DEL PARAGUAY

● Ley Nº 1682 que reglamenta la información de carácter privado.

● LEY Nº 1969 que modifica, amplía y deroga varios artículos de la Ley Nº1682 que reglamenta la información de carácter privado.

REPÚBLICA DEL PERÚ

● Ley nº 29733, Ley de Protección de Datos Personales, publicada el 3 de julio de 2011.

REPÚBLICA ORIENTAL DEL URUGUAY

● Ley 18.331 (11 de noviembre de 2008). Protección de Datos Personales y Acción Habeas Data (deroga Ley 17.838).

ESTADOS UNIDOS

Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (1970).

● Privacy Act, 5 U.S.C. § 552 (1974).

● The Freedom of Information Act (FOIA), 5 U.S.C. § 552 (1974).

● Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g et seq. (1974).

● Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. (1978).

● Privacy Protection Act, 42 U.S.C. § 2000aa et seq. (1980).

● Cable Communications Policy Act 47 U.S.C. § 551 et seq. (1980).

● Electronic Communications Privacy Act (ECPA), 18 USC §§ 2701-11 (1986).

● Video Privacy Protection Act, 18 U.S.C. § 2710 (1988).

● Telephone Consumer Protection Act, 47 U.S.C. § 227 (1991).

● Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994).

● Telecommunications Act, 47 U.S.C. §222 (1996).

● Electronic Freedom of Information Act Amendments of 1996, Public Law No. 104-231, 110 Stat. 3048 (1996).

● Children's Online Privacy Protection Act, 16 U.S.C. §6501 (1998).

● Financial Modernization Services Act, Public Law 106-102**,** Gramm-Leach-Billey Act of 1999.

● Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USAPA), H.R. 3162, (2001) también conocida como USA Patriot Act.

● Pen/trap Statute 18 USC §§ 3121-27 (2002).

● Wiretap Statute, 18 USC §§ 2510-22, (2002).

B. Documentos

OCDE

Directrices de la Organización de Cooperación y Desarrollo Económicos, de 23 de septiembre de 1980 sobre la protección de la vida privada y los flujos transfronterizos de datos.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (22/02/2002

UNIÓN EUROPEA

● Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos, personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Bruselas, 25.1.2012, COM (2012) 11 final, 2012/0011 (COD). Existe una versión no oficial del texto tras su aprobación por la Comisión LIBE del Parlamento Europeo.

→ Reform of the data protection legal framework (http://ec.europa.eu/justice/data-protection/review/index_en.htm)

● Grupo de trabajo del artículo 29.

2013

- Working Document 02/2013 providing guidance on obtaining consent for cookies (WP 208 (02.10.2013)
- Opinion 06/2013 on open data and public sector information ('PSI') reuseWP 207 (05.06.2013)
- Explanatory Document on the Processor Binding Corporate Rules, WP 204 (19.04.2013)
- Opinion 03/2013 on purpose limitation WP 203 (02.04.2013)
- Opinion 02/2013 on apps on smart devices WP 202 (27.02.2013)
- Working Document 01/2013 - Input on the proposed implementing acts WP 200 (22.01.2013)

2012

- Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications, WP 197 (12.07.2012)
- Opinion 05/2012 on Cloud Computing, WP 196 (01.07.2012)

- Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, WP 195a (17.09.2012)
- Opinion 04/2012 on Cookie Consent Exemption- WP 194 (07.06.2012)
- Opinion 03/2012 on developments in biometric technologies- WP 193 (27.04.2012)
- Opinion 02/2012 on facial recognition in online and mobile services- WP 192 (22.03.2012)
- Opinion 01/2012 on the data protection reform proposals- WP 191 (23.03.2012)

2011

- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising- WP 188 (08.12.2011)
- Opinion 15/2011 Consent- WP 187 (13.07.2011)
- Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing- WP 186 (13.06.2011)
- Opinion 13/2011 on Geolocation services on smart mobile devices- WP 185 (16.05.2011)
- Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments - WP 184 (05.04.2011)
- Opinion 12/2011 on smart metering - WP 183 (04.04.2011)
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications
    - Annex: Privacy and Data Protection Impact Assessment Framework for RFID Applications - WP 180 (11.02.2011)

2010

- Opinion 8/2010 on applicable law- WP 179 (16.12.2010)
- Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries- WP 178 (12.11.2010)
- FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC- WP 176 (12.07.2010)
- Opinion 5/2010on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications - WP 175 (13.07.2010)
- Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing - WP 174, (13.07.2010)
- Opinion 3/2010 on the principle of accountability- WP 173 (13.07.2010)
- Opinion 2/2010 on online behavioural advertising- WP 171 (22.06.2010)

- Opinion 1/2010 on the concepts of "controller" and "processor- WP 169 (16.02.2010)

2009

- The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data- WP 168 01.12.2009
- Opinion 8/2009 on the protection of passenger data collected and processed by duty-free shops at airports and ports- WP 167 (01.12.2009)
- Contribution of the Article 29 Working Party to the public consultation of DG MARKT on the report of the Expert Group on Credit Histories-WP 164 (01.12.2009)
- Opinion 5/2009 on online social networking- WP 163 (12.06.2009)
- Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) - WP 161 (05.03.2009)
- Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) - WP 160 (11.02.2009)
- Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) - WP 159 (10.02.2009)
- Working Document 1/2009 on pre-trial discovery for cross border civil litigation- WP 158 (11.02.2009)

2008

- Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules- WP 155 rev 04 (24.06.2008)
- Working Document setting up a framework for the structure of Binding Corporate Rules- WP 154 (24.06.2008)
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules- WP 153 (24.06.2008)
- Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008- WP 151 (24.06.2008)
- Opinion 1/2008 on data protection issues related to search engines- WP 148 (04.04.2008)
- Working Document 1/2008 on the protection of Children's Personal Data- WP 147 (18.02.2008)

2007

- Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007- WP 145 (05.12.2007)

- Opinion Nº 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007- WP 138 (17.08.2007)
- Report 1/2007 on the first joint enforcement action: evaluation and future steps -WP 137 (20.06.2007)
- Opinion Nº 4/2007 on the concept of personal data - WP 136 (20.06.2007)
- Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data- WP 133 (10.01.2007)
- Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities- WP 132
- Working Document on the processing of personal data relating to health in electronic health records (EHR) - WP 131 (15.02.2007)
- Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities- WP 129 (09.01.2007)

2006

- Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) - WP 128 (22.11.2006)
- Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data- WP 127 (27.09.2006)
- Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement - WP 124 (27.09.2006)
- Opinion 4/2006 on the Notice of proposed rule making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71) - WP 121
- Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC- WP 119 (25.03.2006)
- Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services- WP 118 21.02.2006
- Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime- WP 117 (01.02.2006)

2005

- Opinion 5/2005 on the use of location data with a view to providing value-added services- WP 115 (25.11.2005)
- Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology- WP 111 (28.06.2005)
- Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules- WP 108 (14.04.2005)
- Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"- WP 107 (14.04.2005)
- Working document on data protection issues related to RFID technology- WP 105 (19.01.2005)
- Working document on data protection issues related to intellectual property rights - WP 104 (18.01.2005)

2004

- Model Checklist, Application for approval of Binding Corporate Rules- WP 102 (25.11.2004)
- Declaration of the Article 29 Working Party on Enforcement- WP 101 (25.11.2004)
- Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)] - WP 99 (09.11.2004)
- Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America- WP 97 (30.09.2004)
- Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS) - WP 96 (11.08.2004)
- Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection- WP 95 (22.06.2004)
- Joint Statement in response to the terrorist attacks in Madrid- WP 93 (17.03.2004)
- Working Document on Genetic Data- WP 91 (17.03.2004)

- Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC- WP 90 (27.02.2004)
- Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance- WP 89 (11.02.2004)
- Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP) - WP 87 (29.01.2004)

2003

- Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business associations- WP 84 (17.12.2003)
- Opinion 7/2003 on the re-use of public sector information and the protection of personal data- WP 83 (12.12.2003)
- Working document on biometrics- WP 80 (01.08.2003)
- Level of Protection ensured in the United States for the Transfer of Passengers' Data - WP 78 (13.06.2003)
- Opinion 4/2003 of the Art. 29 Working Party- WP 78 (13.06.2003)
- European code of conduct of FEDMA for the use of personal data in direct marketing - WP 77. Opinion 3/2003 of the Art. 29 Working Party.
- Opinion 2/2003 on the application of the data protection principles to the Whois directories- WP 76 (13.06.2003)
- Working Document on E-Government- WP 73 (08.05.2003)
- Opinion 1/2003 on the storage of traffic data for billing purposes- WP 69 (29.01.2003)
- The Article 29 Working Party gives guidance regarding on-line authentication systems - WP 68. Working Document on on-line authentication services (29.01.2003)

2002

- Working Document on the Processing of Personal Data by means of Video Surveillance- WP 67 (25.11.200)
- Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States- WP 66 (24.10.2002).
- Working document on Black Lists- WP 65 (3.10.2002)
- Working document on functioning of the Safe Harbor Agreement- WP 62 (2.7.2002)
- Opinion 3/2002 on the data protection provisions of a Commission proposal for a Directive on the harmonisation of the laws, regulations and administrative provisions of the Member States concerning credit for consumers- WP 61 (2.7.2002)
- Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPV6- WP 58 (30.5.2002)
- Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe WP 57 (30.5.2002)

- Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites- WP 56 (30.5.2002)
- Working document on the surveillance of electronic communications in the workplace- WP 55 (29.5.2002)

2001

- Opinion 10/2001 on the need for a balanced approach in the fight against terrorism- WP 53 (14.12.2001)
- Opinion 9/2001 on the Commission Communication on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"- WP 51 (November 2001)
- Working Document on IATA Recommended Practice 1774 Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo- WP 49 (14.09.2001)
- Opinion 8/2001 on the processing of personal data in the employment context- WP 48 (13.09.2001)
- Opinion 7/2001 on the Draft Commission Decision (version 31 August 2001) on Standard Contractual Clauses for the transfer of Personal Data to data processors established in third countries under Article 26(4) of Directive 95/46- WP 47 (13.09.2001)
- Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union- WP 43 (17.05. 2001)
- Recommendation 1/2001 on Employee Evaluation Data- WP 42 (22.03.2001)
- Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46- WP 38 (26.01.2001)

2000

- Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection- WP 37 (21.11.2000)
- Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000- WP 36 (2.11.2000)
- Opinion 6/2000 on the Human Genome and Privacy- WP 34 (13.072000)
- Opinion 5/2000 on The Use of Public Directories for Reverse or Multi-criteria Searching Services (Reverse Directories)- WP 33 (13.07.2000)
- Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"- WP 32 (16.05.2000)
- Opinion 3/2000 on the EU/US dialogue concerning the "Safe harbor" arrangement- WP 31 (16.03.2000)

- Recommendation 1/2000 on the Implementation of Directive 95/46/EC- WP 30 (3.02.2000)
- Opinion 1/2000 on certain data protection aspects of electronic commerce- WP 28 (3.02.2000)

1999

- Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce- WP 27 (December 1999)
- Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights- WP 26 (7.09.1999)
- Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes- WP 25 (7.09.1999)
- Working document on the current state of play of the ongoing discussions between the european Commission and the United States Government concerning the International Safe Harbor Principles"- WP 23 (7.09.1999)
- Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles"- WP 21 (7.09.1999)
- Opinion 3/99 on public sector information and the protection of personal data - WP 20 (3.051999)
- Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999- WP 19 (3.051999)
- Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications - WP 18 (3.051999)
- Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware - WP 17 (23.02.1999)
- Working Document: Processing of Personal Data on the Internet - WP 16 (23.02.1999)
- Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government - WP 15 (26.01.1999)

1998

- Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive - WP 12 (July 1998)
- Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) - WP 11 (16.06.1998)
- Recommendation 1/98 on Airline Computerised Reservation Systems (CRS) - WP 10 (28.04.1998)

- Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries- WP 9 (22.04.1998)
- Working Document: Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country? - WP 7 (14.01.1998)

1997

- Recommendation 3/97: Anonymity on the Internet - WP 6 (3.12.1997)
- Recommendation 2/97: Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet") - WP 5 (3.12.1997)
- Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy - WP 4 (26.06.1997)
- (29.05.1997)
- Recommendation 1/97: Data protection law and the media - WP 1 (25.02.1997)

● Jurisprudencia del Tribunal de Justicia de la UE.

CONSEJO DE EUROPA.

- Modernisation of Convention No. 108. Documents.
- Factsheet - Data protection. July 2012. .

● Recomendaciones del Comité de Ministros.

- Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services
- Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines
- Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010)
- Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes (18 September 2002)
- Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999)
- Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997)
- Recommendation No.R(97) 5 on the protection of medical data (13 February 1997)

- Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995)
- Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991)
- Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990)
- Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989)
- Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987)
- Recommendation No.R(86) 1 on the protection of personal data for social security purposes (23 January 1986)
- Recommendation No.R(85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985)
- Recommendation No.R(83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983) [replaced by
- Recommendation No. R(97) 18 with regard to statistics]
- Recommendation No.R(81) 1 on regulations for automated medical data banks (23 January 1981) [replaced by Recommendation No. R (97) 5]
- Resolution (74) 29 on the protection of individuals vis-à-vis electronic data banks in the public sector
- Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector
- Declaration of the Committee of Minister on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013)

OTROS DOCUMENTOS.

- **ENISA**
  - Report on Annual Privacy Forum 2012. Dec 12, 2012
  - Privacy considerations of online behavioural tracking, Nov 14, 2012. Nov 20, 2012
  - The right to be forgotten - between expectations and practice. Nov 20, 2012
  - Study on monetising privacy. An economic model for pricing personal information. Feb 28, 2012
  - Study on data collection and storage in the EU. Feb 23, 2012
  - Technical Guideline on Minimum Security Measures. Dec 13, 2011
  - Technical Guideline on Incident Reporting. Dec 13, 2011
  - Smartphone Secure Development Guidelines. Nov 25, 2011

- To log or not to log? - Risks and benefits of emerging life-logging applications. Nov 11, 2011
- Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments. Jan 31, 2011
- Data breach notifications in the EU Jan 13, 2011
- Appstore security: 5 lines of defence against malware. Sep 12, 2011
- Privacy, Accountability and Trust – Challenges and Opportunities. Feb 18, 2011
- Cloud Computing Risk Assessment, 2009.
- Web 2.0 Security and Privacy. Dec 10, 2008
- Technology-induced challenges in Privacy & Data Protection in Europe [Spanish Version]. Oct 01, 2008

● EE.UU

- Consumer Privacy Bill of Rights. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. February 2012
- Federal Trade Commision. COPPA Rulemaking and Rule Reviews

● APEC. APEC. Privacy Framework.

● Privacy by Design.

- Ann Cavoukian, Ph.D.Information and Privacy Commissioner,Ontario, Canada. Operationalizing *Privacy by Design*: A Guide to Implementing Strong Privacy Practices. Ontario, 2012.

● Privacy Impact Assessment.

- ICO's PIA handbook,2009.
- Privacy impact assessment and risk management. Report for the Information Commissioner's Office prepared by Trilateral Research & Consulting. 4 May 2013.
- Privacy Impact Assessments: International Study of their Application and Effects. October. Prepared for Information Commissioner's Office United Kingdom, 2007.
- Trilateral Research & Consulting . PIAF. A Privacy Impact Assessment Framework for data protection and privacy rights. Prepared for the European Commission Directorate General Justice. JLS/2009-2 010/DAP/AG.

Bibliografía general.

- ABERASTURI GORRIÑO, UNAI. *La Protección de Datos en la Sanidad*. Aranzadi, 2013.
- ALLEN, ANITA L. «Dredging up the Past: Lifelogging, Memory, and Surveillance», *The University of Chicago Law Review*, 75.1 (2008), accessed February 19, 2012, http://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/75.1/75_1_Allen.pdf.

- ALLEN, ANITA L. «Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm», en en *Connecticut Law Review*, vol. 32, Spring 2000.
- ÁLVAREZ-CIENFUEGOS SUÁREZ, JOSÉ MARÍA. «La libertad informática, un nuevo derecho fundamental en nuestra Constitución», en *La Ley*, núm. 5230, 2001.
- ÁLVAREZ-CIENFUEGOS SUÁREZ, JOSÉ MARÍA. *La defensa de la intimidad de los ciudadanos y la tecnología informática.* Aranzadi, Pamplona, 1999.
- ANA MARZO PORTERA. *Auditoria de seguridad en la protección de datos de carácter personal*. Experiencia Ed. 2009.
- ANA MARZO PORTERA. *Guía práctica para la protección de datos de carácter personal*. Experiencia Ed. 2009.
- APARICIO SALOM, JAVIER. *Estudio sobre la proteccion de datos* (4ª ed.). Aranzadi, 2013.
- ARENAS RAMIRO, MÓNICA. *El derecho fundamental a la protección de datos personales.* Tirant lo Blanch, 2006.
- ARNOLD, MARC y KISSELOFF, ANDREW. «Note, An Introduction to the Federal Privacy Act of 1974 and its Effect on the Freedom of Information Act» en *New England Law Review*, vol. 11, 1976.
- ARRIBAS LUQUE, JOSÉ MARÍA. «Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EEUU: el sistema de Principios de Puerto Seguro», en *La Ley. Revista jurídica española de doctrina, jurisprudencia y bibliografía*, núm. 3, 2002.
- ARROYO YANES, LUÍS MIGUEL. «El Derecho de Autodeterminación Informativa frente a las Administraciones Públicas (Comentario a la STC 254/93, de 20 de julio», en *Administración de Andalucía. Revisa Andaluza de Administración Pública,* núm. 16, octubre-diciembre 1993.
- ASPAS ASPAS JOSÉ MANUEL. «La libertad informática, un nuevo derecho fundamental desvelado por el Tribunal Constitucional (STC 254/1993, de 20 de julio)», en *Revista Aragonesa de Administración Pública*, nº 4, 1994.
- BALDASSARRE, ANTONIO. *Privacy e costituzione. L'esperienza statunitense*. Roma, Bulzoni, 1974.
- BARRIUSO RUIZ, CARLOS. «Las redes sociales y la protección de datos hoy», *Anuario de la Facultad de Derecho de Alcalá de Henares 2*, (2009): 303-340.
- BATLLE SALES, GEORGINA. *El derecho a la intimidad privada y su regulación*. Marfil, Alcoy, 1972.
- BING, JON. «Data Protection, Jurisdiction and the Choice of Law*», en 21st International Conference on Privacy and Personal Data Protection*, Privacy Commissioner for Personal Data, Hon Kong, 1999.
- BLOUSTEIN, EDWARD J. «Privacy as an aspect of human dignity: an answer to Dean Prosser» en *New York University Law Review*, vol. 39, december 1964.
- BUISAN SERRANO NIEVES. *La ley de protección de datos: análisis y comentario de su jurisprudencia*. Lex Nova, 2008.
- BUTTARELLI, GIOVANNI. *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*. Milano, Giufré, 1997.

- CAMPUZANO TOMÉ, HERMINIA. *Vida privada y datos personales.* Tecnos, Derecho y realidad, Madrid, 2000.
- CARDONA RUBERT, MARÍA BELÉN. *Informática y contrato de trabajo: (aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal).* Tirant lo Blanch, Valencia, 1999.
- CASAS VALLÉS, RAMÓN. «Honor, intimidad e imagen: su tutela en la LO 1/82» en *Revista Jurídica de Catalunya,* núm. 2, 1989.
- CASTELLS, MANUEL. *La era de la información: economía, sociedad y cultura. Vol. I. La sociedad red*. Alianza Editorial, Madrid, 1999.
- CASTELLS, MANUEL. *La Galaxia Internet.* Areté, Barcelona, 2001.
- CASTILLA DEL PINO, CARLOS. «Público, privado e íntimo» en ARANGUREN, JOSÉ LUÍS. *De la intimidad.* Crítica, Barcelona, 1989.
- CATE, FRED H. ET AL. «The Right to Privacy and the Public's Right to Know: The Central Purpose of the Freedom of Information Act» en *Administrative Law Review*, vol. 46, 1994.
- CATE, FRED. H. «Principles on Internet Privacy» en *Connecticut Law Review*, vol. 32, Spring 2000.
- CATE, FRED. H. *Privacy in Perspective*. The AEI Press, Wahington, D. C., 2001.
- CATE, FRED. H. *Privacy in the Information Age*, Brookings Institution Press, Washington, D.C., 1997.
- CHANG, NANCY. *The USA Patriot Act: What's So Patriotic About Trampling on the Bill of Rights?.* Center for Constitutional Rights, New York, 2001.
- CONCEPCIÓN RODRÍGUEZ, JOSÉ LUÍS. *Honor, intimidad e imagen. Un análisis jurisprudencial de la LO. 1/1982*. Bosch, Barcelona, 1996.
- COUNCIL OF THE EUROPEAN UNION. *Council conclusions on the protection of children in the digital world*, doc. 2011/C 372/04 (2011), accessed February 19, 2012 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:372:0015:0018:ES:PDF
- DAVARA RODRIGUEZ, MIGUEL ANGEL. *Guía práctica de protección de datos para ayuntamientos*. La Ley, 2006.
- DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *La protección de datos en Europa*. Ed. Grupo Asnef-Equifax. Madrid, 1998.
- DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *La protección de datos personales en el sector de las telecomunicaciones*. Universidad Pontificia de Comillas – Fundación Airtel, Madrid, 2000.
- DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *Manual de Derecho Informático*. Aranzadi, Pamplona, 2002.
- DENHAM ELIZABETH. R*eport of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act. July 16, 2009*. Office of the Privacy Commissioner of Canada. PIPEDA Case Summary #2009-008. En http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.

- DESDENTADO BONETE, AURELIO, MUÑOZ, BELÉN RUIZ, ANA. *Control informático, videovigilancia y protección de datos en el trabajo*. Lex Nova, 2012,
- DUMORTIER FRANCK. «Facebook y los riesgos de la "descontextualización" de la información», *IDP: Revista de Internet, Derecho y Política*, 9 (2009) accessed February 19, 2012, http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp.
- DYSON, ESTHER. *Release 2.0*. B.S.A, Barcelona, 2000.
- ÉCIJA ABOGADOS. *Protección de datos personales (Factbook) de Ecija Abogados*. Thomson, 2010.
- EFF. *Analysis Of The Provisions Of The USA Patriot Act. That Relate To Online Activities.* Electronic Frontier Foundation, 2001.
- EPIC. Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001. Electronic Privacy Information Center, 2001.
- ESTADELLA YUSTE, OLGA. *La protección de la intimidad frente a la transmisión internacional de datos personales.* Tecnos, Madrid, 1995.
- ETXEBERRÍA GURIDI, JOSÉ FRANCISCO. *La protección de los datos de carácter personal en el ámbito de la investigación penal*. Agencia de Protección de Datos, Madrid, 1998.
- EUROPEAN COMMISION. *Implementation of the Safer Social Networking Principles for the EU*, (2011), accessed February 19, 2012, http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip_2011/index_en.htm.
- FAIRÉN GUILLÉN VÍCTOR. «El Habeas data y su protección actual sugerida por la Ley española de Informática de 29 de oct ubre de 1992. (Primera parte)», en *Revista de Derecho Procesal*, núm. 3, 1996.
- FAIRÉN GUILLÉN VÍCTOR. «El Habeas data y su protección actual sugerida por la Ley española de Informática de 29 de octubre de 1992. (Segunda parte)», en *Revista de Derecho Procesal*, núm. 1, 1997.
- FARIÑAS MANTONI, LUÍS. *El derecho a la intimidad,* Trivium, Madrid, 1983.
- FAYOS GARDÓ, ANTONIO. *El derecho a la intimidad. Un estudio de derecho comparado: los sistemas legales de estados Unidos, España, y en especial el del Reino Unido.* Tesis doctoral, Universidad de Castellón, 1997.
- FERNÁNDEZ ESTÉBAN, MARÍA LUISA. «Limitaciones constitucionales e inconstitucionales a la libertad de expresión en Internet», en *Revista Española de Derecho Constitucional,*núm. 53, mayo-agosto, 1998.
- FERNÁNDEZ ESTÉBAN, MARÍA LUISA. *Nuevas tecnologías, Internet y Derechos Fundamentales*. MacGraw Hill, Madrid, 1998.
- FREIXAS GUTIÉRREZ, GABRIEL. *La protección de los datos de carácter personal en el derecho español: aspectos teóricos y prácticos*. Bosch, Barcelona, 2001.
- FRIED CHARLES. «Privacy» en *The Yale Law Journal,* vol. 77, 1967-1968.
- FROOMKIN, A. MICHAEL. «Technological Change and the Destruction of Informational Privacy» en *XXII Conferenza Internazionale sulla privacy e la protezione dei dati personali*, Venecia, 28-30 de septiembre de 2000.

- FROSINI, V. *Il diritto nella società tecnologica*. Giuffré, Milano, 1981.
- FUMERO ANTONIO, ROCA GENÍS AND ENCINAR JESÚS. *Web 2.0.* **(**Fundación Orange España, 2007), accessed February 19, 2012 http://www.fundacionorange.es/fundacionorange/analisisprospectiva.html.
- GARCÍA SAN MIGUEL, LUÍS (ED). *Estudios sobre el derecho a la intimidad.* Tecnos, Madrid, 1992.
- GARCÍA SANZ. ROSA MARÍA. «Redes sociales online: fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)», *Revista de Derecho Político*, (2011): 101-154.
- GARRIDO GÓMEZ, M. ISABEL. «Datos personales y protección del ciudadano» en *Revista de la Facultad de Derecho de la Universidad Complutense,* núm. 87, 1996.
- GARRIGA DOMÍNGUEZ, ANA. *Historia clínica y protección de datos personales: especial referencia al registro obligatorio de los portadores del VIH.* Dykinson, 2011.
- GARRIGA DOMÍNGUEZ, ANA. *La protección de los datos personales en el Derecho español*. Dykinson, Madrid, 1999.
- GAY FUENTES, CELESTE. *Intimidad y tratamiento de datos en las Administraciones Públicas*. Editorial Complutense, Madrid, 1995.
- GONZÁLEZ MURUA ANA ROSA. «Comentario a la S.T.C. 254/1993, algunas reflexiones en torno al artículo 18.4 de la Constitución y la Protección de los Datos personales», en *Revista Vasca de Administración Pública,* núm. 37, 1993.
- GOÑI SEIN, JOSÉ LUIS. *La videovigilancia empresarial y la protección de datos personales.* Thomson, 2007.
- GRIMALT SERVERA, PEDRO, *La responsabilidad civil en el tratamiento automatizado de datos personales*. Comares, Granada, 1999.
- GUICHOT EMILIO. *Publicidad y privacidad de la información administrativa*. Thomson, 2010.
- HECKH, NORMAN. *Memento Experto Protección de Datos*. Francis Lefebvre, 2012.
- HENDERSON, NATHAN C. «The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications» en *Duke Law Journal*, vol 52, 2002.
- HEREDERO HIGUERAS, M. *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter Personal: comentario y textos.* Madrid, Tecnos 1996.
- HEREDERO HIGUERAS, MANUEL. «La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983» en *Documentación Administrativa,* núm. 198, 1983.
- HEREDERO HIGUERAS, MANUEL. «La transposición de la Directiva 95/46/CE en el Derecho positivo español. Una segunda oportunidad en *X años de Encuentros sobre Informática y Derecho*, Aranzadi, Pamplona, 1997.
- HEREDERO HIGUERAS, MANUEL. *La Directiva Comunitaria de protección de los datos de carácter personal*. Tecnos, Madrid, 1998.

- HERRÁN ORTIZ, ANA ISABEL. *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*. Dykinson, Madrid, 2002.
- HERRÁN ORTIZ, ANA ISABEL. *La violación de la intimidad en la protección de datos personales.* Dykinson, Madrid, 1999.
- HERRERO TEJEDOR, FERNANDO. *Honor, intimidad y propia imagen (2. ª ed.).* Colex, Madrid, 1994.
- HERRERO TEJEDOR, FERNANDO. *La intimidad como derecho fundamental.* Colex, Madrid, 1998.
- ISABEL DAVARA FERNÁNDEZ DE MARCOS, JESÚS RUBÍ NAVARRETE Y MARÍA MARVÁN LABORDE. *Hacia la estandarización de la protección de datos personales*. Temas. La Ley, de 2011.
- J. VELASCO DOBAÑO Y LLUIS VELASCO MASSIP. *Auditoría de la protección de datos*. Bosch, 2005.
- JOSÉ LUIS PIÑAR MAÑAS, ÁLVARO CANALES GIL, Mª JOSÉ BLANCO ANTÓN Y MERCEDES ORTUÑO SIERRA. *Protección de Datos de Carácter Personal en Iberoamérica*. Agencia Española de Protección de Datos, 2006.
- KALVEN, HARRY. «Privacy in tort law. Where Warren and Brandeis wrong?» en *Law and Contemporary Problems*, n. 31, 1966.
- KAYSER, PIERRE. *La protection de la vie privée*. Economica, París, 1984.
- KILLIAN, JOHNNY H Y COSTELLO, GEORGE A. *The Constitution of the United States of America. Analysis and Interpretation*. Congressional Research Service, Library Of Congress,U.S. Government Printing Office. Washington, 1996.
- LESSIG LAWRENCE. *Code v2.* Disponible en http://www.codev2.cc/
- LESSIG, LAWRENCE. *El código y otras leyes del ciberespacio.* Taurus, Madrid, 2001.
- Lindop Report on Data Protection. Report of the Committee on Data Protection, Cmnd 7341, 1978.
- LITAN, ROBERT E. «Law and Policy in the Age of the Internet» en *Duke Law Journal*, vol. 50, 2001.
- LÓPEZ GARRIDO, DIEGO. «Aspectos de inconstitucionalidad de la Ley Orgánica 5/92, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal» en *Revista de Derecho Político nº 38.* Madrid, UNED, 1993.
- LÓPEZ JIMÉNEZ, DAVID. «La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación", *Anuario de la Facultad de Derecho de Alcalá de Henares 2*, (2009): 239-276.
- LUCAS MURILLO DE LA CUEVA, PABLO. «La construcción del derecho a la autodeterminación informativa» en *Revista de Estudios Políticos*, Nueva Época, núm. 104, abril-junio 1999.
- LUCAS MURILLO DE LA CUEVA, PABLO. «La primera jurisprudencia sobre el derecho a la autodeterminación informativa», en *Datos Personales, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 1, Marzo 2003.
- LUCAS MURILLO DE LA CUEVA, PABLO. «La protección de los datos personales ante el uso de la informática», en VV. AA., *Diez años de desarrollo constitucional Estudios en*

homenaje al Profesor Don Luis Sánchez Agesta. Universidad Complutense, Madrid, 1989.

- LUCAS MURILLO DE LA CUEVA, PABLO. «Las vicisitudes del Derecho de la protección de datos personales», en *Revista Vasca de Administración Pública*, núm. 58, septiembre-diciembre de 2000.
- LUCAS MURILLO DE LA CUEVA, PABLO. *El derecho a la autodeterminación informativa.* Tecnos, Temas clave, Madrid, 1990.
- LUCAS MURILLO DE LA CUEVA, PABLO. *Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Persona*). Centro de Estudios Constitucionales, Cuadernos y Debates. Madrid, 1993.
- MADRID CONESA, FULGENCIO. *Derecho a la intimidad, informática y Estado de Derecho*. Universidad de Valencia, Valencia, 1984.
- MARÍA DEL CARMEN GUERRERO PICO. *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*. Thomson, 2006.
- MARTÍNEZ DE PISÓN CAVERO JOSÉ. «La configuración constitucional del derecho a la intimidad» en *Derechos y Libertades, Revista del Instituto Bartolomé de las Casas*, año II, núm. 3, 1994.
- MARTÍNEZ DE PISÓN CAVERO JOSÉ. «Vida privada e intimidad: implicaciones y perversiones», en *Anuario de Filosofía del Derecho*, vol. XIV, 1997.
- MARTINEZ DE PISÓN CAVERO, JOSÉ. *El derecho a la intimidad en la jurisprudencia constitucional.* Civitas, Madrid,1992.
- MARTÍNEZ MARTÍNEZ, RICARD. «El Reglamento de desarrollo de Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consideraciones Generales». *Revista española de protección de datos*, págs. 63-94.
- MARTÍNEZ MARTÍNEZ, RICARD. «Videovigilancia y protección de datos personales: la Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos». *Revista Aranzadi de derecho y nuevas tecnologías*, Nº. 13, 2007, págs. 73-92.
- MARTÍNEZ MARTÍNEZ, RICARD. *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*. Tirant lo Blanch, 2009.
- MARTÍNEZ MARTÍNEZ, RICARD. "El derecho fundamental a la protección de datos: perspectivas" in *Internet, Derecho y Política. Las transformaciones del derecho y la Política en 15 artículos*, edited by Pere Fabra, 141-165. Barcelona: Editorial UOC, 2009.
- MARTÍNEZ MARTÍNEZ, RICARD. «¿Controlar a los trabajadores?» en *Actualidad jurídica Aranzad*i, Nº 864, 2013.
- MARTÍNEZ MARTÍNEZ, RICARD. « ¿Interrogantes jurídicos ante los smartphone?», *Actualidad jurídica Aranzadi*, Nº 822, 2011.
- MARTÍNEZ MARTÍNEZ, RICARD. «¿Quién debería olvidarnos en Internet?». *Actualidad jurídica Aranzadi*, Nº 857, 2013.
- MARTÍNEZ MARTÍNEZ, RICARD. «Acceso de los sindicatos a datos correspondientes a los empleados públicos: comentario a la STSJ de Murcia, de 29 de abril 2004, se la Sección Segunda de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Murcia (RJCA 2004, 749)». *Aranzadi social*, Nº 3, 2004, págs. 2896-2900.

- MARTÍNEZ MARTÍNEZ, RICARD. «El complejo encaje normativo de la propuesta de Reglamento general de protección de Datos de la Unión Europea», *Actualidad jurídica Aranzadi*, , Nº 839, 2012.
- MARTÍNEZ MARTÍNEZ, RICARD. «El control de la Agencia de Protección de Datos sobre los ficheros automatizados de datos de carácter personal de las Fuerzas y Cuerpos de Seguridad del Estado». *Cuadernos de la Cátedra Fadriqve Furió,* número 30-31, monográfico en homenaje al profesor Joaquín García Morillo, 2001
- MARTÍNEZ MARTÍNEZ, RICARD. «El control por el Garante Italiano para la protección de los datos personales de los ficheros y archivos de imágenes policiales». I Congreso Internacional de Derecho e Informática en Internet. Marzo a mayo de 2000. Disponible en http://derin.uninet.edu .
- MARTÍNEZ MARTÍNEZ, RICARD. «En torno a la consideración jurídica del número IP». *Nuevas Politicas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nº. 1, 2005 (Ejemplar dedicado a: Los derechos fundamentales y las nuevas tecnologías), págs. 283-304
- MARTÍNEZ MARTÍNEZ, RICARD. «Interés legítimo y protección de datos personales en la sentencia de 8 de febrero de 2012 del TS», en *Revista El Derecho.com*, disponible 20/01/013 en http://www.elderecho.com/administrativo/Interes-proteccion-personales-Tribunal-Supremo_11_372805001.html.
- MARTÍNEZ MARTÍNEZ, RICARD. «La protección de datos en los despachos de abogados», *Actualidad jurídica Aranzadi*, Nº 829, 2011.
- MARTÍNEZ MARTÍNEZ, RICARD. «Las obligaciones del fiscal como usuario de un sistema de información». *Estudios jurídicos*, , Nº. 2012, 2012.
- MARTÍNEZ MARTÍNEZ, RICARD. «Legislación sobre datos personales y Fuerzas y Cuerpos de Seguridad. Los casos español e italiano» en *Ágora Revista de Ciencias Sociales*, monográfico núm. 5 sobre *Policía y Sociedad Democrática*, octubre de 2000.
- MARTÍNEZ MARTÍNEZ, RICARD. «Los ficheros de datos y archivos de imágenes policiales en la legislación italiana. Análisis de las resoluciones dictadas por el Garante Italiano para la protección de los datos personales» en *Revista Española de Derecho Constitucional* núm. 60, septiembre-diciembre de 2000.
- MARTÍNEZ MARTÍNEZ, RICARD. «Protección de datos en la administración de justicia». *Gestión pública de la administración de justicia*. Coord. por Alberto Palomar Olmeda, Aranzadi, 2010, págs. 645-697.
- MARTÍNEZ MARTÍNEZ, RICARD. «Secreto de las comunicaciones v. protección de datos en el ámbito laboral: a propósito de la Sentencia 281/2005 del Tribunal Constitucional Español y del Informe 101/2008 de la Agencia Española de Protección de Datos». *Aranzadi Social*, Vol. 1, Nº. 13 (Dic), 2008, págs. 91-113.
- MARTÍNEZ MARTÍNEZ, RICARD. «Videovigilancia en lugares públicos» en *Repertorio Aranzadi del Tribunal Constitucional,* núm. 17, enero 2000.
- MARTÍNEZ MARTÍNEZ, RICARD. «Videovigilancia, seguridad ciudadana y derechos humanos» en *Claves de Razón Práctica*, núm. 89, enero-febrero 1999.
- MARTÍNEZ MARTÍNEZ, RICARD. El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/ 1999, de 13 de diciembre, de Protercción de Datos de Carácter Personal: aspectos clave». *Revista jurídica de Castilla y León*, (Ejemplar dedicado a: Protección de datos de carácter personal), págs. 257-294.

- MARTÍNEZ MARTÍNEZ, RICARD. *Tecnologías de la información, Policía y Constitución* . Editorial Tirant lo Blanch Llibres, 2001.
- MARTÍNEZ, RICARD . "¿Interrogantes jurídicos ante los Smartphone?", *Actualidad Jurídica Aranzadi* 822 (2010): 13.
- MAYER-SCHONBERGER, VIKTOR. *Delete: The Virtue of Forgetting in the Digital Age*. New Jersey: Princeton University Press, 2009.
- MEGÍAS TEROL, JAVIER. "Privacy by design, construcción de redes sociales garantes de la privacidad " en *Derecho y redes sociales*, ARTEMI RALLO LOMBARTE Y RICARD MARTÍNEZ, 319-334. Pamplona: Civitas: 2010.
- MESSIA, DE LA CERDA, JESÚS. *La protección de datos de carácter personal en las telecomunicaciones*. URJC, 2008.
- MILLER, ARTHUR, R. «Personal privacy in the Computer Age: the challenge of a new technology and information oriented society» en *Michigan Law Review*, vol. 67, 1969.
- MITJANS PERELLÓ, ESTHER. "Derecho y nuevas tecnologías. Impacto de las redes sociales en el derecho a protección de datos personales", *Anuario de la Facultad de Derecho de Alcalá de Henares 2*, (2009): 111-132.
- MORILLAS FERNÁNDEZ, MARTA. "La protección jurídica del menor ante las redes sociales" in *La protección jurídica de la intimidad*, ANGELES JAREÑO LEAL Y FRANCISCO JAVIER BOIX REIG. 361-380. Madrid: IUSTEL, 2010.
- O'HARA KIERON, TUFFIELD MISCHA M. AND SHADBOLT NIGEL. "Lifelogging: Privacy and Empowerment with Memories for Life", *Identity in the Information* Society, 1(2008) accessed February 19, 2012, *DOI 10.1007/s12394-009-0008-4 .*
- ORTEGA SORIANO, JORGE Y SALLA, XAVIER. *Actuaciones inspectoras en materia de protección de datos. El protocolo de inspección*. Bosch, 2008.
- ORTÍ VALLEJO, ANTONIO. «El nuevo derecho fundamental a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)», en *Derecho Privado y Constitución*, núm. 2, 1994.
- PABLO GONZÁLEZ-ESPEJO Y ALBERTO PALOMAR OLMEDA. *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos*. Civitas 2008.
- Palfrey John and Gasser Urs. *Born digital: understanding the first generation of digital natives*. New York: Basic Books, 2008.
- PANIZA FULLANA, ANTONIA. "Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores", *Revista Española de Protección de Datos* 6, (2009): 41-68.
- PÉREZ LUÑO (COORD). *Derechos humanos y constitucionalismo ante el tercer milenio.* Marcial Pons, Madrid, 1996.
- PÉREZ LUÑO, A, E. «El concepto de los derechos humanos y su problemática actual», en *Revista del Instituto Bartolomé de las Casas* año I, febrero-octubre, 1993, núm. I.
- PÉREZ LUÑO, A, E. «El derecho a la autodeterminación informativa», en *Informática y Derecho*, núms. 27-29, 1998.

- PÉREZ LUÑO, A, E. «La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo», en *Anuario de Derechos Humanos*, núm. 4, 1986-1987.
- PÉREZ LUÑO, A, E. «La protección de la intimidad frente a la informática en la Constitución Española de 1978. *Revista de Estudios Políticos. Nueva Época nº 9.* Mayo-junio, 1979.
- PÉREZ LUÑO, A. E. «Informática y libertad. Comentario al artículo 18.4 de la Constitución Española», en *Revista de Estudios Políticos,* núm. 24 (nueva época), noviembre-diciembre 1981.
- PÉREZ LUÑO, A. E. *Derechos humanos, Estado de derecho y constitución. 2.ª ed.* Tecnos, Madrid, 1986.
- PÉREZ LUÑO, A. E. *Los derechos fundamentales.* (6.º Ed.). Ed. Tecnos. Col. Temas clave de la Constitución Española, Madrid, 1995.
- PÉREZ LUÑO, A. E. *Manual de informática y derecho.* Ariel, Barcelona, 1996.
- PÉREZ LUÑO, ANTONIO ENRIQUE. «Dilemas actuales de la protección de la intimidad», en VV. AA, *Problemas actuales de los derechos fundamentales,* (J. M.ª Sauca coord.). Universidad Carlos III y B.O.E., Madrid, 1994.
- PÉREZ LUÑO, ANTONIO ENRIQUE. «Internet y el Derecho», en *Informática y Derecho*, núms. 19-22, Actas de las Jornadas sobre el marco legal y deontológico de la informática. Vol. I, UNED, Mérida, 1998.
- PÉREZ LUÑO, ANTONIO ENRIQUE. «Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data», en GARCÍA SAN MIGUEL, LUÍS (ED). *Estudios sobre el derecho a la intimidad.* Madrid, Ed. Tecnos, 1992.
- PEREZ LUÑO, ANTONIO ENRIQUE. «La tutela de la libertad informática» en VV. AA. *Jornadas sobre el Derecho español de la protección de datos personales*. Agencia de protección de Datos, Madrid 28, 29 y 30 de octubre de 1996.
- PÉREZ LUÑO, ANTONIO ENRIQUE. «Libertad informática y derecho a la autodeterminación informativa», en *I. Congreso sobre Derecho Informático*, Facultad de Derecho de la Universidad de Zaragoza, 1989.
- PÉREZ LUÑO, ANTONIO ENRIQUE. «Perfiles morales y políticos del derecho a la intimidad», en *Anales de la Real Academia de Ciencias Morales y Políticas,* año XLVIII, núm. 73, 1996.
- PIATTINI, MARIO. *Auditoria Informatica*. Un Enfoque Practico. Alfa-Omega. 2001.
- PIÑAR MAÑAS, JOSÉ LUIS. *Redes sociales y privacidad del menor*. Editorial Reus, 2011.
- POST, DAVID G. «Anarchy, State, and the Internet: an essay on law-making in cyberspace»,en *The Journal of Online Law*, junio 1995 artículo 3.º. Disponible en http://warthog.cc.wm.edu/law/publications/jol.
- POST, ROBERT C. «The Social Foundations of Privacy: Community and Self in the Common Law Tort», en *California Law Review*, núm. 5, vol. 77, 1989.
- POULLET, YVES. «Internet et vie privée» en *VV.AA Società dell'informazione. Tutela della riservatezza*. Collana dell'Osservatorio Giordano dell'Amore sui rapporti tra Diritto ed Economia. Giuffré, Milano, 1998.
- PROSSER, WILLIAM. «Privacy», en *California Law Review,* vol. 48, 1960.

- RALLO ARTEMI Y MARTÍNEZ, RICARD *Derecho y redes sociales*. Pamplona: Civitas-Thomson Reuters, 2010.
- RALLO LOMBARTE, ARTEMI Y MARTÍNEZ MARTÍNEZ, RICARD. *Derecho y redes sociales.* 2.ª Ed. Civitas, 2013.
- RAMÓN LACASTA CASADO, ERMENGOL SANMARTÍ GIMÉNEZ … *Auditoría de la protección de datos: Adaptado al Reglamento de Desarrollo de la LOPD (Real Decreto 1720/2007)*. Bosch,2009.
- REBOLLO DELGADO, LUCRECIO. *El derecho fundamental a la intimidad*. Dykinson, Madrid, 2000.
- REBOLLO DELGADO, LUCRECIO. *Vida privada y protección de datos en la Unión Europea*. Dikynson, 2008.
- REIDENBERG, JOEL R. «E-Commerce and Trans-Atlantic Privacy» en *Houston Law Review* vol 38, 2001.
- RODOTÀ STEFANO. «La «privacy» tra individuo e collettività», en *Politica del Diritto,* núm. 5, octubre, 1974.
- RODOTÁ, STEFANO. *Tecnologie e diritti.* Il Mulino, Bologna, 1995.
- RODRÍGUEZ RUIZ, BLANCA. *El secreto de las comunicaciones: tecnología e intimidad*. McGraw Hill, Madrid, 1998.
- ROIG ANTONIO. "E-privacidad y redes sociales", *IDP: Revista de Internet, Derecho y Política*, 9 (2009) *accessed* February 19, 2012, http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp.
- RUBENFELD, JED. «The right of Privacy» en *Harvard Law Review*, vol. 102, núm. 4, 1989.
- RUIZ CARRILLO, ANTONIO. *La protección de los datos de carácter personal*. Bosch, Barcelona, 2001.
- RUIZ MIGUEL, CARLOS, *La Configuración Constitucional del Derecho a la Intimidad.* Tecnos, Madrid, 1995.
- RUIZ MIGUEL, CARLOS. «El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, enero-abril, 2003.
- RUIZ MIGUEL, CARLOS. «En torno a la protección de los datos personales automatizados». *Revista de Estudios Políticas* (Nueva Época), núm. 84 abril-junio, 1994.
- RUIZ MIGUEL, CARLOS. *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas, Madrid, 1994.
- RUÍZ, BLANCA R. «The Right to Privacy: A Discourse-Theoretical Approach», en *Ratio Juris,* vol. 11, núm. 2, junio 1998.
- SANCHO VILLA, DIANA. *Negocios internacionales de tratamiento de datos personales*, Thomson, 2010.
- SCHWARTZ, PAUL M. «Beyond Lessig's *code* for internet privacy: Cyberspace filters, privacy-control, and fair information practices», en *Wisconsin Law Review*, 2000.

- SCHWARTZ, PAUL. M. «Charting a Privacy Research Agenda: Responses, Agreements, and Reflections» en *Connecticut Law Review*, vol. 32, Spring 2000.
- SCHWARTZ, PAUL. M. «Internet privacy and the State» en *Connecticut Law Review*, vol. 32, Spring 2000.
- SCHWARTZ, PAUL. M. «Privacy and Democracy in Cyberspace», en *Vanderbilt Law Review*, vol. 52, 1999.
- SHELTON, DINAH. «Human Rights and the Environment: Jurisprudence of Human Rights Bodies» en *Joint UNEP-OHCHR Expert Seminar on Human Rights and the Environment*. Background Paper No. 2, Geneva, 14-16 January 2002.
- SIBILIA PAULA. *La intimidad como espectáculo*. Buenos Aires: Fondo de Cultura Económica, 2008.
- TASCÓN LÓPEZ, RODRIGO. *El tratamiento por la empresa de datos personales de los trabajadores.* Thomson, 2005.
- TÉLLEZ AGUILERA, ABEL. *Nuevas tecnologías, intimidad y protección de datos*. *Estudio sistemático de la Ley orgánica 15/1999*. EDISOFER, Madrid, 2001.
- TRONCOSO REIGADA, ANTONIO. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, 2010 .
- TRONCOSO REIGADA, ANTONIO. *La Protección de Datos Personales. En Busca del Equilibrio*. Tirant lo Blanch, 2011.
- VELA SÁNCHEZ-CRESPO, CAYETANA. "La privacidad de los datos en las redes sociales", *Revista Española de Protección de Datos* 5, (2008): 231-272.
- VELÁZQUEZ BAUTISTA RAFAEL. *Protección jurídica de datos personales automatizados.* Colex, Madrid, 1993.
- VILASAU SOLANA, MÓNICA. "¿Hasta dónde deben regularse las redes sociales?", *Revista Española de Protección de Datos* 6, (2009): 105-138.
- VILLAVERDE MENENDEZ, IGNACIO. «Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993.» *Revista Española de Derecho Constitucional*, año 14, núm 1. Mayo-agosto 1994.
- VV.AA (LEGALIA). *La protección de datos personales en el ámbito sanitario*. Aranzadi, Pamplona, 2002.
- WARREN , SAMUEL D. Y BRANDEIS, LOUIS D. .«The right to privacy», en *Harvard Law Review*, vol. IV, núm. 5, diciembre de 1890.
- WESTIN, ALAN F. *Privacy and freedom (6.ª ed,).* Atheneum, New York, 1970.
- XALABARDER PLANTADA, RAQUEL. "Redes sociales y propiedad intelectual" in *Derecho y redes sociales*, ARTEMI RALLO LOMBARTE Y RICARD MARTÍNEZ MARTÍNEZ,, 335-354. Pamplona: Civitas: 2010.
- Younger Report on Privacy. Report of Commitee on Privacy, Cmnd, 5012, 1972.
- ZABÍA DE LA MATA, JUAN. *Protección de datos Comentarios al Reglamento*. Lex Nova, 2008.

2.5. Procedimientos de consulta internos y externos.

Para la propuesta del título de Máster en Protección de Datos, (Data Protection Officer), se ha formado un equipo de trabajo interno integrado por varios miembros de la Universidad Internacional de la Rioja. Este trabajo ha sido coordinado por el Dr. D. Ricard Martínez Martínez (redactor de la memoria).

● Carlos Represa Estrada.

Es Licenciado en Derecho. Abogado del Ilustre Colegio de Abogados de Madrid (ICAM). Consultor certificado ISO 27001 por APPLUS. Perito Judicial Informático. Coordinador de la Sección de menores de la Asociación nacional de tasadores y peritos judiciales informáticos Coordinador de la Escuela de Seguridad en la Red de la Junta de Castilla la Mancha. Profesor Asociado de la UNIR y Director del Área de Seguridad en la Red y Protección de menores de la Universidad Internacional de la Rioja.

● Dª Mónica Pérez Iniesta.

Licenciada en Ciencias Empresariales y en Humanidades, y Dª María Gómez Espinosa, Licenciada en Matemáticas, expertas en plataformas de enseñanza virtual, han contribuido en la elaboración de los apartados referentes a la didáctica en entorno virtual.

Las cuestiones referidas a la calidad del título y adecuación del mismo a los criterios de ANECA, han sido enfocados por Dª Mª Asunción Ron Pérez, Directora de la Unidad de Calidad de UNIR. El trabajo de este equipo ha sido posible a través de varias reuniones presenciales entre los meses de junio a octubre de 2013, así como de múltiples consultas telefónicas y reuniones a través de videoconferencia en este mismo periodo. Finalmente, el 4 de noviembre, se llegó a una redacción final consensuada.

Además se ha tenido en cuenta:

1. Al profesorado de UNIR que aportó la visión práctica y de contenidos.
2. Al Vicerrectorado de Estudiantes y Calidad Académica cuya misión es comprobar que el Grado posee un sistema adecuado de acogida para el estudiante y que los requisitos para el estudiante se encuentran correcta y claramente definidos. Además de comprobar que el plan de estudios posee una calidad académica adecuada a los requisitos de UNIR.
3. Al Vicerrectorado de Ordenación Docente y Doctorado con el fin de analizar la capacidad e idoneidad del profesorado de UNIR con el plan de estudios propuesto.
4. Al Consejo Asesor que ratificó la propuesta y aportó la visión de la futura empleabilidad de los egresados.

Y por último y como agentes externos a UNIR se contó con la opinión de la Agencia Española de Protección de Datos y de las empresas que a continuación se indican sobre la idoneidad, pertinencia y futura empleabilidad de los egresados de este Grado.

- Roca y Junyent Abogados.
- Deloitte.
- Gómez Acebo y Pombo, Abogados.
- Ecix Group.
- Hogan Lovells.
- Rosaud Costas Durán.
- Legistel.

Para el desarrollo de la propuesta del título de Máster en Protección de Datos (Data Protection Officer), se han realizado consultas a distintos expertos de reconocido prestigio teniendo en cuenta los siguientes criterios:

● Excelencia académica.

● Vinculación directa con la aplicación práctica de la materia.

● Prestigio Profesional.

De acuerdo con este criterio, en la revisión de la Memoria tomaron parte, así mismo, los siguientes expertos:

● Dr. D. Artemi Rallo Lombarte.

Artemi Rallo Lombarte es Licenciado en Derecho con Premio Extraordinario (1988) y Doctor en Derecho por la Universidad de Valencia (1990). Ha desarrollado su actividad investigadora en centros internacionales como el Instituto Internacional de Derechos Humanos con sede en Estrasburgo, el Departamento de Teoría del Estado de la Universidad La Sapienza (Roma) y el Centre de Recherche de Droit Constitutionnel de la Universidad Paris I Pantheòn- Sorbonne.

Es autor de numerosas monografías, libros colectivos y artículos científicos en revistas especializadas nacionales e internacionales. Ha participado en líneas y proyectos de investigación nacionales e internacionales sobre las transformaciones contemporáneas de la Administración Pública protagonizadas por las Administraciones independientes, las garantías electorales, las amenazas al pluralismo informativo, la problemática del Parlamento actual, la protección de los derechos fundamentales en el proceso de integración europea y los procesos de descentralización política en los Estados miembros de la Unión Europea. Ha colaborado con programas europeos de apoyo institucional en América Latina destinados a promover la descentralización política y al fortalecimiento de las instituciones parlamentarias, del Poder Ejecutivo y del Poder Judicial.

De 2004 a 2007 fue Director General del Centro de Estudios Jurídicos del Ministerio de Justicia. De 2007 a 2011 fue Director de la Agencia Española de Protección de Datos y. miembro del Grupo de Trabajo del Artículo 29 y presidente de la Red Iberoamericana de Protección de Datos. Desde este periodo hasta nuestros días ha desempeñado una intensa labor académica en el ámbito del derecho fundamental a la protección de datos.

● Dr. D. José Luís Goñi Sein.

José Luis Goñi Sein es Catedrático de Derecho del Trabajo y de la Seguridad Social de la Universidad Pública de Navarra. Ha sido Letrado del Tribunal Constitucional durante los años 1991-1995. Es doctor en Derecho por la Universidad de Salamanca con premio extraordinario (1986). Ha desempeñado distintos cargos académicos: Secretario y Subdirector-Director de la Escuela Universitaria de Graduados Sociales en la Universidad de Salamanca (1987-1990); Adjunto al Rector de la Universidad Pública de Navarra (1999-2001), Secretario General de la Universidad Pública de Navarra (2001-2003), Director del Departamento de Derecho Privado de la UPNA (2004-2008), Vicedecano de la Facultad de Ciencias Jurídicas de la UPNA (2008-2009) Decano de la Facultad de Ciencias Jurídicas desde octubre de 2009 hasta marzo de 2012.

Ha impartido docencia en la Facultad de Derecho de San Sebastián de la Universidad del País Vasco (1981-1982 y 1995-1997), Facultades de Derecho y Ciencias Empresariales de la Universidad de Salamanca (1982-1991), y en las Facultades de Ciencias Humanas y Sociales, Ciencias Empresariales y Ciencias Jurídicas de la Universidad Pública de Navarra (1997-hasta la actualidad). Ha sido profesor colaborador del Instituto de Empresa (IE Law School-Executive Education) (Madrid) y del Institut d'Educació Continua de la Universitat Pompeu Fabra (Barcelona). Ha impartido alrededor de ciento cincuenta conferencias y ponencias dentro y fuera de España, sobre temas de su especialidad, en particular en lo relativo a los derechos fundamentales en la relación laboral.

Es responsable de un grupo de investigación de Derecho del Trabajo y ha dirigido y participado en proyectos de investigación financiados por España, la Comunidad Europea y la Comunidad Foral de Navarra, habiendo recibido en 2007 la calificación de excelencia nacional por parte de la Agencia Nacional Evaluadora de la Actividad Investigadora (ANEP).

Entre otras tareas profesionales, ha colaborado como experto y asesor científico del Gobierno de Navarra en la elaboración de diversos planes y proyectos normativos para la Comunidad Foral de Navarra y ha intervenido en la solución extrajudicial de conflictos de trabajo de Navarra, siendo lo más destacable de su participación sendos laudos de obligado cumplimiento dictados en la huelga de ambulancias y en la huelga de autobuses urbanos de transporte público. Desde 1997 pertenece a los Colegios Arbitrales del Tribunal Laboral de Navarra y del Servicio Interconfederal de Mediación y Arbitraje (Fundación SIMA) con sede en Madrid.
Es autor de más de 75 publicaciones sobre temas de su especialidad, de los que destacan las siguientes monografías y participaciones en obras colectivas, de entre las que cabe destacar por su carácter pionero en lo que a esta memoria se refiere su obra "El respeto a la esfera privada del trabajador. Un estudio sobre los límites del poder de control empresarial, Civitas, Madrid, 1988, pp. 322., ISBN: 84-7398-554-0" así como "La videovigilancia empresarial y la protección de datos personales: Thomson-Civitas/ APDCM, Pamplona, 2007, PP. 254, ISBN: 978-84-470-2701-9".

● Dr. D. Mario Piattini Velthuis.

Doctor y Licenciado en Informática por la Universidad Politécnica de Madrid. Licenciado en Psicología por la Universidad Nacional de Educación a Distancia. Máster en Auditoría Informática

(CENEI). Especialista en la Aplicación de Tecnologías de la Información en la Gestión Empresarial (CEPADE-UPM). Máster en Dirección de Recursos Humanos (IMAFE). Master´s Certificate en Dirección de Proyectos (The George Washington University). Diplomado en Calidad por la Asociación Española para la Calidad. Auditor Jefe ISO 15504 por AENOR. CISA, CISM, CRISC y CGEIT por la ISACA. Ha trabajado como consultor para numerosas organizaciones (Ministerio de Industria y Energía, Ministerio de Administraciones Públicas, Siemens-Nixdorf, Unisys, Hewlett-Packard, Oracle, ICM, Atos-Ods, Indra/Soluziona, Sistemas Técnicos de Loterías, etc.). Socio fundador de las empresas Cronos Ibérica y Kybele Consulting, S.L. Ha sido profesor asociado en las universidades Complutense y Carlos III de Madrid y Coordinador del Área de Ciencias de la Computación y Tecnología Informática de la Agencia Nacional de Evaluación y Prospectiva (ANEP). Catedrático de Universidad de Lenguajes y Sistemas Informáticos en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha (UCLM), donde dirige el grupo de investigación Alarcos, especializado en Calidad de Sistemas de Información y Socio-Director Científico de Alarcos Quality Center, S.L. empresa de base tecnológica de la UCLM. También es Director del Centro Mixto de Investigación y Desarrollo de Software UCLM-INDRA Software Labs y Director del Instituto de Tecnologías y Sistemas de Información (ITSI) de la UCLM.

● Dr. D. Julián Valero Torrijos

Profesor de Derecho Administrativo en la titulación conjunta Derecho-ADE y director del Curso a distancia sobre Protección de Datos Personales en la Universidad de Murcia. Entre sus líneas de investigación hay que señalar:

- Participante en el Proyecto de Investigación Breaking barriers to e-Government, coordinado por el Internet Institute de la Universidad de Oxford y financiado por la Comisión Europea

-Participante en el Proyecto de Investigación Estudio interdisciplinar de las responsabilidades de los proveedores de información en Internet. Problemas de segunda generación: los límites de la neutralidad tecnológica, financiado por el Ministerio de Ciencia y Tecnología

-Participante en el Proyecto de Investigación La problemática jurídica de las tecnologías de la información y las comunicaciones en la Administración Pública, financiado por la Fundación Séneca

-Miembro del Grupo de Investigación "Derecho Administrativo" de la Universidad de Murcia

Últimas publicaciones:

-El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común, 2ª ed., Comares, Granada, 2007

-E. Gamero Casado y J. Valero Torrijos (Coordinadores): La Ley de Administración electrónica. Comentario sistemático a Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, Ed. Aranzadi, 2007

-"Acceso a los servicios y difusión de la información por medios electrónicos", en E. Gamero Casado y J. Valero Torrijos (Coordinadores): La Ley de Administración electrónica. Comentario

sistemático a Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, Ed. Aranzadi, 2007, capítulo 3

-"Potestad administrativa sancionadora", en VV.AA.: Responsabilidades de los proveedores de información en Internet, Comares, Granada, 2007.

-"Responsabilidad patrimonial de las Administraciones Públicas por difusión de contenidos propios en Internet", en VV.AA.: Responsabilidades de los proveedores de información en Internet, Comares, Granada, 2007.

-La nueva regulación legal del uso de las tecnologías de la información y las comunicaciones en el ámbito administrativo: ¿el viaje hacia un nuevo modelo de Administración, electrónica?, Autonomies, Revista Catalana de Derecho Público, núm. 35, 2007

-(junto con D. Sánchez Martínez) Protección de datos personales, DNI-e y prestación de servicios de certificación: ¿un obstáculo para la e-Administración? , Datospersonales.org Revista de Agencia de Protección de Datos de la Comunidad de Madrid, núm. 25, enero 2007

-El acceso telemático a la información administrativa: un presupuesto inexcusable para la e-Administración, en L. COTINO HUESO (Coord.), Libertades, democracia y gobierno electrónicos, Comares, Granada, 2005.

● D. Jesús Rubí Navarrete.

- Abogado.1977
- Director del Gabinete del Ministro de Justicia.1982-1986
- Secretario General Técnico del Ministerio de Relaciones con las Cortes 1988.
- Director General de Relaciones con las Cortes 1989-1994
- Vocal del Tribunal de Defensa de la Competencia 1996-1999
- Adjunto al Director de la Agencia de Protección de Datos. 1999-2002
- Subdirector General de Inspección de Datos de la Agencia de Protección de Datos. 2002-2005
- Actualmente Adjunto al Director de la Agencia Española de Protección de Datos

Ha sido autor de diversas publicaciones en materia de publicidad, derecho de la competencia, procedimiento administrativo y protección de datos personales. Asimismo, ha colaborado como Profesor en diferentes Universidades de España y ha participado en diferentes reuniones y conferencias internacionales.

● D. Javier Puyol Montero.

Magistrado en excedencia y Letrado del Tribunal Constitucional actualmente es Director de la Asesoria Juridica Contenciosa Corporativa de BBVA. Es consultor en tecnologias de la informacion y la comunicación y especialista universitario en comercio electrónico. Diploma de Estudios Avanzados con y un trabajo sobre cloud computing en ICADE Universidad Pontificia de Comillas, con tesis doctoral en curso (prevista su lectura en enero 2014). Premio estatal de investigacion de la Agencia Española de Protección de Datos-2013.

Director de la Revista de Derecho de las Nuevas Tecnologias SEPIN. Participante habitual en la Red Iberoamericana de Protección de Datos y en el Congreso Iberoamericano de Proteccion de Datos (Cartagena de Indias). Colaborador con la Universidad de Berkeley (California). Co-Director del Primer Congreso Europeo de Proteccion De Datos. Miembro del Consejo de Certificacion de la Asociacion Española de Privacidad (APEP).

Ha participado como director y profesor en diversos estudios de máster como el Master de asesoria juridica de empresas (Escuela de Negocios San Pablo CEU). Asimismo ha sido director y profesor en:

● Curso general sobre proteccion de datos del Ilustre Colegio de Abogados de Madrid (ICAM).

● Curso sobre procedimientos y documentos en materia de proteccion de datos del Ilustre Colegio de Abogados de Madrid (ICAM).

● Curso sobre aspectos contractuales de la proteccion de datos del Ilustre Colegio de Abogados de Madrid (ICAM).

Ha sido profesor en materia de protección de datos en:

● Master de Derecho privado del Ilustre Colegio de Abogados de Madrid (ICAM).

● Curso de Derecho bancario del Ilustre Colegio de Abogados de Madrid (ICAM).

● Master de del Instituto de Empresa sobre “proteccion de datos y seguridad”

● Cátedra Google sobre proteccion de datos Universidad San Pablo CEU.

Mantiene una intensa producción editorial en esta materia en la que destaca su condición de coautor del libro “20 Años de Proteccion de Datos en España”. Agencia Española de Protección de Datos, ZABÍA DE LA MATA, JUAN. *Protección de datos Comentarios al Reglamento*. Lex Nova, 2008. Y TRONCOSO REIGADA, ANTONIO. *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, 2010.

● Dña. Mª José de Artaza y Torres.

Licenciada en Derecho por la Universidad Complutense de Madrid.

Socia Gerente y Responsable de área de SOLUCIONES OPERATIVAS DE CONSULTORIA, S.L. Responsable del área de relaciones laborales y Creación de Empresas. Responsable del Área de consultoría fundamentalmente Implantación y Auditoría de la ISO 9000 y 14000. Consultoría de Protección de Datos y Privacidad.

Socia Gerente y Responsable de Área CAU MADRID CONSULTORES, S.L.

Asesoría y Consultoría de Empresas, fundamentalmente PYMES. Especialización en Consultoría de Empresas, subvenciones y ayudas públicas.

Consultor Senior: Especializado en las áreas de budgeting, forecasting, implantación y supervisión de sistemas de control de gestión, reporting gestional y análisis económico-financieros.

Tipo	Referente/medio de consulta	Aportación al Plan de Estudios
Expertos		
	Dr. D. Artemi Rallo Lombarte.	Conocimiento profundo del marco constitucional del derecho fundamental a la protección de datos, sobre la conformación de las autoridades administrativas independientes y su experiencia en la dirección de la Agencia Española de Protección de Datos.
	Dr. D. José Luís Goñi Sein.	Conocimiento profundo del marco de los aspectos sobre el tratamiento de datos personales en el marco de las relaciones laborales. Destacado experto en videovigilancia.
	Dr. D. Mario Piattini Velthuis.	Experto en aspectos informáticos y en particular en el desarrollo de bases de datos, la seguridad informática y la auditoría de seguridad.
	Dr. D. Julián Valero Torrijos	Experto en protección de datos personales en las administraciones públicas, administración electrónica, transparencia y acceso a la información y en general en el impacto de internet en el Derecho.
	D. Jesús Rubí Navarrete.	Su ámbito de gestión le permite un conocimiento exhaustivo sobre el desarrollo, aplicación e implementación práctica del derecho fundamental a la protección de datos en todos los sectores.
	D. Javier Puyol Montero	Su ámbito de gestión le permite un conocimiento exhaustivo sobre el desarrollo, aplicación e implementación práctica del derecho fundamental a la protección de datos en el marco de la gestión empresarial, con particular atención a los aspectos de gestión financiera, marketing y publicidad, solvencia, blanqueo de capitales, gestión de personal o videovigilancia. A lo que añada su expertise en materia de Cloud Computing.

Tipo	Referente/medio de consulta	Aportación al Plan de Estudios
Legislación		
	LOPD[11] y RLOPD[12]	Marco jurídico básico general.

[11] Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
[12] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

	Ley Catalana (APDCAT)[13]	Especificidad y conformación de la autoridad autonómica de protección de datos personales
	Ley Vasca (AVPD)[14]	Especificidad y conformación de la autoridad autonómica de protección de datos personales
	Normativa nacional conexa	Indispensable para aplicar el derecho fundamental a la protección de datos sectorialmente
	Convenios de la ONU	Define el valor universal de la privacidad
	C. Europeo de Derechos Humanos.[15]	Define el marco europeo de protección de datos.
	Convenio 108/1981[16]	Define el marco europeo de protección de datos.
	Tratados de La Unión Europea	Consagra el derecho fundamental a la protección de datos en el contexto de la UE.
	Carta de los Derechos Fundamentales de la Unión Europea.	Consagra el derecho fundamental a la protección de datos en el contexto de la UE.
	Directiva 95/46/CE[17]	Define el marco regulador común y el modelo de protección de datos personales en la UE

Tipo	Referente/medio de consulta	Aportación al Plan de Estudios
Legislación		
	Directivas conexas[18].	Desarrollan el derecho fundamental a la protección de datos especialmente en el sector de las telecomunicaciones.
	Legislación iberoamericana	Constituyen un marco de evolución del derecho fundamental a la protección de datos basado en el modelo de la UE.
	Legislación EE.UU.	Indispensable para confrontar los distintos modelos de privacidad
	Propuesta de Reglamento UE[19]	Indispensable para definir el futuro marco de actuación

[13] Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.
[14] Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
[15] Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Instrumento de Ratificación de 26 de septiembre de 1979.
[16] Convenio del Consejo de Europa, de 28 de enero 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984 .
[17] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (D.O.C.E. serie L. núm. 281, de 23 de noviembre de 1995).
[18] ● Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos (DOCE, serie L, núm. 77 de 27 de abril).
● Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (DOCE, serie L, núm. 24 de 30 de enero).
● Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DOCE, serie L, núm. 178/1 de 17 de julio).
● Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas o Directiva sobre la privacidad y las comunicaciones electrónicas (DOCE, Serie L, núm. 201 de 31 de julio).
● Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.
● Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
● Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores
[19] Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos, personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Bruselas, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD). Existe una versión no oficial del texto tras su aprobación por la Comisión LIBE del Parlamento Europeo.

	Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura).	profesional de los profesionales dela privacidad.
Jurisprudencia		
	Tribunal Constitucional	Define los aspectos nucleares del derecho fundamental a la protección de datos en España.
	Tribunal Supremo/Audiencia nacional	Define las condiciones de aplicación de la normativa de desarrollo del derecho fundamental a la protección de datos en España.
	Tribunal de Justicia de la UE	Define los aspectos nucleares del derecho fundamental a la protección de datos en la UE y determina las condiciones de aplicación de las directivas que la desarrollan.
	Tribunal Europeo de Derechos Humanos	Define los aspectos nucleares del derecho fundamental a la protección de datos en el sistema del Consejo de Europa.

Tipo	Referente/medio de consulta	Aportación al Plan de Estudios
Documentos		
	Memorias de la Agencia Española de Protección de Datos	Permiten conocer la trayectoria, las condiciones de aplicación y el futuro inmediato del derecho fundamental a la protección de datos en España.
	Guías y publicaciones de la Agencia Española de Protección de Datos.	Constituyen verdaderas Guidelines para la aplicación sectorial de la normativa en España.
	Informes de la Agencia Española de Protección de Datos	Constituyen verdaderas Guidelines para la aplicación de la normativa en los supuestos concretos a los que responden.
	Resoluciones de la Agencia Española de Protección de Datos	Operan como una especie de jurisprudencia y orientan las políticas de cumplimiento normativo del sector.
	Publicaciones de Inteco.	Constituyen guías prácticas de referencia generalmente basadas en estudios empíricos que aproximan la realidad social y económica al Derecho y a la inversa. ● Estudio sobre la protección de datos en las empresas españolas. ● Estudio sobre seguridad en dispositivos móviles y smartphones (1er cuatrimestre 2012). ● Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles, 1er cuatrimestre de 2012 (18ª oleada). ● Estudio sobre la percepción de los usuarios acerca de su privacidad en Internet. ● Estudio sobre seguridad en dispositivos móviles y smartphones, informe anual 2011. ● Estudio sobre cloud computing en el sector público en España.

		● Guía para empresas: identidad digital y reputación online. ● Guía para usuarios: identidad digital y reputación online. ● Guía para empresas: seguridad y privacidad del cloud computing.
	Agenda Digital para España. Ministerio de Industria, Energía y Turismo-Junio 2013. Agenda digital para España el Plan de confianza en el ámbito digital.	Define objetivos de futuro que o bien deberán implementarse teniendo en cuenta la normativa sobre protección de datos personales o exigirán desarrollos específicos.
	Planes de estudio.	Demuestran la existencia de un mercado con una oferta específica muy limitada.
	Directrices de la OCDE	Indispensable para confrontar los distintos modelos de privacidad y en este caso los basados en la autorregulación.
	Documentos del Grupo de trabajo del artículo 29.	Indispensables para entender cómo aplicar los elementos esenciales de las Directivas UE y como abordar desde estas los retos tecnológicos emergentes.
	Recomendaciones del Comité de Ministros del Consejo de Europa.	Referentes interpretativos y aplicativos de las normas del sistema del Consejo de Europa a sectores específicos.
	ENISA	Documentación indispensable para entender el impacto de la seguridad en el derecho fundamental a la protección de datos y las condiciones para el análisis de riesgos y la implementación de medidas de seguridad.
	Consumer Privacy Bill of Rights.	Propuesta del Gobierno Obama que define el futuro de la Privacidad en EE.UU.
	APEC. Privacy Framework.	Indispensable para confrontar los distintos modelos de privacidad y en este caso los compartidos por el bloque de países Asia-pacífico.
	Privacy by Design.	Documento indispensable para el desempeño profesional del experto en protección de datos.
	Privacy Impact Assessment.	Documento indispensable para el desempeño profesional del experto en protección de datos.
	Bibliografía general.	Se plantea una bibliografía exhaustiva que permita orientar tanto el trabajo final de máster como futuros trabajos de investigación doctoral.
Bibliografía	Dialnet	Referencias a trabajos publicados indexadas en Dialnet
Tesis doctorales	Dialnet	Referencias a tesis doctorales indexadas en Dialnet
Asociación profesional	Asociación Profesional Española de Privacidad	Dos millones de empresas en España no han registrado sus ficheros en la Agencia Española de Protección de Datos. http://www.apep.es/28-de-enero-da-de-la-proteccin-de-datos-en-europa/

El conjunto de documentación y aportaciones internas y externas analidas acreditan que un estudio de máster sobre protección de datos resulta plenamente justificado ya que:

● Constituye un ámbito de interés académico e investigador de primera magnitud con multitud de campos abiertos a la innovación.

● En un futuro cercano el delegado de protección de datos será una figura obligatoria y necesaria en virtud de la regulación europea.

● Incluso con la normativa vigente las carencias en el cumplimiento evidencian la existencia de un mercado emergente para este tipo de profesionales.

● Los distintos estudios y los planes de la UE y el Gobierno de España para el impulso de una Agenda Digital erigen la privacidad como uno de los motores de confianza para la economía digital.

3. COMPETENCIAS.

3.1. Competencias Básicas (CB)

	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 de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
CB8	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
CB9	Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
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.

3.2. Competencias Generales (CG)

	COMPETENCIAS GENERALES
CG1	Integrar la normativa específica, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, en el conjunto del Ordenamiento Jurídico para adoptar soluciones sectoriales válidas.
CG2	Abordar procesos de implementación del cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
CG3	Ser capaz de integrarse en equipos de trabajo con profesionales de distintos perfiles y en particular los relativos a la seguridad informática y áreas afines, y de ofrecer soluciones de cumplimiento normativo útiles desde el punto de vista de la protección de datos.
CG4	Ser capaz de evaluar las necesidades sectoriales de protección de datos interpretando de modo sistemático las necesidades del negocio.

CG5	Diseñar un proceso sustancial de investigación con seriedad académica integrando en su procedimiento de análisis conocimientos específicos relativos a al tipo de datos personales, naturaleza del tratamiento, flujo de la información y necesidades de cumplimiento normativo, así como en su caso, respecto de una comprensión de la tecnología susceptible de investigación.
CG6	Realizar un análisis crítico, evaluación y síntesis de ideas nuevas y complejas integrando en los parámetros normativos vigentes, criterios que permitan abordar nuevos fenómenos tecnológicos que requieran un diseño basado en privacidad/protección de datos.
CG7	Ser capaces de fomentar, en contextos académicos y profesionales, el avance tecnológico, social o cultural dentro de una sociedad basada en el conocimiento, integrando el respeto al derecho fundamental a la protección de datos en el desarrollo de las tecnologías de la información y las comunicaciones.
CG8	Predecir y controlar la evolución de situaciones complejas, mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional de la aplicación de las normas sobre protección de datos personales en el contexto de las tecnologías de la información y las comunicaciones, en general multidisciplinar.
CG9	Desarrollar la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia del conocimiento.
CG10	Asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio sectorial, integrando conocimientos de áreas relacionadas con las tecnologías de la información y las comunicaciones.

3.3. Competencias Específicas (CE)

	COMPETENCIAS ESPECÍFICAS
CE1	Adquirir una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en el ámbito de la protección de datos personales.
CE2	Ser capaces de insertarse en entornos de trabajo multidisciplinar con profesionales de otras áreas de especialización ya sea jurídica, gestión y administración de empresa, tecnologías de la información, publicidad y marketing o cualesquiera otras afectadas por su tarea.

CE3	Conocer los distintos modelos de regulación de la privacidad en las distintas áreas regionales (Europa, América, Asia-Pacífico) y establecer condiciones para el tratamiento de datos personales en cada una de ellas.
CE4	Conocer los distintos modos de tutela judicial y administrativa del derecho fundamental a la protección de datos y asesorar en el desarrollo de procedimientos sancionadores.
CE5	Ser capaz de definir sus funciones y competencias cuando se inserte en el marco de una organización como delegado de protección de datos o responsable de seguridad, y dimensionar sus tareas cuando actúe como proveedor externo de estos servicios.
CE6	Ser capaz de definir el ámbito de aplicación de la legislación vigente, identificar ficheros, tratamientos y flujos de información sujetos a la misma y diseñar proyectos de adecuación.
CE7	Ser capaz de evaluar la proporcionalidad, legalidad y viabilidad de los tratamientos de datos personales conforme a la legalidad vigente.
CE8	Ser capaz de diseñar procesos de recogida y tratamiento de datos personales en cualquier circunstancia (entrevista, formulario, formulario online, o proveniente de terceros), y en particular en aquellos casos sometidos a obligaciones específicas en materia de consentimiento y/o verificaciones de edad o identidad.
CE9	Ser capaz de implementar sistemas de atención y monitorización para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento.
CE10	Ser capaz de evaluar prestaciones de servicios con acceso a datos personales y redactar contratos de “encargado del tratamiento” así como de elaborar el pliego de condiciones técnicas para contratos de externalización de servicios que comporten un tratamiento de datos personales que cumpla los estándares y normativas vigentes.
CE11	Capacidad para comprender la importancia de la negociación, los hábitos de trabajo efectivos, el liderazgo y las habilidades de comunicación en entornos de gobierno corporativo y en particular en entornos de desarrollo de software.
CE12	Capacidad para diseñar, desarrollar, seleccionar o evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
CE13	Capacidad para planificar, concebir, desplegar y dirigir proyectos de implementación del cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre,

	de protección de datos de carácter personal, liderando su puesta en marcha y su mejora continua y valorando su impacto económico y social.
CE14	Capacidad para aplicar metodologías de “privacy by design” y "privacy impact Assessment” en el desarrollo e implementación de proyectos de cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
CE15	Capacidad para evaluar la seguridad exigible en el tratamiento de datos personales con identificación de los niveles y toma de decisiones sobre su desarrollo e implementación.
CE16	Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes y en particular la Disposición Adicional Única del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y/o del Esquema Nacional de Seguridad.
CE17	Capacidad para planificar, concebir, desplegar y dirigir proyectos de auditoria de seguridad conforme al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter persona y en su caso conforme al Esquema Nacional de Seguridad.
CE18	Conocer los distintos estándares de seguridad existentes en el mercado.
CE19	Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones desde el punto de vista jurídico, informático y de gestión.
CE20	Ser capaz de aplicar sectorialmente el derecho fundamental a la protección de datos en cada ámbito de gestión.
CE21	Informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les incumben y documentar esta actividad.
CE22	Ser capaz de supervisar la implementación y aplicación de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
CE23	Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.

3.4. Competencias transversales (CT)

	COMPETENCIAS TRANSVERSALES
CT1	Analizar de forma reflexiva y crítica las cuestiones más relevantes de la sociedad actual para una toma de decisiones coherente.
CT2	Identificar las nuevas tecnologías como herramientas didácticas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje grupal.
CT3	Aplicar los conocimientos y capacidades aportados por los estudios a casos reales y en un entorno de grupos de trabajo en empresas u organizaciones.
CT4	Adquirir la capacidad de trabajo independiente, impulsando la organización y favoreciendo el aprendizaje autónomo.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1. Sistemas de información previa a la matriculación

4.1.1. Perfil de ingreso recomendado

Para el acceso a los estudios de Máster en Protección de Datos (Data Protection Officer), se recomienda poseer las siguientes capacidades previas:

● Idioma: castellano.

● Estar en posesión de un título superior de Graduado o Licenciado en Derecho.

● Estar en posesión de un título superior de grado, diplomatura o licenciatura cuya troncalidad obligue a recibir formación jurídica básica: Ciencias Políticas, Administración y Dirección de Empresas, Relaciones Laborales-Graduado Social y Criminología.

● Haber cursado estudios de postgrado en materias afines como Derecho de las Telecomunicaciones o aspectos jurídicos del Comercio Electrónico.

● Haber cursado estudios de postgrado relacionados con la seguridad de la información que necesariamente deban haber incorporado como formación obligatoria materias de introducción al Derecho y Derecho sectorial.

● Ser capaz de entender conceptos tecnológicos en el ámbito de las tecnologías de la información.

4.1.2. Canales de difusión para informar a los potenciales estudiantes

Para informar a los potenciales estudiantes sobre la Titulación y sobre el proceso de matriculación se emplearán los siguientes canales de difusión:

- Página web oficial de la Universidad Internacional de La Rioja
- Sesiones informativas en diversas ciudades de España y en algunos puntos del extranjero. En concreto para este año se prevé la asistencia a ferias y *workshops* tanto en España como en el exterior, organizados por Eduespaña en colaboración con el Instituto de Comercio Exterior (ICEX).
- Inserciones en los medios de comunicación nacionales internacionales incluidos los distintos canales de comunicación en Internet: Google AdWords, E-magister, Oferta formativa, Infocursos y Universia.

Asimismo y con el objetivo de internacionalizar UNIR ya que el carácter de su enseñanza así lo permite, se están estableciendo los primeros contactos con promotores educativos de estudios universitarios en el extranjero (Study Abroad):

ACADEMIC YEAR ABROAD (AYA): www.ayabroad.org/

STUDY ABROAD SPAIN: www.studyabroad.com/spain.html

Study, travel or work in Spain (UNISPAIN): www.unispain.com/

Cultural Experiences Abroad (CEA): www.gowithcea.com/programs/spain.html

4.1.3. Procedimientos de orientación para la acogida de estudiantes de nuevo ingreso

UNIR cuenta con una oficina de Atención al Alumno que centraliza y contesta todas las solicitudes de información (llamadas y correos electrónicos) y un Servicio Técnico de Orientación (Contact center) que gestiona y soluciona todas las preguntas y posibles dudas de los futuros estudiantes referidas a:

- Descripción de la metodología de UNIR. Para ello, los alumnos tendrán acceso a una demo donde se explica paso por paso.
- Niveles de dificultad y horas de estudio estimadas para poder llevar a cabo un itinerario formativo ajustado a las posibilidades reales del estudiante para poder planificar adecuadamente su matrícula.
- Descripción de los estudios.
- Convalidaciones de las antiguas titulaciones.
- Preguntas sobre el Espacio Europeo de Educación Superior.

Finalmente, el personal de administración y servicios (PAS) a través del el Servicio de Admisiones proporcionará al estudiante todo el apoyo administrativo necesario para realizar de manera óptima todo el proceso de admisión y matriculación por medio de atención telefónica, por correo electrónico, con información guiada en la web para la realización de la matrícula on-line.

4.2. Requisitos de acceso y criterios de admisión

4.2.1. Requisitos de acceso

Para poder acceder al Máster es necesario contar con titulación universitaria, según el artículo 7 del RD 39/1997. Este requisito se corresponde con los criterios de acceso establecidos en el artículo 16 del RD 1393/2007 modificado por el RD 861/2010:

- Estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior del Espacio Europeo de Educación Superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster
- Titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de homologar sus Títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes Títulos universitarios oficiales españoles y que facultan en el país expedidor del Título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará en ningún caso, la homologación del Título previo de que esté en posesión el

interesado, ni su reconocimiento a otros efectos que el cursar las enseñanzas del Máster.

4.2.2. Criterios de admisión

El Máster se dirige preferentemente a graduados o licenciados en Derecho. Asimismo, podrán cursarlo graduados, licenciados o postgraduados cuyas áreas de conocimiento guarden relación directa con entornos de gestión de las organizaciones que requieran de un tratamiento intensivo de datos de carácter personal con el correspondiente uso de tecnologías de la información, siempre que incorporen conocimientos jurídicos adecuados para abordar el objeto de estudio del máster: Administración y Dirección de Empresas, Ciencias políticas, Relaciones Laborales-Graduado Social y Criminología.

Así mismo, podrán cursar el máster postgraduados cuyas áreas de conocimiento guarden relación directa por tratarse de materias afines como el Derecho de las Telecomunicaciones o aspectos jurídicos del Comercio Electrónico.

En caso de que la demanda de preinscripción supere el número de plazas ofertadas se concederá prioridad a los graduados o licenciados en Derecho o Informática atendiendo como criterio secundario al orden de preinscripción.

4.3. Sistemas de apoyo y orientación a los alumnos una vez matriculados

4.3.1. Primer contacto con el campus virtual

Cuando los estudiantes se enfrentan por primera vez a una herramienta como es una plataforma de formación en Internet pueden surgir muchas dudas de funcionamiento.

¿Cómo superamos este primer problema? A través de un periodo de adaptación previo al comienzo del curso denominado semana cero, en el que el alumno dispone de un aula de información general que le permite familiarizarse con el campus virtual.

En esta aula se explica mediante vídeos y textos el concepto de UNIR como universidad en Internet. Incluye la metodología empleada, orientación para el estudio y la planificación del trabajo personal y sistemas de evaluación. El estudiante tiene un primer contacto con el uso de foros y envío de tareas a través del aula virtual.

Además los alumnos reciben en su domicilio una guía de funcionamiento del aula virtual.

4.3.2. Seguimiento diario del alumnado

UNIR aplica un Plan de Acción Tutorial, que consiste en el acompañamiento y seguimiento del alumnado a lo largo del proceso educativo. Con ello se pretende lograr los siguientes objetivos:

- Favorecer la educación integral de los alumnos.
- Potenciar una educación lo más personalizada posible y que tenga en cuenta las necesidades de cada alumno y recurrir a los apoyos o actividades adecuadas.
- Promover el esfuerzo individual y el trabajo en equipo.

Para llevar a cabo el plan de acción tutorial, UNIR cuenta con un grupo de tutores personales. **Es personal no docente** que tiene como función la guía y asesoramiento del estudiante durante el curso. Todos ellos están en posesión de títulos superiores en el ámbito de la pedagogía. Se trata de un sistema muy bien valorado por el alumnado, lo que se deduce de los resultados de las encuestas realizadas a los estudiantes.

A cada tutor personal se le asigna un grupo de alumnos para que realice su seguimiento. Para ello cuenta con la siguiente información:

- El acceso de cada usuario a los contenidos teóricos del curso además del tiempo de acceso.
- La utilización de las herramientas de comunicación del campus (chats, foros, grupos de discusión, etc.).
- Los resultados de los test y actividades enviadas a través del campus.

Estos datos le permiten conocer el nivel de asimilación de conocimientos y detectar las necesidades de cada estudiante para ofrecer la orientación adecuada.

4.3.3. Proceso para evitar abandonos

Cuando se detecta poca o nula participación de un estudiante en las actividades del curso, el tutor personal se pone en contacto con el estudiante. El objetivo es que se sienta «arropado» y motivado, y facilitar su integración y participación. De esta manera, se evitan buena parte de abandonos causados por desmotivación, sensación de aislamiento, pérdida de interés, etc.

4.4. Sistemas de transferencia y reconocimiento de créditos

http://gestor.unir.net/userFiles/file/documentos/normativa/reconocimiento_tranferencia_creditos.pdf

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales No Universitarias	
MÍNIMO	**MÁXIMO**
0	**0**

Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	**9**

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	**9**

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1. Descripción general del plan de estudios

5.1.1. Distribución del Plan de estudios en créditos ECTS, por tipo de materia

El plan de estudios consta de 50 ECTS de carácter obligatorio y unas prácticas y un TFM de 4 y 6 ECTS respectivamente.

Materias	Créditos ECTS
Obligatorias	50
Prácticas Externas	4
Trabajo Fin de Máster	6
Créditos totales	**60**

5.1.2. Estructura del Plan de estudios.

El plan de estudios se estructura en un total de diez asignaturas cuya ordenación se corresponde con tres objetivos principales:

- Familiarizar al estudiante con los conceptos básicos en materia de protección de datos personales.
- Capacitar al estudiante para desarrollar proyectos de implementación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y de implantación de políticas de seguridad.
- Profundizar en la formación de modo que se garantice la capacidad de abordar el cumplimiento normativo en protección de datos en sectores específicos.

Las asignaturas del **primer cuatrimestre** se engloban en la materia Elementos Básicos de la Protección de Datos, que persigue los siguientes objetivos:

Objetivo 1. Familiarizar al estudiante con los conceptos básicos en materia de protección de datos personales.

Asignatura I. El derecho fundamental a la protección de datos.

A través de esta asignatura el estudiante adquiere las competencias básicas para entender la génesis del derecho fundamental a la protección de datos y los derechos relacionados con la privacidad y su plasmación en los Ordenamientos jurídicos regionales.

Asignatura II y III. Derechos del ciudadano y obligaciones del responsable (I). Derechos del ciudadano y obligaciones del responsable (II).

Estas dos asignaturas, que se corresponden con los aspectos básicos de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, capacitarán al estudiante para abordar los aspectos generales del cumplimiento normativo en esta materia.

Objetivo 2. Capacitar al estudiante para desarrollar proyectos de implementación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y de implantación de políticas de seguridad.

Asignatura IV. Protección de datos personales y gestión de las organizaciones.

Esta asignatura permite al estudiante conocer el funcionamiento y modelo de gestión de las organizaciones y, gracias a ello, le confiere flexibilidad para buscar soluciones funcionales e interactuar en equipos multidisciplinares.

Asignatura V. Las TIC y la seguridad.

Esta asignatura permitirá familiarizarse con aspectos tecnológicos esenciales para el desempeño de las funciones propias del data protection officer.

Asignatura VI. Los deberes de secreto y seguridad.

Esta asignatura cumple con un doble objetivo en función del perfil de origen del estudiante: a) ser capaz de identificar la regulación del deber de secreto en normas reglamentarias; b) ser capaz de concretar el significado y las implicaciones técnicas de los conceptos de seguridad y secreto.

Todas las asignaturas obligatorias del **segundo cuatrimestre**, se engloban en la materia de Ficheros Específicos.

Objetivo 1. Profundizar en la formación de modo que se garantice la capacidad de abordar el cumplimiento normativo en protección de datos en sectores específicos.

Asignatura VII. Gestión económica y empresarial y protección de datos personales.

Esta asignatura familiarizará al estudiante con todos los aspectos relevantes en materia de gestión de información personal que se proyectan sobre una empresa.

Asignatura VIII. Salud e investigación biomédica.

La importancia de la salud, el carácter de datos especialmente protegidos y la dimensión investigadora convierten este tipo de ficheros en un entorno particularmente complejo de gestionar. Por otra parte la evolución hacía modelos de e-Health obliga a un conocimiento profundo de la materia.

Asignatura IX. Ficheros públicos.

Este constituye el segundo gran bloque especializado en el ámbito de la aplicación de la normativa sobre protección de datos personales con una complejidad derivada del abanico de funciones con el que cumple la Administración, desde el más simple procedimiento, pasando por la provisión de servicios sociales y educación hasta la seguridad pública.

Asignatura X. El futuro de la protección de datos personales

Finalmente el curso ofrecerá una perspectiva que permita abordar al estudiante tanto los procesos de cambio normativo como la innovación tecnológica.

Prácticas Externas:

El aprendizaje del master se completa con un plan de prácticas externas cuyos objetivos esenciales son los siguientes.

1) Ofrecer una amplia gama de despachos e instituciones en todo el territorio nacional permitiendo el desarrollo de prácticas en el entorno geográfico del estudiante.

2) Seleccionar un conjunto de entidades, despachos profesionales o consultoras especializadas en la materia.

3) Integrar a los estudiantes en equipos de trabajo con una trayectoria consolida en materia de protección de datos.

4) Acompañar el segundo cuatrimestre, dedicado a la formación especializada en ficheros sectoriales con un entorno práctico donde el aprendizaje de la materia tenga un referente inmediato de orden práctico

Trabajo Fin de Máster.

El Trabajo Fin de Máster permitirá a los estudiantes desarrollar sus competencias tanto desde el punto de vista de la investigación dogmática como, si así lo prefieren aplicada, no perdiendo en ningún caso de vista la dimensión profesionalizadora del mismo.

La estructura de las enseñanzas, queda según el siguiente esquema:

MATERIA	ASIGNATURA	CARÁCTER	ECTS
Elementos Básicos de la Protección de Datos	El Derecho Fundamental a la Protección de Datos.	OB	4
	Derechos del Ciudadano y Obligaciones del Responsable (I).	OB	6
	Derechos del Ciudadano y Obligaciones del Responsable (II).	OB	6
	Protección de Datos Personales y Gestión de las Organizaciones.	OB	4
	Las TIC y la Seguridad.	OB	6
	Los Deberes de Secreto y Seguridad.	OB	6
Ficheros Específicos	Gestión Económica y Empresarial y Protección de Datos Personales.	OB	6
	Salud e Investigación Biomédica.	OB	4
	Ficheros Públicos.	OB	4

	El Futuro de la Protección de Datos Personales	OB	4
Prácticas Externas	Prácticas Externas	PE	4
TFM	Trabajo Fin de Máster	TFM	6
	TOTAL ECTS		60

5.1.3. Distribución temporal del Plan de estudios

El plan de estudios se estructura en un total de diez asignaturas cuya secuencia temporal se corresponde con los tres objetivos principales antes descritos:

- Familiarizar al estudiante con los conceptos básicos en materia de protección de datos personales.
- Capacitar al estudiante para desarrollar proyectos de implementación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y de implantación de políticas de seguridad.
- Profundizar en la formación de modo que se garantice la capacidad de abordar el cumplimiento normativo en protección de datos en sectores específicos.

Para ello la estructura organizativa del curso dedica el primer semestre a la satisfacción de los dos primeros objetivos. Una vez superado este semestre, que abarca las asignaturas I a la VI el estudiante iniciará el segundo cuatrimestre donde ese abordará el estudio sectorial de ficheros específicos y también desarrollará un programa de prácticas formativas externas que le permite desplegar el conocimiento adquirido en entornos de asesoramiento dedicado a la protección de datos personales.

PRIMER CUATRIMESTRE		**SEGUNDO CUATRIMESTRE**	
Asignaturas	**ECTS**	**Asignaturas**	**ECTS**
El Derecho Fundamental a la Protección de Datos	4	Gestión Económica y Empresarial y Protección de Datos Personales.	6
Derechos del Ciudadano y Obligaciones del Responsable (I)	6	Salud e Investigación Biomédica.	4
Derechos del Ciudadano y Obligaciones del Responsable (II)	6	Ficheros Públicos	4
Protección de Datos Personales y Gestión de las Organizaciones	4	El Futuro de la Protección de Datos Personales	4
Las TIC y la Seguridad	6	Prácticas Externas	4
Los Deberes de Secreto y Seguridad.	6	TFM	6
Total primer cuatrimestre	**32**	**Total segundo cuatrimestre**	**28**

5.1.4. Igualdad hombre y mujeres, fomento de la educación y cultura de la paz, no discriminación

El plan de estudios que se presenta, cumple con la legalidad vigente y el compromiso de enseñar a los estudiantes a ser respetuosos con el ordenamiento jurídico siguiendo las directrices que marcan las siguientes leyes:

Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. BOE núm. 71, Viernes 23 marzo 2007.

Ley 27/2005, de 30 de noviembre, de fomento de la educación y la cultura de la paz. BOE núm. 287, Jueves 1 diciembre 2005.

Ley 51/2003, de 2 de diciembre de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. BOE núm. 289, Miércoles 3 diciembre 2003.

5.1.5. Procedimiento de coordinación académico-docente

Cada módulo cuenta con un plan docente que da unidad a la agrupación de asignaturas, las cuales, al mismo tiempo, tienen sus respectivos programas.

El director del Máster asume la responsabilidad de la ordenación académica de todos los módulos. Cada módulo está coordinado por un profesor que se responsabiliza de la adecuada aplicación del plan docente y de la relación con los otros módulos del curso.

El director del Máster, tiene reuniones presenciales periódicas con los coordinadores de materias y con el conjunto del profesorado, con la finalidad de asegurar la coherencia entre los distintos planes docentes y el cumplimiento de los objetivos del Máster.

Además de las reuniones, el director de Máster contará al menos con los siguientes mecanismos de coordinación docente:

1. Cada profesor entregará para su revisión copias de la Guía Docente de la asignatura al profesor coordinador de módulo quien comprobará la conformidad en cada caso con el contenido de la presente memoria y la compatibilidad y posibles sinergias con otras asignaturas del mismo módulo o curso.
2. El director de Máster estudiará los correspondientes informes y en su caso las guías que sea necesario y autorizará si procede la publicación de cada guía.
3. El director del Máster confeccionará la agenda del proceso, la presentará para su aprobación al Vicerrector de Calidad, y velará especialmente por el cumplimiento de los plazos aprobados.
4. La estrecha colaboración con la Comisión de Garantía de Calidad del Título.

5.2. Metodología de la Universidad Internacional de La Rioja

La Universidad Internacional de La Rioja basa su enfoque pedagógico en los siguientes puntos:

- Participación de los alumnos y trabajo colaborativo que favorece la creación de redes sociales y la construcción del conocimiento. Las posibilidades técnicas que ofrece el campus virtual permiten crear entornos de aprendizaje participativos (con el uso de foros, chats, correo web, etc.) y facilitar y fomentar la creación colaborativa de contenidos (blogs, videoblogs, etc.).

- A partir de aquí, los procedimientos y estrategias cognitivas llevan al alumno, mediante su actividad directa y personal, a la construcción del propio conocimiento y elaboración de significados. Los docentes son mediadores en el proceso. Además de programar y organizar el proceso, el docente anima la dinámica y la interacción del grupo, facilita recursos. Se destaca el aprendizaje significativo, la colaboración para el logro de objetivos, la flexibilidad, etc.

- Organización de los contenidos y variedad de recursos de aprendizaje.

Los puntos clave de nuestra metodología son:

- Formular los objetivos de aprendizaje.
- Facilitar la adquisición de las competencias básicas para el ejercicio de la profesión.
- Elaborar los contenidos que el profesor desea transmitir.
- Organizar los contenidos divididos en básicos, específicos y complementarios.
- Elaborar las herramientas de evaluación necesarias que garanticen el aprovechamiento de su formación.
- Evaluación continua de las respuestas de los alumnos
- Control del ritmo de progreso de los alumnos.
- Crear aportaciones para que los alumnos se enfrenten a situaciones que entren en contraste con sus experiencias anteriores.
- Sugerir actividades que les ayuden a reestructurar su conocimiento.
- Proponer actividades de resolución de problemas.
- Fomentar actividades que requieran interacción y colaboración con otros alumnos.
- Crear contextos “reales”. El formador puede diseñar simulaciones de la realidad que ayuden al alumno a comprender la validez de lo que aprende para resolver problemas concretos y reales.
- Utilizar casos prácticos que muestren al alumno experiencias reales.
- Aprovechar las posibilidades del hipertexto para permitir a los alumnos que construyan sus propios caminos de aprendizaje (un camino adecuado a su estilo de aprendizaje).

5.2.1. Aula virtual

5.2.1.1 Descripción general del aula virtual

El aula virtual es un espacio donde los alumnos tienen acceso a la totalidad del material didáctico asociado a la asignatura (unidades didácticas, documentación de interés complementaria, diccionario digital de términos asociados a las asignaturas del programa de formación, etc.).

Este recurso se encuentra en el campus virtual, una plataforma de formación donde además del aula, el alumno encuentra otra información de interés. Se hace a continuación una descripción general sobre las diferentes secciones de campus virtual con una descripción más detallada del aula.

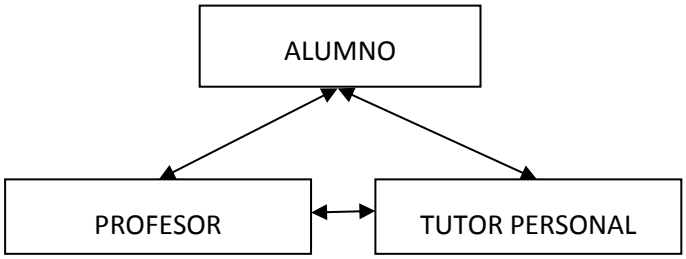
CAMPUS VIRTUAL	
AGENDA	Permite al estudiante consultar los principales eventos (exámenes, actividades culturales, clases presenciales). La agenda puede estar sincronizada con dispositivos móviles.
CLAUSTRO	En este apartado se encuentran los nombres de todo el personal docente de UNIR y el nivel de estudios que poseen.
NOTICIAS	Información común a todos los estudios que puede resultar interesante.
FAQ	Respuestas a preguntas frecuentes.
DESCARGAS	Apartado desde donde se pueden descargar exploradores, programas, formularios, normativa de la Universidad, etc.
LIBRERÍA/BIBLIOTECA	Acceso a libros y manuales para las diferentes asignaturas, existen también herramientas donde se pueden comprar o leer libros online.
EXÁMENES	Cuestionario a rellenar por el alumno para escoger sede de examen y una fecha de entre las que la Universidad le ofrece.
ENLACES DE INTERÉS	UNIR propone enlaces tales como blogs, voluntariado, actividades culturales destacadas, etc.
AULA VIRTUAL	El alumno tendrá activadas tantas aulas virtuales como asignaturas esté cursando. Contiene el material necesario para la impartición de la asignatura, que se organiza en las **SECCIONES que se describen a continuación:**

RECURSOS	**Temas:** Cada uno de los temas incluye varias secciones que serán básicas en el desarrollo de la adquisición de las competencias de la titulación: - **Ideas claves:** Material didáctico básico para la adquisición de competencias. - **Lo más recomendado:** lecturas complementarias, videos y enlaces de interés, etc. - **+ Información:** pueden ser textos del propio autor, opiniones de expertos sobre el tema, artículos, páginas web, Bibliografía, etc. - **Actividades:** diferentes tipos de ejercicios, actividades y casos prácticos. - **Test:** al final de cada uno de los temas se incluye un test de autoevaluación para controlar los resultados de aprendizaje de los alumnos.
	Programación semanal: Al comienzo de cada asignatura, el alumno conoce el reparto de trabajo de todas las semanas del curso. Tanto los temas que se imparten en cada semanas como los trabajos, eventos, lecturas. Esto le permite una mejor organización del trabajo.
	Documentación: A través de esta sección el profesor de la asignatura puede compartir documentos con los alumnos. Desde las presentaciones que emplean los profesores hasta publicaciones relacionadas con la asignatura, normativa que regule el campo a tratar, etc.
TV DIGITAL	**Presenciales virtuales:** permite la retransmisión en directo de clases a través de Internet, donde profesores y estudiantes pueden interactuar.
	Clases magistrales: En esta sección se pueden ver sesiones grabadas en la que los profesores dan una clase sobre un tema determinado sin la presencia del estudiante.
	UNIRTV: Desde esta sección, los alumnos pueden subir vídeos y ver los que hayan subido sus compañeros.
COMUNICACIONES	**Última hora:** Se trata de un tablón de anuncios dedicado a la publicación de noticias e información de última hora interesantes para los alumnos.
	Correo: Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente.

	Foros: Este es el lugar donde profesores y alumnos debaten y tratan sobre los temas planteados.
	Chat: Espacio que permite a los distintos usuarios comunicarse de manera instantánea.
ACTIVIDADES	**Envío de actividades:** Para realizar el envío de una actividad hay que acceder a la sección *Envío de actividades*. En este apartado el alumno ve las actividades que el profesor ha programado y la fecha límite de entrega. Dentro de cada actividad, el alumno descarga el archivo con el enunciado de la tarea para realizarla. Una vez completado, el alumno adjunta el documento de la actividad. En caso de necesitar enviarla de nuevo, solo hace falta repetir el proceso. La plataforma, automáticamente, sustituirá el archivo anterior por el nuevo. Una vez completado el proceso, solo queda conocer el resultado. Para ello hay que ir a *Resultado de actividades.*
	Resultado de actividades: El alumno puede consultar los datos relacionados con su evaluación de la asignatura hasta el momento: calificación de las actividades y suma de las puntuaciones obtenidas hasta el momento, comentarios del profesor y del tutor personal, etc. y descargarse las correcciones.

5.2.1.2 Comunicación a través del aula virtual

El aula virtual dispone de sistemas de comunicación tanto síncrona como asíncrona que facilitan la interacción en tiempo real o diferido para sus usuarios: profesor, estudiante y tutor personal:



La comunicación entre los usuarios es un elemento fundamental que permite al alumnado la adquisición de competencias y resultados de aprendizaje de las diferentes materias y se realiza a través de las siguientes herramientas del aula virtual:

HERRAMIENTA	UTILIDAD
CLASES PRESENCIALES VIRTUALES	Permite a los alumnos ver y escuchar al docente a la vez que pueden interactuar con él y el resto de alumnos mediante chat y/o audio. El profesor dispone de una pizarra electrónica que los alumnos visualizan en tiempo real. También se permite al alumno **acceder a las grabaciones** de las sesiones presenciales virtuales de las asignaturas, de manera que puede ver la clase en diferido.
FORO	Son los profesores quiénes inician los foros. Existen diferentes tipos: - Foro *"Consúltale al profesor de la asignatura":* trata los aspectos generales de la asignatura. Los profesores y tutores personales lo consultan a diario. - Foros programados: tratan sobre un tema específico y son puntuables. Los profesores actuarán de moderadores, marcando las pautas de la discusión. - Foros no programados: se trata de foros no puntuables cuyo objetivo es centrar un aspecto de la asignatura que considere importante el profesor. En la programación semanal de la asignatura se especifica la fecha de inicio y fin de los foros, el tema sobre el que se va a debatir y la puntación máxima que se puede obtener por participar. Las intervenciones se pueden filtrar por título, leídas/no leídas, participante, ponente y fecha y pueden descargar los foros en formato EXCEL para guardarlos en su ordenador.
CORREO ELECTRÓNICO	A través del correo electrónico el estudiante se pone en contacto con el tutor personal, quien contesta todas las consultas de índole técnico o deriva el correo al profesor si se trata de una cuestión académica.
CHAT	Permite una comunicación instantánea entre los usuarios conectados ya sea de manera colectiva o privada. Fomenta el debate y consultas entre estudiantes. Además, a través de esta herramienta el profesor realiza tutorías en grupos reducidos u otras actividades.
ÚLTIMA HORA	Desde este medio el tutor personal pone en conocimiento del alumnado eventos de interés como pueden ser: foros, sesiones, documentación, festividades etc.

Además de las herramientas del aula virtual, también existe comunicación vía telefónica. Asiduamente el tutor personal se pone en contacto con los estudiantes y si es necesario y/o el estudiante lo solicita el profesor llamará al estudiante para resolverle cualquier cuestión.

Toda esta información se resume de manera esquemática en la tabla que a continuación se presenta:

Herramientas / **Usuarios**	Clase	Foro	Correo	Chat	Última hora	Vía telefónica
Profesor-tutor personal			**X**			**X**
Profesor-estudiante	**X**	**X**		**X**		**X**
Tutor personal -estudiante		**X**	**X**	**X**	**X**	**X**

5.2.1.3 Sesiones presenciales virtuales

En este apartado se explica, con mayor detalle el funcionamiento de las sesiones presenciales virtuales, que se considera el elemento pionero y diferenciador de esta Universidad. El aula virtual, permite a través de la televisión digital, crear un espacio donde profesor y estudiantes pueden interactuar del mismo modo que lo harían en un aula física. Además, el uso de chat en las sesiones virtuales fomenta la participación de los estudiantes.

Las características de estas aulas es que permiten realizar las siguientes acciones:

- El alumno ve y escucha al profesor a tiempo real.
- El alumno puede participar en cualquier momento a través de un chat integrado en la sesión virtual.
- Si para la adquisición de competencias lo requiere, el aula ofrece una gran variedad de posibilidades, entre las más utilizadas están:
    - Intervención de los estudiantes a través de audio y video, ya sea de manera grupal o individual.
    - Realización de talleres de informática.
    - Construcción de laboratorios virtuales.

5.3. Actividades formativas

La distribución de las actividades formativas responde a un criterio de dedicación del alumno a cada una de las actividades que le permitirán adquirir satisfactoriamente las competencias asignadas a cada una de las asignaturas del máster. Con ayuda del aula virtual, se programan las siguientes actividades formativas:

Sesiones presenciales virtuales: clases presenciales impartidas por profesores expertos a través de la ITPV. Todas las clases son en directo y, además, éstas pueden verse en diferido.

Estudio personal de material básico: permite al estudiante integrar los conocimientos necesarios para superar satisfactoriamente la asignatura.

Lectura y análisis de material complementario: entran en este apartado elementos auxiliares del estudio, como la documentación complementaria, la legislación, artículos y enlaces de interés, ejemplos de expertos, vídeos, etc., que permiten a los estudiantes ahondar en la información y estudio de la materia, y les facilitan el logro de los objetivos de aprendizaje propuestos en cada asignatura.

Casos prácticos: en cada una de las asignaturas, se programan varios casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.

Test de autoevaluación y prueba final: por cada unidad didáctica se propone un test de autoevaluación. Su finalidad es analizar el grado de conocimiento del tema expuesto. El sistema proporciona al estudiante la respuesta correcta de forma inmediata; esto le permite dirigirse –también inmediatamente– al lugar concreto de la unidad, para revisar los conocimientos. Al final de la asignatura realiza un examen presencial.

Tutorías: durante el desarrollo de la asignatura, el estudiante tiene la posibilidad de solicitar tutorías al profesor por vía telemática. En caso de ser necesario también se utiliza la vía telefónica.

Foros y debates (trabajo colaborativo): el profesor de la asignatura plantea temas para que junto con los alumnos, se debata, se aporten experiencias, compartan e inicien discusiones constructivas.

5.4. Sistemas de evaluación

Las asignaturas se evaluarán a través de una prueba final presencial y de la evaluación continua.

- **El examen final presencial** representa el 60% de la nota
  La naturaleza virtual de las enseñanzas de UNIR, hace necesaria la realización de una prueba presencial (certificada mediante ante documentación fehaciente de identidad) que supone un 60% de la evaluación final. Esta tiene un carácter básico y solo cuando se supera la nota establecida para el aprobado, puede completarse la calificación con los procedimientos específicos de evaluación continua que establezca cada materia.

- **La evaluación continua** representa el 40% de la nota y contempla los siguientes criterios:
    - **Participación del estudiante:** se evalúa teniendo en cuenta la participación en las sesiones presenciales virtuales, en foros colaborativos y tutorías (5%).
    - **Trabajos, proyectos y casos:** en este criterio se valoran las actividades que el estudiante envía a través del aula virtual, tales como trabajos, proyectos o casos prácticos (30%).
    - **Test de autoevaluación:** al final de cada tema, los estudiantes pueden realizar este tipo de test, que permite al profesor valorar el interés del estudiante en la asignatura (5%).

Trabajo Fin de Máster

El Trabajo Fin de Máster será objeto de seguimiento continuo por parte del director del Trabajo Fin de Máster, que será el que finalmente le otorgue el visto bueno final. La evaluación final le corresponderá a una comisión integrada por tres profesores del área de conocimiento. La comisión valorará no sólo el proyecto, sino también la defensa oral del mismo. Se evaluará del siguiente modo:

- **Estructura:** Atender a la estructura y organización del Trabajo Fin de Máster: 20%
- **Exposición:** Valorar la claridad en la exposición, así como la redacción y la capacidad de síntesis, análisis y respuesta: 30%
- **Contenido:** Se tomará como referencia la memoria del Trabajo y todo el resto de la documentación técnica de apoyo para comprobar la validez de la exposición. Se valorará la capacidad de síntesis y su fácil lectura. También se valorará la corrección y claridad de la expresión, tanto escrita como gráfica: 50%

Prácticas Externas

Se llevará a cabo una evaluación continua durante la realización de las mismas tanto por un tutor asignado por la empresa como por el profesor de la asignatura. La nota final se obtendrá en base al siguiente criterio:

- **Evaluación del tutor externo**: 40%
- **Memoria de prácticas,** tutorizada y corregida por un profesor de la universidad: 60%

5.5. Sistema de calificaciones

El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el artículo 5 del Real Decreto 1125/2003 de 5 de Septiembre (BOE 18 de Septiembre), por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional.

- 0 - 4,9 Suspenso (SS)
- 5.0 - 6,9 Aprobado (AP)
- 7,0 - 8,9 Notable (NT)

- 9,0 - 10 Sobresaliente (SB)

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

5.6. Descripción detallada de los módulos

Elementos Básicos de la Protección de Datos	
Créditos ECTS:	32
Carácter	Obligatorio.
Unidad temporal:	6 cuatrimestrales en el primero cuatrimestre.

REQUISITOS PREVIOS
No se han establecido.

DESCRIPCIÓN DE LAS ASIGNATURAS			
Denominación de la asignatura	**Cuatrimestre**	**Créditos ECTS**	**Carácter**
Asignatura I. El Derecho Fundamental a la Protección de Datos.	Primero	4	Obligatorio
Asignatura II. Derechos del Ciudadano y Obligaciones del Responsable (I).	Primero	6	Obligatorio
Asignatura III. Derechos del Ciudadano y Obligaciones del Responsable (II).	Primero	6	Obligatorio
Asignatura IV. Protección de Datos Personales y Gestión de las Organizaciones.	Primero	4	Obligatorio
Asignatura V. Las TIC y la Seguridad.	Primero	6	Obligatorio
Asignatura VI. Los Deberes de Secreto y Seguridad.	Primero	6	Obligatorio

SISTEMA DE EVALUACIÓN	PONDERACIÓN MIN	PONDERACIÓN MAX
Participación del estudiante	5%	25%
Trabajos, proyectos y casos	10%	30%
Test de autoevaluación	5%	25%
Examen final presencial	60%	60%

ACTIVIDADES FORMATIVAS	HORAS	% PRESENCIAL
Sesiones Presenciales Virtuales	140	0%
Estudio Personal de material básico	260	0%
Lectura y análisis de material complementario	150	0%
Casos Prácticos	210	0%
Test de autoevaluación y prueba final	70	20%
Tutorías	40	0%
Foros y debates (trabajo colaborativo)	90	0%
Total	**960**	

COMPETENCIAS		
Generales	**Específicas**	**Transversales**
CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10	**CE1, CE2, CE3, CE4, CE5, CE6, CE7, CE8, CE9, CE10, CE11, CE12, CE13, CE14, CE15, CE16, CE17, CE18, CE19, CE20, CE21, CE22, CE23**	**CT1, CT2, CT3, CT4**

CONTENIDOS DE LAS ASIGNATURAS

El Derecho Fundamental a la Protección de Datos.

1. Origen y evolución del derecho fundamental a la protección de datos: del right to privacy al web 2.0. 1.1 El derecho a la privacidad en el derecho norteamericano. Su influencia en el contexto Asia-Pacífico 1.2 El modelo europeo: la privacidad un derecho fundamental. El sistema del Consejo de Europa. El modelo de la Unión Europea. 1.3 Latinoamérica ¿Habeas Data, privacy o protección de datos personales? 1.4. Los principios de privacidad de la OCDE.

2. La tutela del derecho fundamental a la protección de datos. 2.1. Las autoridades administrativas independientes. 2.2 La Agencia Española de Protección de Datos. 2.3 La Autoridad Catalana de Protección de Datos. 2.4 La Agencia Vasca de Protección de datos. 2.5 La tutela judicial.

3. Protección de datos personales y ejercicio profesional. 3.1 El delegado de protección de datos. Chief Privacy Officer. 3.2. Chief Securiy Information Officer.

Derechos del Ciudadano y Obligaciones del Responsable (I).

1. Introducción. La dimensión prestacional del derecho fundamental a la protección de datos: derechos del ciudadano v. obligaciones del responsable. 1.1 El ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 1.2 Exclusiones al régimen general.

2. Conceptos básicos: dato personal, fichero, tratamiento. La disociaciación. El sistema de información como elemento determinante para el cumplimiento normativo. 2.1 La creación de ficheros públicos. 2.2 El deber de inscripción y la publicidad registral.

3. El flujo de la información como elemento determinante para la implementación de procesos de cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo. 3.1 El deber de información en la recogida de datos personales. 3.2 El consentimiento. 3.2.1 Principios definitorios. Las clases de consentimiento. 3.2.2 El régimen jurídico de los datos especialmente protegidos. 3.2.3 El consentimiento de los menores. 3.3 El principio de calidad de los datos. 3.3.1 La proporcionalidad, adecuación y pertinencia del tratamiento. 3.3.2 El principio de veracidad. 3.3.3 El principio de finalidad. 3.3.4 cancelación, bloqueo y conservación de los datos. 3.3.5 El uso de datos con fines históricos, científicos o estadísticos.

4. Los derechos de acceso, rectificación, cancelación y oposición al tratamiento: principios comunes y requisitos. 4.1 El derecho de acceso. 4.2 El derecho de rectificación. 4.3 El derecho de cancelación. 4.4 El derecho de oposición.

5. La garantía del derecho fundamental a la protección de datos. 5.1 El garante del derecho fundamental a la protección de datos: autoridades de protección de datos personales. 5.1.1 procedimientos de tutela. 5.1.2 La denuncia. 5.2 La tutela jurisdiccional.

Derechos del Ciudadano y Obligaciones del Responsable (II)

1. Las comunicaciones de datos personales. 1.1 Principios rectores: consentimiento, proporcionalidad y finalidad. 1.2 Cesiones de datos sin consentimiento. 1.3 los deberes del cedente y del cesionario.

2. Las prestaciones de servicios: outsourcing y protección de datos. 2.1 La relación responsable-encargado. 2.2 Deberes de diligencia del encargado. 2.3 El contrato de acceso a los datos por cuenta de terceros. Contenido necesario y obligaciones de las partes. 2.4 La subcontratación.

3. Las transferencias internacionales de datos personales. 3.1 Régimen general. 3.2 consideración de las excepciones al régimen general. 3.3 Las transferencias a países seguros. 3.3.1 concepto de país seguro y procedimiento de declaración por la Comisión Europea. 3.3.2 El caso de Safe harbour. Prestadores norteamericanos y Principios de Puerto Seguro. 3.4 Transferencias sujetas a autorización de la Agencia Española de Protección de Datos. 3.4.1 Las Cláusulas Contractuales tipo de la Comisión. 3.4.2 Binding

Corporate Rules. 3.4.3 Las transferencias encargado-encargado. 3.4.5 Procedimiento de autorización.

4. El régimen de infracciones y sanciones a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. El procedimiento sancionador.

Protección de Datos Personales y Gestión de las Organizaciones.

1. Conceptos básicos sobre organización empresarial. 1.1 El Gobierno corporativo. 1.2 El valor de los sistemas de información en la estrategia empresarial. 1.3 Negocio, comunicación comercial y tecnologías de la información. 1.4 Habilidades directivas y trabajo en equipos multidisciplinares (negocio-TI-marketing).

2. Gobierno de las tecnologías de la información. 2.1. Modelos de gestión del Gobierno TI. 2.2 Tecnologías de la información y estrategia de negocio. 2.3 Compliance y marco regulador de las TI. 2.4 Privacy by design y/o by default.

3. La implementación de proyectos de cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. 3.1 La identificación de ficheros y flujos de información: entrevista de auditoría. 3.2. El despliegue de los principios jurídicos aplicables a la auditoria LOPD. Determinación de la viabilidad de los tratamientos. Calidad delos datos. Principios de uso, conservación y destrucción de la información. 3.4 Análisis de impacto de los tratamientos. (PIA-Privacy Impact Assessment). 3.5 El informe de auditoría. La documentación de los tratamientos. 3.6 La ejecución del proyecto de implantación.

Las TIC y la Seguridad.

1. Conceptos básicos de Informática. 1.1 Elementos de hardware y soportes capaces de almacenar información. 1.2 Principios básicos de las redes de comunicaciones.1.3 Elementos de software: aplicaciones, redes y sistemas operativos. 1.4 Principios básicos del desarrollo de software. 1.5 Nuevos horizontes tecnológicos: cloud computing, smartphones, RFID, domótica, Internet de las Cosas.

2. Tecnologia de bases de datos. 2.1 Concepto de Sistema de Gestion de Bases de Datos. 2.2. Modelos de datos 2.3 Los SGBD relacionales y el lenguaje SQL 2.4 Diseño de bases de datos 2.5 Los almacenes de datos, datawarehouses 2.6 Big data 2.7 Mineria de datos e inteligencia del negocio 2.8 otros tipos de bases de datos: no sql, documentales, etc.

3. Seguridad TIC. 3.1 La seguridad en la tecnología: seguridad en sistemas operativos, bases de datos, redes. Desarrollo de software seguro. 3.2 Metodologías de análisis y gestión de riesgos. 3.3 Modelos de gestión de la seguridad. 2.4 estándares Normas ISO-IEC. La familia de las normas 27000. 2.5 Certificaciones y recursos profesionales.

4. Gestión y ejecución de proyectos en materia de seguridad. 4.1 Roles y perfiles funcionales en materia de seguridad: a) Comité de seguridad; b) CISO-Responsable de

seguridad; c) Administradores; d) Usuarios. 4.2 El rol de la seguridad en el gobierno y gestión de las organizaciones.

5. El valor de la seguridad en las organizaciones. 5.1 Los objetivos de la seguridad: confidencialidad, integridad, disponibilidad y trazabilidad. 5.2 Tipo de medidas: a) medidas organizativas; b) medidas técnicas.

Los Deberes de Secreto y Seguridad.

1. La naturaleza del deber de secreto y seguridad como garantía del derecho fundamental a la protección de datos. 1.1 El valor de la seguridad en las organizaciones. 1.2 Los objetivos de la seguridad: confidencialidad, integridad, disponibilidad y trazabilidad. 1.3) Tipo de medidas: a) medidas organizativas; b) medidas técnicas. 1.3 Niveles de seguridad en el Real Decreto 1720/2007. 1.4 El documento de seguridad. 1.5 Medidas de seguridad y políticas de cumplimiento. 1.6 La seguridad de las administraciones en el Esquema Nacional de Seguridad. 2.6 Otros conceptos relevantes para la seguridad: el Cloud Computing.

2. Gestión y ejecución de proyectos en materia de seguridad. 2.1 Gestión de la seguridad. 2.2 Roles y perfiles funcionales en materia de seguridad: a) Comité de seguridad; b) CISO-Responsable de seguridad; c) Administradores; d) Usuarios. 2.3 El rol de la seguridad en el gobierno y gestión de las organizaciones. 2.4. La auditoría de seguridad.

RESULTADOS DE APRENDIZAJE

El Derecho Fundamental a la Protección de Datos.

Al finalizar la asignatura el estudiante será capaz de entender el significado jurídico y constitucional del concepto de privacidad. Aprenderá a insertar el derecho fundamental a la protección de datos en el contexto regional Europeo y a diferenciar los regímenes jurídicos existentes en otros ámbitos regionales (América-APEC). Podrá ser capaz de comprender y aplicar los distintos mecanismos de tutela de estos derechos. Finalmente podrá definir su rol funcional en las organizaciones con las que trabaje.

Derechos de los Titulares de Datos (I).

Al finalizar la asignatura el estudiante será capaz de identificar ficheros y tratamientos sujetos a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establecer su legalidad y definir las condiciones básicas para la obtención y el uso de información personal.

Derechos de los Titulares de Datos (II).

Al finalizar la asignatura el estudiante será capaz de: a) implementar sistemas de cumplimiento normativo idóneos para la garantía de los derechos del titular de los datos; b) redactar políticas de privacidad; c) gestionar jurídicamente los flujos de datos personales que

salgan de su organización ya sea en virtud de cesiones o transferencias internacionales de datos personales o en virtud de tratamientos o por cuenta de terceros; d) redactar un contrato del artículo 12 LOPD; e) negociar acuerdos de nivel de servicio SLA's; f) tramitar transferencias internacionales de datos; g) redactar binding corporate rules; h) tramitar un procedimiento sancionador; h) redactar o tramitar un código tipo.

Protección de Datos Personales y Gestión de las Organizaciones.
Al finalizar la asignatura el estudiante será capaz de: a) trabajar en entornos de negocio integrándose en equipos multidisciplinares; b) entender los procesos de negocio y los procesos de gestión ofreciendo soluciones funcionales a las necesidades de la organización; c) realizar auditorías sobre cumplimiento normativo; d) integrar el concepto de privacy by design en la metodología de la organización; e) aplicar en la práctica los principios básicos de la LOPD.

Las TIC y la Seguridad.
Al finalizar la asignatura el estudiante será capaz de adquirir conocimientos informáticos básicos que le permitan interactuar con expertos en tecnologías de la información y tomar decisiones conjuntas en materia relacionadas con la gestión y el Gobierno TI y la seguridad.

Los Deberes de Secreto y Seguridad.
Al finalizar la asignatura el estudiante será capaz de: a) evaluar los requerimientos de seguridad de la organización; b) afrontar un plan de seguridad; c) documentar la seguridad; e) abordar los requerimientos de seguridad en contextos particulares como el Cloud Computing; f) aplicar los requerimientos de seguridad adicionales exigidos en el ámbito de la Administración Pública; g) manejar los principios rectores de una auditoría de seguridad.

Ficheros específicos	
Créditos ECTS:	18
Carácter	Obligatorio
Unidad temporal:	4 cuatrimestrales a realizar en el segundo cuatrimestre.

REQUISITOS PREVIOS
No se han establecido requisitos previos de acceso a este módulo.

DESCRIPCIÓN DE LAS ASIGNATURAS			
Denominación de la asignatura	**Cuatrimestre**	**Créditos ECTS**	**Carácter**
Asignatura VII. Gestión Económica y Empresarial y Protección de Datos Personales.	2	6	Obligatoria
Asignatura VIII. Salud e Investigación Biomédica.	2	4	Obligatoria
Asignatura IX. Ficheros Públicos.	2	4	Obligatoria
Asignatura X. El Futuro de la Protección de Datos Personales	2	4	Obligatoria

SISTEMA DE EVALUACIÓN	PONDERACIÓN MIN	PONDERACIÓN MAX
Participación del estudiante	5%	25%
Trabajos, proyectos y casos	10%	30%
Test de autoevaluación	5%	25%
Examen final presencial	60%	60%

ACTIVIDADES FORMATIVAS	HORAS	% PRESENCIAL
Sesiones Presenciales Virtuales	70	0%
Estudio Personal de material básico	180	0%
Lectura y análisis de material complementario	100	0%
Casos Prácticos	140	0%
Test de autoevaluación y prueba final	40	20%
Tutorías	30	0%
Foros y debates (trabajo colaborativo)	40	0%
Total	**600**	

COMPETENCIAS		
Generales	**Específicas**	**Transversales**
CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10	**CE1, CE2, CE5, CE6, CE7, CE8, CE9, CE10, CE11, CE12, CE13,CE14, CE16, CE17, CE19, CE20, CE21,CE22**	**CT1,CT2, CT3, CT4**

CONTENIDOS DE LAS ASIGNATURAS

Gestión Económica y Empresarial y Protección de Datos Personales.

1. Los ficheros de solvencia patrimonial y crédito. 1.2 Contrato, información previa y condiciones de legitimación para el tratamiento. 1.3 Responsable del fichero y del tratamiento: las relaciones con el fichero común. 1.4 Especialidades en el ejercicio y atención de los derechos de acceso rectificación y cancelación.

2. La protección de datos personales en el ámbito actuarial: el seguro. 2.1 Posición jurídica de las corredurías de seguros. 2.2 Evaluación de riesgos y seguros de vida. 2.3 Seguros vinculados al contrato de hipoteca.

3. El tratamiento de información financiera. 3.1 La legislación sobre blanqueo de capitales. 3.2 Custodia de información, seguridad y secreto en los ficheros relacionados con el blanqueo de capitales. 3.3 Las excepciones a los derechos de acceso, rectificación, cancelación y oposición al tratamiento. 3.4 El control del flujo internacional de capitales: Swift.

4. Ficheros de marketing y prospección comercial. 4.1 Roles en publicidad anunciante, editor y empresa publicitaria. 4.2 Condiciones para el desarrollo de la actividad publicitaria. 4.3 Especialidades en el ejercicio y atención de los derechos de acceso rectificación y cancelación. 4.4 Publicidad por medios electrónicos. Las relaciones LSSI-LOPD. Mensajería electrónica, análisis comportamental y cookies.

5. La gestión de las relaciones laborales. 5.1 El contrato de trabajo y el tratamiento de datos personales. 5.2 Las obligaciones del trabajador en materia de protección de datos personales. 5.3 Controles empresariales: videovigilancia y telecomunicaciones (internet, correo-e). 5.4 Prevención de riesgos laborales. 5.5. Los ficheros de "Whistleblowing". 5.6 Nuevos escenarios. El uso de dispositivos móviles con fines laborales y privados (BYOD-By Your Own Device). La geolocalización. 5.7 Protección de datos personales y libertad sindical.

6. Servicios de seguridad privada. 6.1 Condiciones de legitimación para el tratamiento. 6.2 Ámbito físico de prestación de los servicios. 6.3 Control de acceso a edificios. 6.4 Videovigilancia y seguridad privada.

Salud e Investigación Biomédica.

1. Marco general. 1.1 Ley General de Sanidad. 1.2 Ley de cohesión y Calidad del Sistema Nacional de Salud. 1.3 Ley del medicamento.

2. Atención sanitaria y protección de datos personales. 2.1 La historia clínica. 2.2 Perfiles funcionales de los profesionales de la salud. 2.3 El consentimiento en el ámbito de la salud. 2.4 El acceso a la historia clínica. 2.5 E-Health. La historia clínica y la receta electrónicas. 2.6 La gestión privada de la salud. 2.6 Nuevos modelos de atención sanitaria: genética y datos personales. 2.7. Laboratorios de análisis clínicos. 2.8 Prevención de riesgos laborales: la salud del trabajador (remisión).

3. Investigación y salud. 3.1 Condiciones para la investigación respecto de datos contenidos en historias clínicas. 3.2 Investigación biomédica. El uso de datos genéticos. 3.3 Investigación farmacológica. El código tipo de Farmaindustria.

Ficheros Públicos

1. Los ficheros de titularidad pública. 1.1 El ejercicio de funciones y/o potestades públicas como legitimación para el tratamiento. 1.2 La creación de ficheros públicos. 1.3 Comunicaciones de datos personales entre administraciones públicas. 1.4 Corporaciones y fundaciones de Derecho Público.

2. Protección de datos y administración electrónica. 2.1 Principios aplicables. 2.2 Esquema Nacional de Seguridad. 2.3 Esquema nacional de Interoperabilidad.

3. Los ficheros de las Fuerzas y Cuerpos de Seguridad. 3.1 El régimen jurídico de la investigación policial. 3.2 Base de datos policial sobre identificadores obtenidos a partir de ADN. 3.3 La videovigilancia con fines de investigación policial. 3.4 Videovigilancia y seguridad vial.

4. El servicio público de educación. 4.1 Protección de datos personales y ordenación general del sistema educativo. El interés superior del menor. 4.2 Régimen jurídico del tratamiento de datos

personales en educación de la educación infantil a la secundaria. 4.3 La prestación del servicio público de educación superior. 4.4 Problemas específicos del sector educativo.

5. Servicios sociales y protección de datos personales. 4.2 Uso de datos especialmente protegidos: la violencia de género.

El Futuro de la Protección de Datos Personales

1. Las redes sociales. Naturaleza y régimen jurídico aplicable. 1.2 La protección de los menores en las redes sociales. 1.3 Garantía de los derechos individuales y derecho al olvido.

2. El tratamiento de datos personales en la nube. 2.1 Análisis de contratos y Service Level Agreements. 2.2 La seguridad en el Cloud Computing. 2.3 Régimen jurídico del encargado del tratamiento. Subcontratación. 2.4 Flujos internacionales de datos en el Cloud. 2.5 Riesgo regulatorio.

3. Nuevos horizontes para la protección de datos personales. 3.1 Las aplicaciones móviles y servicios de valor añadido en Smartphones y dispositivos portátiles. La geolocalización. 3.2 Domótica e internet de los objetos. 3.2 Big Data, gamificación y análisis comportamental. 3.3 Biometría. Reconocimiento facial. 3.4 Herramientas de análisis e implementación de desarrollos tecnológicos con respeto a la privacidad.

RESULTADOS DE APRENDIZAJE

Gestión Económica y Empresarial y Protección de Datos Personales.

Al finalizar la asignatura el estudiante será capaz de realizar proyectos de adaptación y cumplimiento de la LOPD en: a) gestión financiera, solvencia patrimonial y crédito; b) seguros; c) publicidad y márquetin; d) comercio electrónico; e) relaciones laborales; f) seguridad privada.

Salud e Investigación Biomédica.

Al finalizar la asignatura el estudiante será capaz de: a) conocer en profundidad la naturaleza de los ficheros de salud y los tratamientos de datos personales a ellos asociados; b) implementar medidas de cumplimiento normativo en entornos asociados a la prestación de servicios de salud; c) asistir en proyectos de investigación relacionados con la saludo, la genética o la biomedicina.

Ficheros Públicos

Al finalizar la asignatura el estudiante será capaz de: a) evaluar las condiciones de aplicación de la LOPD en una administración pública; b) garantizar el cumplimiento de la normativa sobre protección de datos personales en los proyectos de administración electrónica; c) implantar medidas de cumplimiento en materia de seguridad pública con adaptación de los principios de protección de datos a la legislación reguladora de la actividad de las Fuerzas y Cuerpos de Seguridad; d) implementar proyectos de cumplimiento de la LOPD en el ámbito de la educación; e) implementar proyectos de cumplimiento de la LOPD en el ámbito de los servicios sociales.

El Futuro de la Protección de Datos Personales

Al finalizar la asignatura el estudiante será capaz de conocer los nuevos entornos de avance de las tecnologías de la información y garantizar la adaptación de los objetivos de las organizaciones y el desarrollo de nuevos modelos de negocio a los principios vigentes en materia de privacidad.

Prácticas Externas	
Créditos ECTS:	4
Carácter	PE
Unidad temporal:	Una Cuatrimestral a realizar en el segundo cuatrimestre.

REQUISITOS PREVIOS
No se han establecido requisitos previos de acceso a este módulo.

DESCRIPCIÓN DE LAS ASIGNATURAS			
Denominación de la asignatura	**Cuatrimestre**	**Créditos ECTS**	**Carácter**
Prácticas Externas	2	4	PE

SISTEMA DE EVALUACIÓN	**PONDERACIÓN MIN**	**PONDERACIÓN MAX**
Memoria de Prácticas	60%	60%
Evaluación del Tutor Externo	40%	40%
ACTIVIDADES FORMATIVAS	**HORAS**	**% PRESENCIAL**
Sesiones Presenciales Virtuales	4	0%
Desarrollo de las Prácticas	100	100%
Lectura y análisis de Material complementario	6	0%

Tutorías	6	0%
Foros y Debates (trabajo colaborativo)	4	0%
Total	**120**	

COMPETENCIAS		
Generales	**Específicas**	**Transversales**
CG1, CG2, CG3, CG4, CG5	**CE1, CE2, CE5, CE6, CE7, CE8, CE9, CE10, CE11, CE12, CE13, CE14, CE15, CE16, CE17, CE19, CE20, CE21, CE22, CE23**	**CT3, CT4**

CONTENIDOS DE LAS ASIGNATURAS

La oferta de prácticas responderá a un proceso de elección competitiva atendiendo al rendimiento académico del primer cuatrimestre y a criterios complementarios de ubicación geográfica. Los estudiantes que se integren en las prácticas deberán dominar a la perfección los aspectos generales de la materia y habrán desarrollado mediante los ejercicios dl curso una primera labor de auditoría de protección de datos. El objetivo de esta metodología es permitir una inserción rápida en los procedimientos de cumplimiento normativo y en las labores en materia de protección de datos de la organización en la que se desarrolle el programa de prácticas.

Desde la dirección académica y la tutorización del curso se desarrollará un programa de seguimiento y monitorización del programa de prácticas.

RESULTADOS DE APRENDIZAJE

El objetivo de las Prácticas Externas es permitir una inserción rápida en los procedimientos de cumplimiento normativo y en las labores en materia de protección de datos de la organización en la que se desarrolle el programa de prácticas.

Trabajo Fin de Máster	
Créditos ECTS:	6
Carácter	TFM
Unidad temporal:	Una Cuatrimestral a realizar en el segundo cuatrimestre.

REQUISITOS PREVIOS
No se han establecido requisitos previos de acceso a este módulo.

DESCRIPCIÓN DE LAS ASIGNATURAS			
Denominación de la asignatura	**Cuatrimestre**	**Créditos ECTS**	**Carácter**
Trabajo Fin de Máster	2	6	TFM

SISTEMA DE EVALUACIÓN	PONDERACIÓN MIN	PONDERACIÓN MAX
Contenido del TFM	50%	50%
Exposición del TFM	30%	30%
Estructura del TFM	20%	20%

ACTIVIDADES FORMATIVAS	HORAS	% PRESENCIAL
Sesiones Presenciales Virtuales	4	0%
Realización del TFM	146	0%
Tutorías	15	0%
Preparación de la exposición y defensa del TFM	15	10%
Total	**180**	

COMPETENCIAS		
Generales	**Específicas**	**Transversales**
CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10	**CE1, CE6, CE7, CE8, CE18, CE19**	**CT1, CT2, CT3, CT4**

CONTENIDOS DE LAS ASIGNATURAS
El trabajo consistirá en la puesta en práctica de las competencias investigadoras unido a los conocimientos adquiridos durante el grado. El alumno deberá desarrollar un trabajo coherente, con una duración realista en cuanto a los objetivos que se pretendan. Se tratará de ofrecer un trabajo de innovación mediante la búsqueda de fuentes y aportación personal del alumno.

RESULTADOS DE APRENDIZAJE
Al finalizar la asignatura el estudiante será capaz de analizar y sintetizar información, desarrollar proyectos de protección de datos con autonomía aplicando correctamente la metodología adecuada, organizar, documentar y comunicar información.

6. PERSONAL ACADÉMICO

6.1. Personal académico disponible

UNIR cuenta con los recursos humanos necesarios para llevar a cabo el plan de estudios propuesto y cumplir así los requisitos definidos en el Anexo I del RD 1393/2007 en cuanto a personal académico disponible. Asimismo, en cuanto a descripción y funciones del profesorado, UNIR sigue lo establecido en el V Convenio colectivo nacional de Universidades Privadas (Resolución de 27 de diciembre de 2005).

- **Profesor/a Agregado/a:** Es el doctor que desarrolla actividades docentes e investigadoras, desarrolla estudios de su especialidad o interdisciplinares y colabora con el Profesor Director para la ejecución de las actividades que a éste encomiende el centro. Asimismo, se encarga de la dirección de tesis doctorales y puede dirigir o coordinar la enseñanza de una o varias asignaturas de los planes de estudios que correspondan a su departamento, a requerimiento del director de éste, cuando no exista Profesor Director encargado de esta tarea. Tiene a su cargo la tutoría de grupos de alumnos.

- **Profesor/a Adjunto/a:** Es el doctor que desarrolla actividades docentes e investigadoras, desarrolla estudios de su especialidad o interdisciplinares, se encarga de la dirección de tesis doctorales y puede coordinar la enseñanza de una o varias asignaturas de los planes de estudios que correspondan a su departamento cuando no exista Profesor Director o Profesor Agregado encargados de esta tarea. Tiene a su cargo la tutoría de grupos de alumnos.

- **Profesor/a Asociado/a:** Es el titulado universitario de grado superior que desarrolla actividades docentes y coordina a varios profesores que imparten la misma o distintas asignaturas de los planes de estudio que corresponden a su departamento. Pueden tener, además, a su cargo la tutoría de grupos de alumnos.

6.1.1. Previsión del profesorado

La ratio de alumnos por profesor no será superior a 50 y al menos el 50 por 100 del total del profesorado deberá estar en posesión del título de doctor.

Categoría	Total %	Doctores%	Horas %
Profesor Agregado	30	100	30
Profesor Adjunto	20	100	20
Profesor Asociado	50	0	50

El equipo docente es experto en los contenidos del Máster y está formado inicialmente por un conjunto de doctores acreditados y expertos en el desarrollo y aplicación de la normativa sobre protección de datos personales.

Titulación	Experiencia profesional y académica e investigadora	Acreditado	Dedicación	Materia en la que imparte
Doctor en Derecho Constitucional	Docente, con más de 10 años de experiencia universitaria e investigadora. Experiencia profesional como responsable de Protección de datos y en el desarrollo de distintos procesos de Twinning de la UE de asesoramiento para la creación y desarrollo de Agencias de Protección de Datos.	SI	25%	El Futuro de la Protección de Datos Personales TFM
Doctor en Derecho	Más de 10 años de experiencia docente e investigadora Línea de investigación: La protección de los Derechos Fundamentales en el proceso de integración europea.	SI	40%	El Derecho Fundamental a la Protección de Datos TFM
Doctor en Derecho	Más de 7 años de experiencia docente	SI	30%	Gestión Económica y Empresarial y

	Línea de investigación: Privacidad y Relaciones Laborales. Autor de monografías especializadas: El respeto a la esfera privada del trabajador. Un estudio sobre los límites del poder de control empresarial, La videovigilancia empresarial y la protección de datos personales Experiencia profesional como responsable de Protección de datos.			Protección de Datos Personales
Doctor en Informática	Más de 5 años de experiencia docente e investigadora. Experiencia profesional de más de 10 años en el ámbito empresarial y de auditoria de seguridad Poseedor de los certificados profesionales en materia de seguridad informática más prestigiosos.	SI	100%	Las TIC y la Seguridad. Los Deberes de Secreto y Seguridad. TFM

	Experto en auditoria y seguridad en protección de datos personales. Línea de investigación: seguridad, diseño y desarrollo de bases de datos. Miembro de RETISBD (Red temática española de investigación en el campo de la seguridad de las bases de datos)			
Doctor en Derecho	Más de 10 años de experiencia docente y online. Línea de Investigación: Protección de Datos y Administraciones Públicas Experiencia profesional en materia de protección de datos personales en el ámbito de la Administración Pública.	SI	15%	Ficheros Públicos.
Licenciado en Derecho	Experiencia profesional en el Área de Seguridad en la Red y Protección de menores.	NO	75%	Protección de Datos Personales y Gestión de las Organizaciones Prácticas Externas

	Más de 3 años de experiencia en docencia on-line Abogado del Ilustre Colegio de Abogados de Madrid (ICAM) y consultor certificado ISO 27001 por APPLUS. Perito Judicial Informático. Coordinador de la Sección de menores de la Asociación nacional de tasadores y peritos judiciales informáticos.			
Doctor en Derecho Constitucional	Docente, con más de 10 años de experiencia universitaria e investigadora. Línea de Investigación: el derecho fundamental a la protección de datos y las repercusiones de las tecnologías de la información y las comunicaciones en la vida privada. Coordinador de monografías colectivas sobre el reglamento de desarrollo de la LOPD, sobre redes sociales y	NO	30%	El Futuro de la protección de Datos de Personales TFM

	sobre Cloud Computing.			
Licenciado en Derecho. Máster en Derecho Sanitario	Más de 8 años de experiencia docente universitaria. Experiencia profesional como letrado de la Administración de la Seguridad Social	NO	30%	Salud e Investigación Biomédica.
Doctor en Derecho	Más de 10 años de experiencia docente universitaria. Línea de Investigación: Protección de Datos y Administración Electrónica Transparencia y Acceso a la Información. Experiencia en docencia on-line	SI	15%	Ficheros Públicos.
Doctor en Derecho Constitucional	Docente con más de 10 años de experiencia docente e investigadora Investigador principal en diversos I+D Autor de 7 libros, ha coordinado otros 8 libros, autor de 70 artículos científicos o	Si	100%	Derecho del Ciudadano y Obligaciones del Responsable I TFM

	capítulos de libro. 122 comunicaciones o ponencias en congresos y seminarios (33 publicadas), destacando la línea de investigación educación, Seguridad y Defensa, e-democracia, e-gobierno y derechos fundamentales y nuevas tecnologías.			
Licenciado en Derecho	Profesional de reconocido prestigio y con experiencia docente de más de diez años en másteres relacionados con el Derecho y las tecnologías de la información. Autor de múltiples artículos en revistas jurídicas especializadas y libros colectivos. Abogado, consultor de la Agencia Española de Protección de Datos.	No procede	30%	Derecho del Ciudadano y Obligaciones del Responsable II Prácticas Externas

Doctor en Derecho	Colaborador docente, con más de 10 años de experiencia universitaria e investigadora (La protección de Datos como Derecho Fundamental en la UE)	NO	30%	TFM
Doctor en Derecho Constitucional	Más de 10 años de experiencia universitaria docente e investigadora.	NO	25%	TFM
Doctor en Derecho Constitucional	Más de 10 años de experiencia universitaria docente e investigadora. Línea de Investigación: El Derecho Fundamental a la Protección de Datos en Europa	NO	20%	TFM
Licenciado en Derecho	Profesional de reconocido prestigio con desempeño en el área de asesoramiento de datos. Asesor consultor externo de la Agencia Española de Protección de Datos. Letrado Asesor en, empresa de consultoría	No procede	35%	Prácticas Externas

	empresarial, estrategia y auditoria en calidad e ISO 9000, 14000.			
Licenciado en Derecho	Abogado del Ilustre Colegio de Abogados de Madrid (ICAM), con más de 10 años de experiencia en el ejercicio profesional. Socio-Consultor en empresa de seguridad homologada y consultora especializada en LOPD y videovigilancia, evidencia de archivos en soporte digital y prueba forense	No procede	40%	Prácticas Externas
Licenciado en Derecho	Experiencia en docencia por medio de internet desde 2001 para varias universidades. Auditor de Seguridad Informática (ISO 17799) y en LOPD y LSSI (2002) Consultor y Docente Homologado por la EOI Escuela de Organización Industrial para asesoría legal tecnológica y gestión	No procede	40%	Prácticas Externas

	estratégica empresarial.			

6.2. Otros recursos humanos disponibles

Este personal conforma los departamentos transversales de la universidad, que prestan apoyo logístico, organizativo y administrativo al servicio de la actividad docente. En función de la experiencia y titulación, se vincula contractualmente a la universidad en las categorías que vienen definidas en el V Convenio de Universidades Privadas. La mayor parte del personal tiene una dedicación a tiempo completo.

En su mayoría es personal titulado, no docente, con una formación específica tal y como en la tabla a continuación, que relaciona el perfil de este personal con los diferentes departamentos y servicios de la Universidad.

Departamentos y Servicios	Apoyo a las Titulaciones	Perfil de PAS
Oficina de atención al alumno	Información sobre las diferentes titulaciones	6 Auxiliares administrativos con experiencia en el campo de la Formación.
Servicio Técnico de Orientación	Orientación a futuros alumnos	30 Licenciados superiores en diferentes titulaciones (Pedagogía, Psicología y Sociología).
Servicio de Admisiones	Acceso, admisión y matrícula	22 Auxiliares administrativos con experiencia en el campo de la Formación.
Servicio Técnico Informático	Mantenimiento, desarrollo e innovación del campus virtual	15 Titulados superiores (ingeniería, técnicos de informática y especialistas en e-learning); uno de ellos responsable del mantenimiento.
Servicio de Publicaciones, Recursos Docentes y Documentación	Diseño y desarrollo de los materiales y Recursos docentes para su aplicación on line	24 Titulados superiores, uno de ellos responsable del diseño y edición de los contenidos.

Comunicación y Expansión Académica	Plan de Comunicación y desarrollo de proyectos nacionales e internacionales.	12 Licenciados en diferentes áreas relacionadas. Marketing, ADE y Relaciones Públicas.
TV y Producción Audiovisual	Grabación, edición y producción de material didáctico audiovisual.	10 Licenciados en diferentes Titulaciones (Comunicación y Periodismo).

6.3. Mecanismos de selección del personal de UNIR

En la selección de personal, se respetará lo dispuesto en las siguientes leyes:

- LEY ORGÁNICA 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. BOE núm. 71 Viernes 23 marzo 2007.
- LEY 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. BOE núm. 289 Miércoles 3 diciembre 2003.

Los criterios de selección, fijados con carácter general son los siguientes:

- Conocimientos exigidos para el desarrollo de su categoría, atendiendo a los estudios de enseñanzas oficiales o complementarias que se acrediten por el candidato y la adecuación de su experiencia profesional a las tareas requeridas.
- Conocimientos de inglés, tanto a nivel hablado y escrito.
- Experiencia profesional acreditada en puestos con alto requerimiento en el manejo de las nuevas tecnologías, así como en tareas de apoyo docente.

7. RECURSOS MATERIALES Y SERVICIOS

7.1. Justificación de la adecuación de los medios materiales y servicios disponibles

En el desarrollo de la actividad propia de la universidad siempre se dispone de la infraestructura necesaria para desarrollar sus actividades de enseñanza, investigación, extensión y gestión.

La infraestructura fundamental para el desarrollo del título es el campus virtual, que se ha descrito en el criterio cinco desde un punto de vista académico, abarcando en este criterio los aspectos técnicos.

Además, para el desarrollo de las funciones de UNIR, se dispone de:

- Rectorado.
- Secretaría General.
- Recepción e información.
- Una biblioteca.
- Un salón de actos para 100 personas.
- Cinco salas de reuniones.
- Tres aulas de trabajo.
- Tres aulas polivalentes.
- Dos aulas totalmente informatizadas de 50 m^2 cada una, con la incorporación de 50 equipos informáticos de última generación.
- Dos salas de sistemas, para albergar los sistemas informáticos y tecnológicos.
- Siete salas de impartición de sesiones presenciales virtuales.
- Un aula-plató con los recursos necesarios para grabar las sesiones magistrales.

7.2. Instituciones colaboradoras para la realización de prácticas externas

Las prácticas del Máster pueden realizarse en despachos de abogados expertos en Protección de Datos, entidades o empresas que cuenten con responsable de protección de datos o consultoras de seguridad, entre otros.

El Departamento de Prácticas de UNIR es el encargado de contactar con cada una de estas entidades, y una vez confirmado que resultan adecuados y tras la firma del convenio, es el propio centro el que asigna al alumno el tutor de prácticas externo adecuado para estas prácticas, que podrá tratarse de abogados con experiencia en protección de datos, experto en seguridad o profesional certificado.

Desde la redacción de este máster se trabaja ya en la oferta de un completo programa de prácticas externas, que facilite la realización de prácticas en despachos de primer nivel en todo el territorio nacional. A continuación se adjunta la lista completa de instituciones con las que ya se ha establecido convenio, así como los nombres de las entidades con las que nos encontramos en tramitación en estos momentos. En total, contamos con más de 40 instituciones, que permitirán atender a nuestros estudiantes. Además, como puede apreciarse en la segunda tabla, seguimos trabajando para establecer nuevos convenios, incluso una vez se haya iniciado la impartición del máster.

INSTITUCIÓN COLABORADORA
Roca y Junyent Abogados (Barcelona)
Ecix Group. Hogan Lovells
Rousaud Costas Durán(Barcelona)
Bufete Abogado Amigo (Valencia)
Legistel (Santa Cruz de Tenerife)
Canosa Abogados sl (Barcelona)
EAD-Consultors (Lleida)
Fernandez de Vera Abogados (Cádiz)
Fidel Andrés Ortega.Abogados (Álava)
EQUIPO MARZO (Valencia)
INSTITUTO CIES(Asturias)
IURISTEC S.L (Córdoba)
Fórum Jurídico (Córdoba)
Diputación de Barcelona
Despacho Esther Botella (Privacidad, IT Law e Internet-Alicante)
Despacho Abogado Amigo (Valencia)
Gabinete Jurídico Jose Enrique Colastra Escobar (Toledo)
Datalia (La Rioja)
Grupo CFI (Palencia)
ADEGUA(Valencia)
Despacho Broseta-Asociados (Valencia)
NT Abogados (Valladolid)
Despacho Iskipa-Protección de Datos (Madrid)
Despacho Hogan Lovells (Madrid)
Eurovima Consulting (Madrid)
Despacho Ecix (Madrid)
Écija Asociados (Madrid)
Suarez de la Dehesa Abogados (Madrid)
Despacho Audens-Marcos Judel (Madrid)
Agencia Española de Protección de Datos*
Audens Legal (Madrid)
Javier Puyol-Abogado
Fernando Andreu Royo- E&K Pro (Zaragoza)

C.FI Construyendo Futuro Informático (Palencia)
Rafael Perales Cañete Abogados (Córdoba)
IPNET Centralized Solutions, SLU (Barcelona)
INPROAS Consultores
Secretaria General de Instituciones Penitenciarias
Juzgado 1ª instancia e Instrucción nº 2 Alzira (Comunidad Valenciana)
Juzgado de lo Penal nº 3 de Cádiz
Juzgado mixto nº1 de la Palma del Condado (Huelva)
Adarve Corporación Jurídica (Madrid)
ARRAEZ PROSPER BOLOGNINI & VALLEJO SLP (Madrid)
Díaz y Garrote Abogados (Castilla y León)
Ofiseg Consulting S.L

Otras instituciones con las que se prevé iniciar colaboraciones:

Uría Menéndez
Gomez Acebo y Pombo
Ramón y Cajal–Abogados
Deloitte.
EDPS BUTTARELLI
MCA Consultores (Sevilla)
Legitec (Murcia)
Despacho Jausas Legal.(Barcelona)
Despacho Agencia Activa (Zaragoza)
Weizmare S.L (Galicia)
Despacho Astrea (Lérida)

(*En espera de recibir el convenio con la Agencia Española de Protección de Datos, que cuenta con 300 asociados. Una vez contemos con él, se adjuntará.)

Así mismo, se y a modo de ejemplo, se adjuntan al final de este documento algunos de estos convenios firmados.

7.3. Dotación de infraestructuras docentes

7.3.1. Software de gestión académica

La Universidad Internacional de La Rioja dispone de herramientas de gestión que permiten desarrollar de forma eficiente los procesos académico-administrativos requeridos por el título que son los de acceso, admisión, expediente, reconocimientos y transferencias, gestión de actas, expedición de títulos, convocatorias) y los procesos auxiliares de gestión de la universidad como

son la gestión de exámenes, gestión de defensas de Trabajo Fin de Grado/Máster, gestión de prácticas, etc.

Dichas herramientas se han desarrollado sobre la base de la gestión por procesos, la gestión de calidad y la satisfacción de las necesidades y expectativas de los usuarios; y todo ello, al tratarse de una universidad en internet, previendo que las solicitudes y trámites puedan desarrollarse íntegramente a distancia.

7.3.2. Campus virtual

UNIR cuenta con una plataforma de formación propia preparada para la realización de los títulos (eLMSCepal) diseñada sobre la base de la experiencia formativa de una de las empresas promotoras de UNIR, que cuenta con más de 13 años en gestión y formación y por la que han pasado más de 30.000 alumnos.

Esta plataforma pertenece a Entornos de Aprendizaje Virtuales (VLE, Virtual Learning Managements), un subgrupo de los Gestores de Contenidos Educativos (LMS, Learning Management Systems).

Se trata de aplicaciones para crear espacios donde un centro educativo, institución o empresa, gestiona recursos educativos proporcionados por unos docentes y organiza el acceso a esos recursos por los estudiantes y, además, permiten la comunicación entre todos los implicados (alumnado y profesorado). Entre sus características cabe destacar:

- Es fácil de utilizar y no requiere conocimientos específicos por lo que el estudiante puede dedicar todos sus esfuerzos al aprendizaje de la materia que le interesa.
- Todo el sistema opera a través de la Web por lo que no es necesario que los alumnos aprendan a utilizar ningún otro programa adicional.
- Es un sistema flexible que permite adaptarse a todo tipo de necesidades formativas.

Dentro del campus virtual el estudiante encuentra tantas aulas virtuales como asignaturas tenga matriculadas. Desde el aula puede acceder a las sesiones presenciales virtuales a través de la televisión en Internet, que está basado en Adobe Flash Player, una aplicación que ya está instalada en más del 98% de los equipos de escritorio conectados a Internet.

La difusión se realiza mediante el streaming, es decir, el usuario no descarga nada en su ordenador, el visionado se realiza almacenando una mínima cantidad de información (buffering) para el visionado de los contenidos.

Los requisitos técnicos para participar en las sesiones virtuales se resumen en la siguiente tabla:

REQUISITOS TÉCNICOS	
Sistema operativo	Windows 98 SE, 2000, XP, Vista, Mac OS

Navegadores	▪ Internet Explorer 6.0 o superior ▪ Mozilla firefox 1.5 ▪ Netscape Navigator 7.1 ▪ Safari 2.x ▪ AOL 9
Resolución pantalla	Resolución Mínima de 800x600 (se recomienda 1024x768 o superior).
Ancho de banda	56 ADSL/ Cable (conexión alámbrica recomendada).
Red	Acceso externo a Internet, sin restricción de puertos o URL no corporativas.
Audio	Tarjeta de audio integrada, con altavoces o toma de auriculares.
Video	WebCam compatible con los sistemas operativos mencionados.
Equipos PC	RAM: mínimo recomendado 512 Mb. Procesador: mínimo Pentium IV o superior

7.3.3. Biblioteca virtual

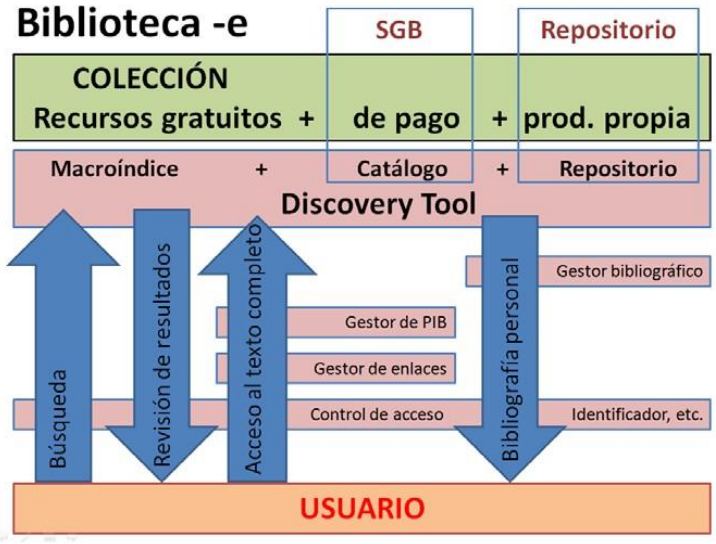
El material bibliográfico y documental, se gestiona a través de una biblioteca virtual. Esta cubre las necesidades de información de sus profesores, investigadores, alumnos y PAS, para la realización de sus tareas de docencia, investigación y gestión.

La política de adquisiciones de la biblioteca de UNIR bascula fundamentalmente sobre recursos en soporte digital. La aún imprescindible adquisición de bibliografía en soporte de papel, se enfocará prioritariamente sobre aquellas áreas de conocimiento en las que se incardinen las líneas de investigación estratégicas de la universidad.

La adscripción de UNIR a la CRUE ha implicado la pertenencia a la red REBIUN, con los derechos y obligaciones que prevé su Reglamento. El servicio de préstamo interbibliotecario de REBIUN es un instrumento fundamental para la investigación de los profesores.

La constitución de la biblioteca virtual se ha iniciado con la adquisición de un sistema de gestión de biblioteca y una herramienta de descubrimiento propiedad de PROQUEST, las cuales son la base para futuras extensiones.

La visión de biblioteca virtual sigue el modelo mostrado en la siguiente figura:



7.4. Dotación de infraestructuras investigadoras

El profesorado está integrado en cuatro ejes académicos fundamentales: Educación, Comunicación, Ciencias Sociales y Tecnología. Estos cuatro ejes vertebran la estructura investigadora.

Ha sido creado, además, la Oficina de Consultoría y Apoyo a Proyectos de Investigación (OCAPI) con carácter interdisciplinar para coordinar todas las actividades investigadoras de UNIR y proporcionar apoyo al personal docente-investigador (PDI) adscrito a la Universidad. Su finalidad es estimular y facilitar la participación efectiva de la comunidad académica UNIR en iniciativas de investigación, tanto propias como europeas, nacionales y regionales.

UNIR desarrolla un plan bienal de investigación (Plan Propio de Investigación) que define las líneas maestras para el presente bienio, y aprueban seis líneas iniciales de I+D, que son desarrolladas por grupos de Investigación formados en torno a las líneas básicas de I+D. Los grupos están dirigidos por catedráticos y académicos de prestigio en sus áreas. Los grupos son flexibles e incorporan candidatos durante el bienio. Así, se parte de una estructura de 7 grupos con 15 miembros, aunque se espera duplicar en el plazo de 18 meses.

Al mismo tiempo, todo profesor recibe orientación y apoyo para mantener una carrera investigadora (publicación científica, dirección de trabajos de grado, tesinas de máster y tesis doctorales, estancias de investigación, etc.) que dependerá tanto de su implicación en Unir como del plan individual de carrera elaborado para cada uno.

De esta manera, articulamos el personal investigador alrededor de Grupos y Líneas de trabajo, sin olvidar la atención individual según parámetros personales.

7.5. Recursos de telecomunicaciones

Los recursos disponibles en UNIR son los siguientes:

- 90 líneas de teléfono a través de tres primarios de telefonía en Madrid.
- 30 líneas de teléfono a través de un primario de telefonía en Logroño.
- Número de teléfono de red inteligente para llamadas entrantes: 902 02 00 03.

- Centralita de telefónica administrativa Panasonic TDA 600. 16 canales voIP + analógicos.
- Nueve enlaces móviles con conexión digital a la central.
- Cuatro líneas de banda ancha redundantes y balanceadas utilizando tecnología Cisco para dar acceso a: Internet, Conectividad con Universitas XXI y al Campo Moodle que tiene UNIR externalizado.
- Telefonía basada en VoIP sobre servidores Cisco Call Manager 5.1 redundados.
- 100 por 100 de los puestos de trabajo con acceso a la red local mediante cable.
- Cobertura WIFI en todas las dependencias universitarias.
- Sistemas de alimentación eléctrica ininterrumpida mediante baterías y un generador diesel que garantiza el servicio necesario para las comunicaciones y el normal funcionamiento de todos los equipos informáticos en caso de fallo eléctrico con autonomía de ocho horas.

7.6. Mecanismos para garantizar el servicio basado en las TIC

El modelo de enseñanza de UNIR hace un uso intensivo de las TIC para garantizar el proceso de enseñanza-aprendizaje. Las infraestructuras tecnológicas que sirven de apoyo a la educación a distancia en UNIR garantizan la accesibilidad a los servicios en todo momento.

UNIR tiene contratado un proveedor europeo de servicios de Presencia en Internet, Hosting Gestionado, Cloud Computing y Soluciones de Infraestructura TIC (Arsys).Que nos permite:

- Optimizar la velocidad de conexión con todos los usuarios de Internet, de esta manera nuestros servidores pueden ser vistos con gran rapidez y sin cuellos de botella por usuarios de conexiones RTB, RDSI, ADSL, cable, etc., así como por internautas extranjeros.
- Redundancia física. Si una línea sufre un corte, las restantes mantendrán la conectividad con Internet.
- Velocidad de descarga hacia cualquier destino. Los paquetes de datos escogerán la ruta más adecuada para llegar al usuario que está viendo las páginas por el camino más corto.

Desde el punto de vista técnico, UNIR dispone de las más avanzadas instalaciones en materia de seguridad física, control de temperatura y humedad, seguridad contra incendios y alta disponibilidad de energía eléctrica. Se detalla a continuación:

INSTALACIONES DE SEGURIDAD
Seguridad física
- Sensores para el control de la temperatura y humedad ambiente. - Filtrado de aire para evitar la entrada de partículas. - Sistema automático balanceado y redundante de aire acondicionado. - Sistema de detección de incendios que dispara, en caso de necesidad, un dispositivo de expulsión de gas inerte que extingue el fuego en pocos segundos.
Seguridad en el suministro eléctrico
- Sistema de Alimentación Ininterrumpida (SAI) para garantizar la estabilidad y continuidad de los equipos. - Grupo electrógeno autónomo que suministraría, en caso de corte prolongado, la energía necesaria para que no haya pérdida de alimentación, de modo que los servicios a clientes no sufran ninguna alteración.
Seguridad perimetral
- Acceso restringido por control de tarjeta magnética y contraseña. - Sistema generalizado de alarmas. - Tele vigilancia.

7.7. Detalle del servicio de alojamiento

7.7.1. Recursos software

La infraestructura lógica necesaria para el funcionamiento del campus virtual se describe en la siguiente tabla:

RECURSOS SOFTWARE	
Acceso Remote Desktop	Servidor de base de datos MySQL
Express Edition Soporte ASP y ASP.NET	Servidor de base de datos PostgreSQL
Extensiones FrontPage	Servidor de base de datos SQL Server 2000/2005
Filtro antivirus / antispam avanzado	Servidor de correo (POP3/SMTP/listas)

Gestor de Base de datos: Microsoft SQL Server 2005/2008	Servidor de estadísticas AWStats
Indexador de ficheros Microsoft Index Server	Servidor FTP
Intérpretes VBScript, JScript, Active Perl, PHP y Python	Servidor Multimedia Windows Media Server
Lenguaje de programación ASP y ASP.NET	Servidor web IIS
Mailenable	Sistema Operativo: Windows 2000/2003/2008 Server
Microsoft oBind	Tecnología Microsoft
Microsoft Servidor DNS	Webmail Horde

7.7.2. Recursos hardware

La infraestructura física necesaria para el funcionamiento del campus virtual se describe en tres puntos: Características técnicas del servidor, Características del hosting y Sistema de copias de seguridad. Tal como se describen a continuación en la tabla:

<table>
<tr><th colspan="2">RECURSOS HARDWARE</th></tr>
<tr><th colspan="2">Características técnicas del servidor</th></tr>
<tr><th>Detalle de la máquina</th><th>Gestión del producto</th></tr>
<tr><td rowspan="7">Fabricante: IBM
Modelo Xeon E5-2630 0
Tipo CPU: Intel Xeon Quad-Core
Número de núcleos: 24
Velocidad de cada núcleo: 2.30 GHz
Memoria RAM: 32 GB ECC
Tamaño de discos 2x300 GB
HDD Discos: 136 GB RAID 1
HDD cabina FC: 2 TB
SAS RAID: RAID 1 Hot Swap –
Transferencia: 18 Mbps</td><td>Panel de control
Reinicios y reseteos
Avisos automáticos (email/SMS)
Gráficos de ancho de banda y transferencia
Direcciones IP extra</td></tr>
<tr><td>Seguridad</td></tr>
<tr><td>Alojamiento IDC Protección firewall
Monitorización avanzada</td></tr>
<tr><td>Garantías y Soporte</td></tr>
<tr><td>Garantía hardware ilimitada Soporte 24x7</td></tr>
</table>

Características del hosting
Disponibilidad 24x7 del portal y la plataforma de formación con un porcentaje de disponibilidad del 99%.
Servicio de backup y recovery de los datos almacenados en los servidores.
Servicios de retenciones: Retención de la imágenes de los backup realizados por el tiempo que se acuerde.
Servicios de sistemas de seguridad: Física (Control de Accesos, Extensión de Incendios, Alimentación ininterrumpida eléctrica, etc.,..) y Lógica (Firewalls, Antivirus, Securización Web, etc.).
Servicio de Monitorización, Informes y estadísticas de Ancho de Banda, disponibilidad de URL, rendimiento, etc.

Sistema de copias seguridad
Compresión de datos de alto nivel
El proceso de copia se realiza a través de una tecnología puntera de copias de seguridad incrementales y completas, FastBit, que le garantiza: - Altos niveles de compresión (un 50% de media), lo que nos permite almacenar en el servidor 2 veces el espacio contratado. - Menor transferencia de datos, por lo que podrá realizar sus copias desde cualquier tipo de acceso a Internet, incluso desde una conexión RTB por línea analógica.
Proceso sencillo y automático
Pues no se ha de recurrir a los métodos manuales en los que tiene que dedicar mucho tiempo y esfuerzo. Con el sistema de Backup Online se realizan las copias de seguridad con gran facilidad, lo que permite despreocuparse del proceso.
Copia segura

El proceso de copia se realiza a través de una clave de cifrado y previa autentificación del usuario de acceso al servicio.

Se utiliza un algoritmo de cifrado de 448 bits (superior a los que se utilizan en certificados de seguridad web), a través de una clave privada, lo que garantiza que la información se almacena de forma segura y no es accesible más que por el usuario del servicio.

Además, al efectuar la copia en un servidor de Internet, sus datos se encuentran a salvo de cualquier incidente y fuera de sus instalaciones, lo que le protege ante catástrofes como incendios, errores humanos, fallos hardware o software, etc.

7.8. Previsión de adquisición de recursos materiales y servicios necesarios

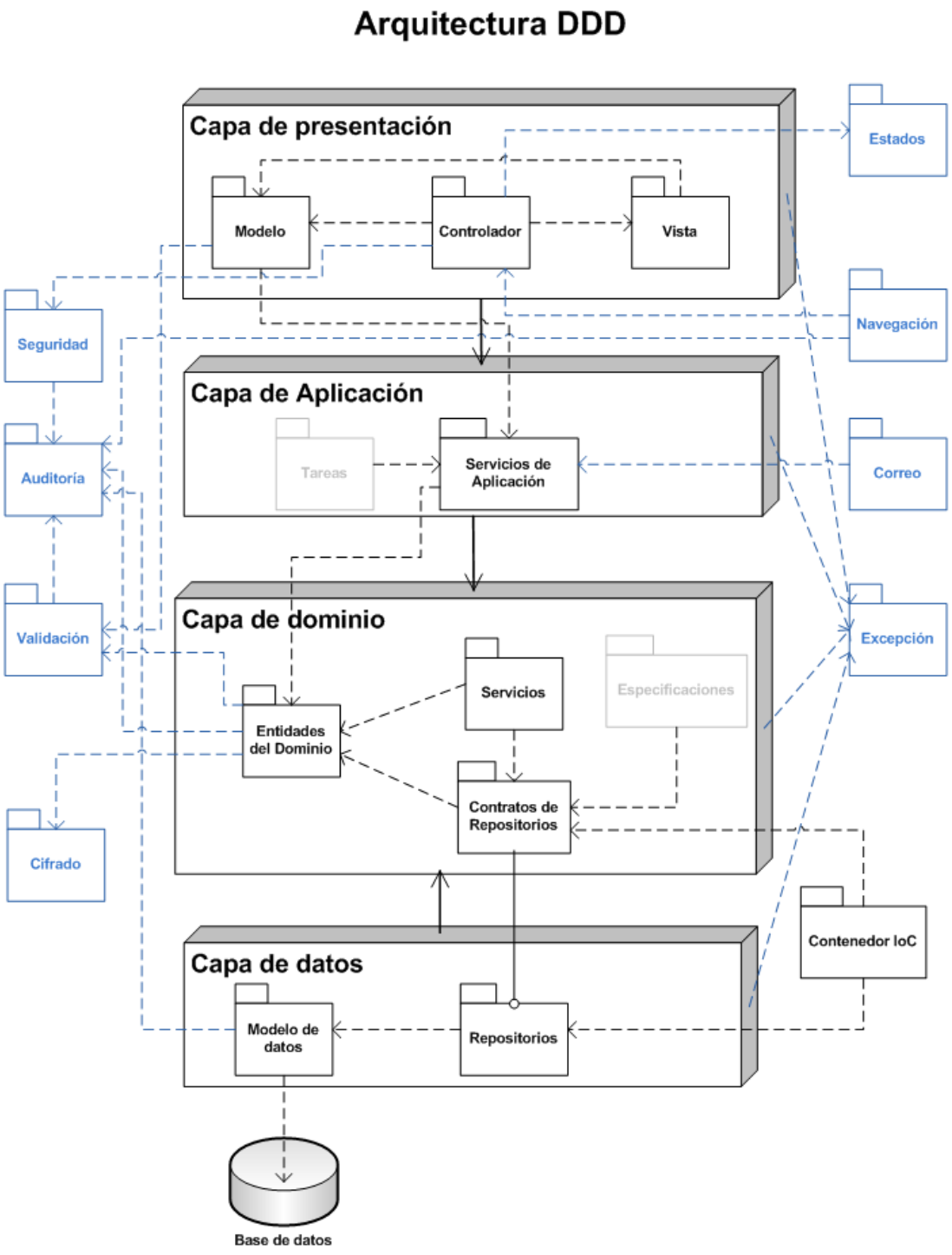
Este cuadro resume la planificación sistemática de infraestructuras, materiales y servicios de los que la Universidad se dotará en los próximos años de acuerdo a la previsión anual de incorporación de personal.

RECURSOS	2013-14	2014-15	2015-16
Capacidad máxima de acceso a Internet	600 Mb	700 Mb	560 Mb
Líneas de acceso a internet redundadas	9	10	8
Capacidad de almacenamiento en servidores centrales en TeraBytes	24	30	24
Impresoras departamentales (con fax y escáner)	32	32	32
Impresoras escritorio	8	10	12
Potencia de SAI	30Kwa	40Kwa	40Kwa
Potencia generadores diésel	50Kw	60Kw	60Kw
Líneas telefónicas	160	190	130
Puntos de acceso *wireless*	14	16	18
Ordenadores sobremesa	460	500	412
Ordenadores portátiles	17	20	25
Teléfonos VoIP sobremesa	20	24	28

Teléfonos VoIP softphone	20	24	28

7.9. Arquitectura de software

Para el desarrollo de las aplicaciones informáticas desarrolladas a partir del 2012. UNIR ha implantado una arquitectura de software orientada a Dominio DDD. Esta arquitectura dispone de componentes horizontales y transversales que se muestran en la siguiente figura:



7.9.1. Componentes horizontales

Componentes horizontales.	
Capa de presentación	Basada en la definición del modelo vista controlador. Implementa las pantallas de usuario y los controladores de estas.
Capa de aplicación	Coordina actividades propias de la aplicación pero no incluye lógica de negocio siguiendo el Principio de “Separation of Concerns”.
Capa de dominio	Basada en la definición del patrón “Entity” e implementada a través de las “IPOCO Entities”. Esta capa está completamente desacoplada de la capa de datos para lo cual se aplica el patrón “Inversion of Control”.
Capa de datos	Basada en la definición del patrón “Repository” y es la encargada de acceder a la base de datos de la aplicación.

7.9.2. Componentes transversales

Componentes transversales	
Componente de seguridad	Gestiona la seguridad en el acceso a la aplicación, y se divide en dos: 1. Autenticación: Permite validar la identidad de los usuarios e incluye el inicio y fin de sesión, el recordatorio y cambio de contraseña y la activación de cuenta de los usuarios. 2. Autorización: Permite gestionar los permisos de los usuarios en la aplicación a partir de los roles que les hubiesen sido asignados e incluye: Permisos de acceso a las páginas Permisos de acceso a las opciones de menú Permisos de lectura, escritura, eliminación y consulta Permisos de ejecución de acciones
Componente de estados	Implementado en base al patrón “Memento” y permite recuperar el estado anterior de una página durante el proceso de navegación del usuario para mantener los valores introducidos en los filtros, listados, asistentes, etc. Deberá estar preparado para escenarios con granja de servidores.
Componente de navegación	Permite establecer la relación de flujos entre las páginas de la aplicación para mantener la coherencia en la navegación del usuario.

Componente de validación	Permite realizar las validaciones de los valores de entrada y salida de la aplicación. Incluye lo siguiente: 1. Validación de definición de campos: Permite validar la definición de los campos en base a la longitud, tipo de dato, rango de valores, etc. 2. Validación de formatos: Permite validar los formatos de texto conocidos como son: NSS, NIE, NIF, CIF, CCC, EMAIL, MOVIL, etc. 3. Filtrado de textos: Permite filtrar los textos de entrada (usuarios) y salida (base de datos) en base a una lista negra de palabras con el fin de evitar inyecciones de SQL y de XSS.
Componente de auditoría	Permite registrar una bitácora de las acciones realizadas por los usuarios en la aplicación almacenando: la naturaleza de la acción, el momento en que se realizó, desde donde y el usuario que la ejecutó. Incluye 5 niveles de auditoría: 1. Auditoría de acceso: Encargado de registrar los inicios, cierres de sesión, intentos fallidos en la aplicación, solicitudes de recordatorio y cambios de contraseña. 2. Auditoría de navegación: Encargado de registrar las páginas visitadas por los usuarios en la aplicación recogiendo la mayor cantidad de parámetros posibles (tiempo, navegador, etc.). 3. Auditoría de acciones: Encargado de registrar todas las acciones realizadas por el usuario en el sistema recogiendo la mayor cantidad de parámetros posibles (contexto, registro, etc.). 4. Auditoría de datos: Encargado de registrar los cambios que un usuario realiza sobre los datos de la aplicación recogiendo la mayor cantidad de parámetros posibles. Incluye operaciones de alta, edición, eliminación y consulta de registros (contexto, registro, filtro, etc.). 5. Auditoría de validación: Encargado de registrar las validaciones incorrectas y filtros aplicados que eliminaron cadenas de inyección SQL y XSS.
Componente de excepciones	Encargado de interceptar, registrar, categorizar y comunicar los errores encontrados en la aplicación en producción. Estas excepciones deberán estar dentro de un contexto para identificar como han ido subiendo por las diferentes capas e incluirán información relativa al espacio de nombres, clase, método y cualquier información adicional como ser el usuario.
Componente de cifrado	Encargado de realizar el cifrado y descifrado de información sensible como la contraseña o datos sensibles según la L.O.P.D.
Componente de correo	Encargado de realizar el envío de los correos electrónicos de la aplicación.

7.10. Criterios de accesibilidad universal y diseño para todos

Se está trabajando para que el campus virtual alcance el nivel AA de las Pautas de Accesibilidad para el Contenido en la Web 2.0 del W3C, cuyos requisitos se recogen en la norma española sobre accesibilidad web (UNE 139803:2012).

Para garantizar la integración de las personas con discapacidad en el aula, se presta especial atención a la accesibilidad de aquellas funcionalidades que promueven la interacción entre estudiantes y de éstos con los profesores: foro, videoconferencia, etc.

El objetivo es que los contenidos formativos y las actividades sean igualmente accesibles, tanto a nivel técnico (aplicación de las citadas Pautas de Accesibilidad para el Contenido en la Web 2.0) como pedagógico (objetivos formativos alcanzables por los distintos perfiles de discapacidad).

Para que la producción de contenidos por parte del equipo docente se ajuste a los requerimientos de accesibilidad establecidos, éstos se desarrollarán mediante plantillas en Word con estilos cerrados. Además, una vez producidos, se exportarán a distintos formatos para facilitar a los estudiantes el acceso multidispositivo: HTML y PDF accesible.

Por último, con el fin de asegurar que tanto el campus virtual como los contenidos se ajustan a los requerimientos del W3C y de la norma española, UNIR está negociando con FundosaTechnosite, empresa especializada en tecnología y accesibilidad de la Fundación ONCE, la certificación del grado de adecuación a los estándares de accesibilidad, y contempla un plan de mantenimiento mediante revisiones periódicas para asegurar que la accesibilidad se mantiene en el tiempo.

8. RESULTADOS PREVISTOS

8.1. Valores cuantitativos estimados para los indicadores y su justificación

Una previsión de los resultados que obtendrán los estudiantes del Máster se enfrenta con los siguientes factores de dificultad.

- Primero.- Se trata de una titulación que se impartirá en una universidad de reciente creación y pocos precedentes sobre los que basarse.

- Segundo.- Su sistema de enseñanza es a distancia, por lo que la comparación de datos con universidades tradicionales debe hacerse con especial cautela.

Los resultados previstos son los siguientes:

Tasa de graduación	95%
Tasa de abandono	5%
Tasa de eficiencia	95%

Estas previsiones, se justifican por tres circunstancias, dos tienen que ver con los datos procedentes de la Universidad, y otro, con los contenidos del Máster:

1º. El perfil mayoritario de alumnos de UNIR son estudiantes muy motivados y que son conscientes de la mejora profesional y/o personal que implican sus estudios.

2º. Los resultados obtenidos en todos los másteres impartidos en la Facultad de Derecho de UNIR, revelan tasas similares.

3º. En tercer lugar, la escasez de profesionales especializados en este ámbito, en un mundo globalizado donde cada vez más entidades y empresas demandan este tipo de profesional, genera una motivación extra, que justifica la elevada tasa de graduación estimada.

8.2. Procedimiento para valorar los resultados

La Unidad de Calidad de cada Titulación hace un estudio, análisis de datos y propuesta de mejora referidas a resultados académicos. Los factores que tienen en cuenta en este análisis son:

- Curso académico de implantación. Los años que lleve el título implantado debe afectar positivamente a los resultados del aprendizaje.

- Fecha de constitución de la UCT. Los años que lleve el título implantado debe afectar positivamente a los resultados del aprendizaje.

- Principales indicadores del título (tasa de rendimiento, abandono, eficiencia y graduación). Estos datos deben interpretarse en función de la normativa de permanencia y el perfil mayoritario de los estudiantes.
- La evaluación de las prácticas externas en su caso. Se relaciona los estudiantes que escogen hacer prácticas con las plazas ofertadas y con el número de tutores.
- La satisfacción de los estudiantes, medida a través de encuestas, sugerencias y reclamaciones.

De este análisis se desprenden los puntos fuertes y los puntos débiles de la titulación, que permitirá fijar las áreas de mejora más convenientes. Esta información queda plasmada en un informe anual que se envía a la Unidad de Calidad de la Universidad (UNICA) para su revisión y búsqueda de puntos en común con el resto de titulaciones. Principalmente debe velar porque los objetivos sean coherentes, medibles, y que tengan asociados indicadores adecuados.

Finalmente en la reunión del Pleno de la UNICA, que se celebra dos veces al año, la Directora de Calidad ratifica los objetivos de mejora propuestos por la UCT para su titulación. También hace una propuesta de objetivos de mejora de la Universidad y que repercutirán en la totalidad de las titulaciones.

9. SISTEMA DE GARANTÍA DE CALIDAD

http://gestor.unir.net/userFiles/file/documentos/planes_calidad/garantia_calidad_grado_master.pdf.

10.CALENDARIO DE IMPLANTACIÓN

10.1. Cronograma de implantación del Título

La implantación se hará de acuerdo con la temporalidad prevista en el plan de estudios del Máster, de un año de duración:

CURSO 2014 - 2015	
Primer cuatrimestre	**Segundo cuatrimestre**
El Derecho Fundamental a la Protección de Datos	Gestión Económica y Empresarial y Protección de Datos Personales.
Derechos de los Titulares de Datos (I)	Salud e Investigación Biomédica.
Derechos de los Titulares de Datos (II)	Ficheros Públicos
Protección de Datos Personales y Gestión de las Organizaciones	El Futuro de la Protección de Datos Personales
Las TIC y la Seguridad	TFM
Los Deberes de Secreto y Seguridad.	

10.2. Procedimiento de adaptación de los estudiantes

No aplicable.

10.3. Enseñanzas que se extinguen

No aplicable.

10.4. Extinción de las enseñanzas

UNIR podrá decidir, a través de los órganos previstos en sus normas de organización y funcionamiento con competencia en la implantación y extinción de titulaciones, que el presente Máster se extinga si, tras tres cursos consecutivos, el número de alumnos de nuevo ingreso no supera la cifra de 15.

La salvaguardia de los derechos de los estudiantes queda asegurada, tal como se indica en la disposición primera de las Normas de Permanencia: “Se garantiza a todo estudiante el derecho a terminar su titulación siempre que cumpla las normas que se indican en el punto 2. En el supuesto de que el Consejo de Administración, debido a causas graves, se plantease la posible extinción de la titulación, esta sólo podría ejecutarse mediante el procedimiento de no ofertar plazas para nuevos estudiantes en el curso siguiente definiendo un plan de extinción que, de acuerdo con la legislación vigente, garantice la finalización de los estudios a quienes lo hubieran comenzado”.