

**TÍTULO: PROTECCIÓN DE DATOS EN LA SOCIEDAD
DIGITAL**

DESTINATARIO: SERVICIO DE ORDENACIÓN ACADÉMICA

UNIVERSIDAD INTERNACIONAL DE
ANDALUCÍA

ENSEÑANZAS PROPIAS DE POSTGRADO
MEMORIA ACADÉMICA

1. DESCRIPCIÓN DEL TÍTULO
1.1 TIPO DE ENSEÑANZA <div style="display: flex; justify-content: space-around;"> <input type="checkbox"/> Máster <input checked="" type="checkbox"/> Diploma de Especialización </div>
1.2 DENOMINACIÓN Protección de datos en la Sociedad Digital
1.3 ÁREA DE CONOCIMIENTO <div style="display: flex; justify-content: space-around;"> <input type="checkbox"/> Artes y Humanidades <input type="checkbox"/> Ciencias <input type="checkbox"/> Ciencias de la Salud </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input checked="" type="checkbox"/> Ciencias Sociales y Jurídicas <input type="checkbox"/> Ingeniería y Arquitectura </div>
1.4 ENTIDADES PARTICIPANTES Universidad Internacional de Andalucía
1.5 DIRECCIÓN ACADÉMICA Prof. Dr. D. Manuel Jesús Díaz Gómez Pfra. Dra. D ^a . Susana Ruiz Tarrías
1.6 COMISIÓN ACADÉMICA Prof. Dr. D. Manuel Jesús Díaz Gómez Pfra. Dra. D ^a . Rocío López San Luis Pfr. Dr. D. Ramón M ^a Orza Linares Pfra. Dra. D ^a . Susana Ruiz Tarrías Pfra. Dra. D ^a . María Serrano Fernández Prof. Dr. D. Javier Valls Prieto Prof. Dr. D. Juan Gómez Romero
(Junto al Presidente/a, debe haber al menos dos representantes del profesorado con docencia en el título. De entre los vocales debe designarse un miembro que hará la labor de Secretario/a de la Comisión.)
1.7 COMISIÓN DE GARANTÍA DE CALIDAD Prof. Dr. D. Manuel Jesús Díaz Gómez Pfra. Dra. D ^a . Rocío López San Luis D ^a . Iciar López Vidriero-Tejedor D. Antonio Muñoz Ropa Prof. Dr. D. Ramón M ^a Orza Linares Pfra. Dra. D ^a . Susana Ruiz Tarrías Pfra. Dra. D ^a . María Serrano Fernández

Prof. Dr. D. Javier Valls Prieto Prof. Dr. D. Juan Gómez Romero Representante PAS: A determinar Representante Alumnos: A determinar		
1.8 NÚMERO DE PLAZAS OFERTADAS		
Ofertadas: 30	Mínimo: 20	Máximo: 40
1.9 NÚMERO DE CRÉDITOS ECTS		
Nº total de ECTS ofertados: 30	Nº total de ECTS necesarios para la obtención del título: 30	
1.10 MODALIDAD DE ENSEÑANZA		
<input type="checkbox"/> Presencial	<input type="checkbox"/> Semipresencial	<input checked="" type="checkbox"/> Virtual
	<ul style="list-style-type: none"> Nº de créditos presenciales: Nº de créditos virtuales: Nº de créditos Trabajo Final: 	
1.11 LENGUA/S UTILIZADA/S		
Español.		
1.12 SUBVENCIONES O APORTACIONES PREVISTAS		
No se contemplan en esta edición.		
2. JUSTIFICACIÓN DEL TÍTULO (interés académico, científico o profesional del mismo)		
<p>El constituyente español se adelantó a su tiempo al prever en el art. 18.4 de la Constitución la limitación legal del uso de la informática para garantizar el pleno uso de los derechos fundamentales. Así lo reconoce, por lo demás, la Exposición de Motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, al afirmar que <i>“los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales (...)”</i>.</p> <p>El derecho a la protección de los datos personales se reconoce también por el artículo 8(1) de la Carta de los Derechos Fundamentales de la Unión Europea, y por el artículo 16(1) del Tratado de Funcionamiento de la Unión Europea (TFUE), y en el ámbito de la ONU se han adoptado dos resoluciones sobre el derecho a la privacidad en la era digital. Estas resoluciones condenan las actividades de vigilancia a gran escala y ponen de manifiesto sus repercusiones para los derechos fundamentales a la privacidad y la libertad de expresión, así como para el funcionamiento de una sociedad democrática. Aunque no resultan jurídicamente vinculantes, dieron lugar al nombramiento de un Relator Especial sobre el derecho a la privacidad, con el mandato de promover y proteger este derecho.</p> <p>Precisamente, como ha afirmado el Relator Especial de Naciones Unidas, Sr. F. La Rue, el acceso a internet ha sido reconocido como un derecho instrumental derivado de la libertad de opinión, expresión, información y comunicación. Según estima, el derecho a la libertad de opinión y de expresión es mucho más que un derecho fundamental, pues por sí mismo puede ‘posibilitar’ otros derechos, incluidos derechos de contenido económico, social y cultural, como el derecho a la educación, el derecho a participar en la vida cultural y disfrutar de los beneficios del progreso científico y sus aplicaciones. En este sentido, actúa como ‘catalizador’ para el ejercicio por los ciudadanos de su derecho a la libertad de opinión y expresión así como otros derechos humanos [United Nations. General Assembly. Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (16 May 2011)].</p> <p style="text-align: center;">Sin embargo, al mismo tiempo, internet se convierte en un ámbito en el que los derechos de los ciudadanos</p>		

se exponen a nuevas amenazas frente a las cuales los poderes públicos deben desarrollar mecanismos adecuados de protección. Ello afecta, especialmente, a los datos personales y los posibles riesgos a los que quedan expuestos tanto desde la perspectiva de la cesión como de la transferencia de datos.

En el ámbito de la cesión de datos personales, la Unión Europea ha vuelto a establecer un hito en la historia de la protección de datos personales, mediante la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (conocido como Reglamento General de Protección de Datos, en adelante RGPD), cuya entrada en vigor tuvo lugar el 25 de mayo de 2018. Como resulta conocido, en desarrollo de las previsiones del RGPD ha sido aprobada la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

La nueva regulación mantiene la consideración de *datos personales*, respecto de toda información sobre una persona física identificada o identificable, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, aunque no se trate de un derecho de carácter absoluto y pueda ser ponderado con respecto a otros derechos fundamentales de acuerdo con el principio de proporcionalidad.

Desde tales premisas, el RGPD se fundamenta en dos pilares. De un lado, pretende alcanzar una protección efectiva de los datos personales de los ciudadanos de la Unión mediante el refuerzo y la especificación de los derechos de los interesados y de las obligaciones de los responsables y los encargados del tratamiento de datos de carácter personal. De otro lado, tiene como objetivo establecer normas coherentes y uniformes que favorezcan la libre circulación de los datos personales dentro del mercado interior o espacio económico europeo (EEE). Como se refiere en el punto 2 de la Memoria Científico Técnica, este objetivo del RGPD, concretado según se detalla, constituye la hipótesis de partida del Proyecto que se solicita.

Con el fin de armonizar la libre circulación de datos personales en el EEE con la garantía adecuada de este derecho fundamental, el RGPD incorpora como novedad respecto a la Directiva 95/46/CE, el principio de responsabilidad activa o *accountability* (art. 5.2). Este modelo de responsabilidad supone el paso del anterior sistema de *checklist*, en el que el legislador europeo y nacional enunciaban con carácter exhaustivo los objetivos a cumplir por los operadores y éstos debían simplemente comprobar el cumplimiento de estas obligaciones, a un modelo de responsabilidad en el que los operadores, atendiendo a las operaciones de tratamiento que se pretendan llevar a cabo, y sobre la base de un enfoque que debe tomar en consideración, esencialmente, el riesgo para los datos personales derivado de ese tratamiento, deben determinar cuáles son las obligaciones a cumplir.

Así, la Exposición de Motivos de la LOPDGDD reconoce que la mayor novedad del RGPD consiste en *“la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan”*.

En este contexto, la figura del Delegado de Protección de Datos adquiere una destacada importancia en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

En concreto, contempla su existencia:

-cuando el tratamiento de datos lo lleve a cabo una autoridad u organismo público

-cuando el tratamiento de datos consista en operaciones que en razón de su naturaleza, alcance ó fines, requieran una observación habitual y sistemática de interesados a gran escala, o

-cuando sean tratados a gran escala categorías especiales de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a su salud o datos relativos a su vida u orientación sexual, así los datos relativos a condenas e infracciones penales, siempre que medie el consentimiento del interesado, el tratamiento sea necesario para el cumplimiento de obligaciones y disfrute de derechos en el ámbito de las relaciones laborales y la seguridad y protección social, sea necesario para la protección de intereses vitales del interesado, se trate de datos que el interesado ha hecho manifiestamente públicos, el tratamiento sea necesario para la formulación, ejercicio o defensa de reclamaciones o los tribunales actúen en ejercicio de la función judicial, el tratamiento sea necesario por razones de interés público esencial, para fines de medicina preventiva o laboral, o con fines de archivo de interés público (arts. 37, en relación con arts. 9 y 10 Reglamento(UE) General de Protección de Datos).

En desarrollo del art. 37 del Reglamento (UE) General de Protección de Datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, dedica su Título III a la regulación de la figura del Delegado de Protección de Datos en España, previendo su **designación** en (art. 34):

-Colegios Profesionales y Consejos Generales;

-Centros de Enseñanza en cualquiera de los niveles previstos en la LOE, así como en Universidades públicas y privadas;

-Entidades que exploten redes y presten servicios de comunicación electrónica cuando traten datos personales a gran escala;

-Prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios;

-Entidades de ordenación, supervisión y solvencia de entidades de crédito;

-Entidades aseguradoras y reaseguradoras;

-Empresas de servicios de inversión reguladas por la legislación del Mercado de Valores;

-Distribuidores y comercializadores de energía eléctrica y gas natural;

-Entidades que desarrollen actividades de publicidad, prospección comercial, incluidas las de investigación comercial y de mercados cuando elaboren perfiles de los afectados;

-Entidades emisoras de informes comerciales relativos a personas físicas;

-Operadores que desarrollen actividades relacionadas con el juego a través de canales electrónicos, informáticos, telemáticos e interactivos;

-Empresas de seguridad privada;

-Federaciones deportivas cuando traten datos de menores de edad.

Asimismo, la legislación española ha previsto detalladamente la **calificación** del Delegado de Protección de Datos, disponiendo (art. 35) su designación a través de mecanismos de certificación que tendrán en cuenta la **obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica de la protección de datos**.

Como desarrollo, a su vez, de esta previsión legal, la **Agencia Española de Protección de Datos** ha elaborado un **Esquema de Certificación de Protección de Datos** (Esquema AEPD-DPD), con objeto de establecer líneas generales

que regulen la Certificación de Personas para la categoría de Delegado de Protección de Datos, y las interrelaciones entre los diferentes Agentes que estarán implicados en dicha certificación.

En consecuencia, la figura del Delegado de Protección de Datos tiene prevista por la legislación española un amplio campo de intervención, que se traduce también en términos de ofertas de empleo en múltiples sectores económicos e institucionales que, en adelante, deberán ser cubiertas para dar cumplimiento a las exigencias legales.

[Redacted text block]

[Redacted text block]

3. COMPETENCIAS

3.1 BÁSICAS O GENERALES

- Capacidad para el manejo de fuentes jurídicas.
- Capacidad para identificar y seleccionar información estadística o numérica relevante.
- Capacidad de organización y planificación.
- Capacidad de gestión de la información, la resolución de problemas y la capacidad de decisión.
- Capacidad de trabajo en equipo y en equipo interdisciplinar.
- Razonamiento crítico y compromiso ético.
- Adaptación a nuevas situaciones.
- Motivación por la calidad y el aprendizaje autónomo.

3.2 ESPECÍFICAS

- Conocimiento exhaustivo de la legislación nacional y europea aplicable en materia de protección de datos.
- Conocimiento en profundidad de la jurisprudencia europea y nacional en materia de protección de datos.
- Conocimiento de las distintas entidades nacionales y europeas en materia de protección de datos y sus procedimientos de control.
- Conocimiento exhaustivo de las funciones, responsabilidades y obligaciones del Delegado de Protección de Datos.
- Conocimiento de las directrices de interpretación del Reglamento General de Protección de Datos.
- Conocimientos de las normativas sectoriales afectadas por la protección de datos y de la normativa española y europea con implicación en la protección de datos.
- Ser capaz de identificar tratamientos responsables y encargados, tratamientos y flujos de información sujetos a la normativa de protección de datos.
- Informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les incumben.

- Ser capaz de implementar los aspectos básicos para el cumplimiento de la normativa: registro de actividades, elaboración de políticas de privacidad, redacción de contratos, evaluación del nivel de seguridad, establecimiento de procedimientos de gestión de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición al tratamiento.
- Capacidad para auditar las necesidades de protección de datos de una organización teniendo en cuenta el ordenamiento sectorial.
- Conocimiento profundo de los aspectos técnicos de la seguridad.
- Capacidad de evaluar y verificar el cumplimiento de los objetivos de seguridad definidos por el Reglamento General de Protección de Datos y la legislación de desarrollo.
- Capacidad de integrar en sus análisis los requerimientos requeridos en la regulación específica en sistemas afectados por el Esquema Nacional de Seguridad y otras normas.
- Capacidad de verificar el grado de cumplimiento normativo de la protección de datos de una organización.

4. REQUISITOS DE ACCESO/ADMISIÓN

4.1 REQUISITOS DE ACCESO GENERALES Y ESPECÍFICOS

Estar en posesión de un título de Grado, acreditar experiencia profesional en el tratamiento de protección de datos, o el desempeño de actividad laboral que implique tratamiento de datos personales.

4.2 CRITERIOS DE ADMISIÓN

- Las solicitudes presentadas para cursar el Diploma de Protección de Datos en la sociedad digital de acuerdo con los requisitos fijados por la UNIA, serán valoradas por la Comisión Académica atendiendo a la experiencia profesional previa en materia de protección de datos acreditada y, en su defecto, al expediente académico oficial.

- En aplicación del art. 15.4 del Reglamento de Enseñanzas de Postgrado y Formación Continua de la Universidad Internacional de Andalucía, la Comisión Académica solicitará autorización para aceptar la matrícula condicional a los alumnos que lo soliciten en relación con el Diploma de Protección de Datos en la sociedad digital.

4.3 SISTEMAS DE APOYO Y ORIENTACIÓN DE LOS ESTUDIANTES UNA VEZ MATRICULADOS

- A través de la Plataforma virtual de la UNIA los estudiantes matriculados tendrán conocimiento de las fechas de inicio y finalización de cada uno de los módulos. Durante ese periodo podrán dirigir dudas y consultas al Profesorado responsable durante el desarrollo de cada uno de los contenidos docentes.

- Asimismo, a través de la Plataforma virtual de la UNIA los estudiantes matriculados tendrán acceso a los materiales de estudio y de trabajo para cada uno de los módulos, pruebas de conocimiento, y resultados de las mismas.

4.4 TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS: SISTEMA PROPUESTO POR LA UNIVERSIDAD

No procede.

4.5 COMPLEMENTOS DE FORMACIÓN



5. DESCRIPCIÓN DEL PLAN DE ESTUDIOSr				
5.1 NÚMERO DE CRÉDITOS ECTS				
Obligatorios: 26	Optativos:	Trabajo Final: 5	Prácticas externas	
			Curriculares:	Extracurriculares:
5.2 ESTRUCTURA DE LAS ENSEÑANZAS (distribución del plan de estudios en créditos ECTS, por módulo y materias/asignaturas)				
Módulo	Coordinador/a del módulo	Materias/Asignaturas que lo conforman	Nº de ECTS presenciales	Nº de ECTS virtuales
Nº1: La protección de datos en el ámbito internacional, supranacional y nacional. Normativa general y sectorial	Dña. Rocío López San Luis	- Contexto normativo: RGPD y LOPDGDD: •Fundamentos y principios. •Legitimación y derechos de los interesados. •Tipologías de datos personales y tratamiento. -El DPD: designación y competencias. -Autoridades de control y directrices de interpretación del RGPD. -Transferencias internacionales de datos y normativa española y europea implicadas. -Normativas sectoriales afectadas. -Procedimientos por vulneración de la normativa de protección de datos y régimen sancionador.		14
Nº2: Responsabilidad activa en la protección de datos personales	D. Antonio Muñoz Ropa	-Análisis y gestión de riesgos de los tratamientos de datos personales. Metodología y programa de cumplimiento. -Seguridad de la información. Marco normativo. Ciberseguridad y gobierno de la SI. -Puesta en práctica de la SI. Control de calidad. Seguridad por diseño y por defecto. -Evaluación de Impacto de Protección de Datos (EIPD)		7
Nº3: Auditoría en los sistemas de información.	Dña. Iciar López-Vidriero Tejedor	-La función de la auditoría en los SI. Estándares y directrices de auditoría de SI.		4

		-Principios de la auditoría -La auditoría: técnicas de auditoría		
Trabajo Final				5
5.3 METODOLOGÍA DOCENTE				
<p>Al tratarse de un Diploma 100% virtual se utilizarán las herramientas tecnológicas necesarias que permite o soporta la plataforma de la UNIA (vídeos, chats, audios, etc.) para presentar los contenidos básicos que deben conocer los alumnos, con material de apoyo y bibliográfico para la preparación de la materia.</p> <p>Los profesores elaborarán los materiales docentes necesarios y los colgarán en la plataforma virtual con la antelación necesaria para que los alumnos sigan cada uno de los módulos. El estudio de los materiales doctrinales, legales y jurisprudenciales se complementará con diferentes ejercicios prácticos que se llevarán a cabo en grupo o bien de forma individual, consistentes en presentaciones, tutoriales, cuadernos de trabajo, etc. Se prevé la discusión con el resto de los compañeros (chat a través de la plataforma) sobre las lecturas y materiales e incluso sobre problemas en el manejo de las aplicaciones y webinar.</p> <p>Asimismo, se prestará especial atención a la inclusión en el proceso de aprendizaje de la resolución de casos prácticos o hipótesis de situaciones reales a las que los alumnos se podrían enfrentar en el desarrollo de la capacitación de cursan.</p>				
5.4 DESCRIPCIÓN DETALLADA DE LOS MÓDULOS O MATERIAS DE ENSEÑANZA-APRENDIZAJE DE QUE CONSTA EL PLAN DE ESTUDIOS (véase ficha de cada módulo en la guía docente)				
<p>MÓDULO 1. La protección de datos en el ámbito internacional, supranacional y nacional. Normativa general y sectorial (14 créditos ECTS).</p> <p>1) Competencias y resultado del aprendizaje:</p> <ul style="list-style-type: none"> -Ofrecer una panorámica del marco jurídico de la protección de datos en el ámbito internacional, tanto a nivel legal como jurisprudencial. -Conocer exhaustivamente la nueva normativa europea y española sobre protección de datos [Reglamento (UE) General de Protección de datos. Delegados de Protección de Datos (DPD, DPO o Data Privacy Officer) y Ley Orgánica de Protección de datos personales y garantía de los derechos digitales]. -Comprender los fundamentos, principios y la legitimación del tratamiento de datos personales atendiendo a la regulación europea y española. -Conocer exhaustivamente las categorías especiales de datos, las normativas sectoriales afectadas por la protección de datos y la normativa española y europea con implicaciones en la protección de datos. -Conocer exhaustivamente los derechos de los interesados en el tratamiento de sus datos personales así como la responsabilidad del responsable y del encargado del tratamiento. Comprender las implicaciones de la responsabilidad proactiva. -Determinar la posición asignada al Delegado de Protección de Datos (DPD ó DPO) en el ámbito de una organización. Conocer exhaustivamente sus requisitos, habilidades, competencias y funciones. -Conocer y comprender las funciones desarrolladas por la Agencia Española de Protección de Datos y otras autoridades de control de ámbito autonómico y europeo. Entender sus procedimientos de cooperación y asistencia mutua. -Entender las distintas garantías de protección del tratamiento de datos personales en el marco de las transferencias 				

internacionales.

- Conocer ampliamente el procedimiento por vulneración de la normativa de protección de datos tras la formulación de denuncias.
- Determinar el régimen sancionador atendiendo a la tipología de infracciones, sanciones y multas.

Como resultado del aprendizaje el alumno/a podrá:

- Identificar la regulación jurídica, las directrices e interpretaciones y la jurisprudencia en el ámbito internacional, europeo y nacional en materia de protección de datos.
- Describir los principios en los que se fundamenta el tratamiento de datos personales según la normativa europea y española.
- Distinguir los distintos niveles de protección de datos previstos por la regulación europea y española atendiendo a las diferentes categorías de datos y al tratamiento que se aplique a los mismos, incluidas las transferencias internacionales de datos.
- Identificar en la práctica los derechos que asisten a los interesados en relación con el tratamiento de datos personales y las responsabilidades y obligaciones que competen al responsable y al encargado del tratamiento.
- Reconocer los requisitos, habilidades, competencias, funciones y obligaciones requeridas como Delegado de Protección de Datos por la normativa española.
- Identificar las autoridades de protección de datos a nivel nacional y europeo, sus funciones y relaciones entre ellas.
- Describir el procedimiento por vulneración de la normativa de protección de datos y el régimen sancionador.

2) Contenidos:

- La protección de datos en el ámbito internacional. -Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, de 23 de septiembre de 1980; Directrices para la regulación de los archivos de datos personales informatizados, adoptada mediante resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990; Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984.
- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Directrices de interpretación del Reglamento (UE) General de Protección de Datos: Guías del GT 29; Opiniones del Comité Europeo de Protección de Datos y de la Agencia Española de Protección de Datos.
- Criterios de los órganos jurisdiccionales internacionales, supranacionales y nacionales en materia de protección de datos.
- Bases jurídicas del tratamiento: licitud, lealtad y transparencia. El interés legítimo como principio legitimador del tratamiento de datos.
- Requisitos legales que posibilitan la legitimación para el tratamiento de datos personales: consentimiento, base jurídica contractual, obligación legal, interés vital del afectado, cumplimiento de fines de interés público o ejercicio de poderes públicos. El tratamiento de datos por las Administraciones Públicas.
- Principios relativos al tratamiento: principio de limitación de finalidad; principio de minimización; principio de exactitud; principio de limitación del plazo de conservación y la obligación de bloqueo; principio de integridad y confidencialidad.
- Categorías especiales de datos. Peculiaridades y límites a su tratamiento.
- Derechos de los interesados: acceso a los datos; rectificación; supresión (derecho al olvido digital), oposición, portabilidad, limitación del tratamiento, y excepciones a los derechos.
- Políticas de protección de datos y medidas de cumplimiento: intervinientes, responsabilidades, registro de actividades de tratamiento; transferencias internacionales de datos.
- Normativas sectoriales afectadas por la protección de datos: sanitaria, farmacéutica y de investigación, menores, solvencia patrimonial, videovigilancia, publicidad, etc.
- Normativa española con implicaciones en protección de datos: e-firma, comercio electrónico y telecomunicaciones.
- Normativa europea con implicaciones en protección de datos: Directiva e-Privacy sobre la privacidad y las comunicaciones electrónicas (o Reglamento e-Privacy cuando se apruebe); Directiva sobre protección de los consumidores; Directiva sobre protección respecto del tratamiento y circulación de datos personales para fines de prevención, investigación, enjuiciamiento o ejecución de infracciones penales.

- El Delegado de Protección de Datos (DPD, DPO o Data Privacy Officer): procedimiento de designación, obligaciones y responsabilidades, independencia, identificación y reporte a dirección.
- Código Ético de las personas certificadas como Delegadas de Protección de Datos conforme al Esquema de la Agencia Española de Protección de Datos.
- Procedimientos de actuación del Delegado de Protección de Datos, colaboración, autorizaciones previas, relación con los interesados, gestión de reclamaciones y comunicación con la autoridad de protección de datos.
- El Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos.
- Estatuto de la Agencia Española de Protección de Datos y procedimientos seguidos por la AEPD.
- Procedimientos por vulneración de la normativa de protección de datos; infracciones; sanciones y multas.

MÓDULO 2. Responsabilidad activa en la protección de datos personales (7 créditos ECTS)

1) Competencias y resultado del aprendizaje:

Ofrecer las bases del conocimiento del análisis, metodología y gestión de riesgos en los tratamientos de datos personales.

- Proporcionar las pautas del diseño e implantación del programa de protección de datos en el contexto de una organización y de la trazabilidad del modelo de cumplimiento (Accountability).
- Exponer el marco normativo de la Seguridad de la Información (SI), conceptos, métricas, estrategia.
- Determinar la puesta en práctica de la seguridad desde el diseño y por defecto.
- Conocer exhaustivamente el concepto, características, estándares, alcance y necesidad de la Evaluación de Impacto de Protección de Datos (EIPD) y los requisitos para la puesta en práctica de una EIPD.

Como resultado del aprendizaje el alumno/a podrá:

- Identificar y aplicar las metodologías de análisis y gestión de riesgos.
- Poner en práctica el diseño e implantación del programa de protección de datos en una organización y la trazabilidad del modelo de cumplimiento (Accountability).
- Reconocer las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información en la Unión Europea.
- Aplicar las técnicas procedentes para garantizar la ciberseguridad y el gobierno efectivo de la seguridad de la información (SI).
- Identificar el fundamento, concepto, alcance y necesidad de la Evaluación de Impacto de Protección de Datos (EIPD).
- Llevar a cabo una evaluación de impacto.

2) Contenidos:

- Análisis y gestión de riesgos de los tratamientos de datos personales. Introducción y conceptos generales.
- Evaluación de riesgos: inventario y valoración de activos; inventario y valoración de amenazas. Salvaguardas existentes y valoración de su protección. Análisis del riesgo resultante.
- Gestión de riesgos: concepto e implementación. Selección y asignación de salvaguardas a amenazas; valoración de la protección; riesgo residual, riesgo aceptable y riesgo inasumible.
- Metodologías en el análisis de gestión de riesgos.
- Cumplimiento de Protección de Datos y Seguridad en una organización: el diseño y la implantación del programa de protección de datos; objetivos del programa de cumplimiento; la trazabilidad del modelo de cumplimiento (Accountability).
- Esquema nacional de Seguridad y Directiva (NIS) (Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información en la Unión.
- Ciberseguridad y gobierno de la seguridad de la información; gobierno efectivo de la Seguridad de la Información (SI); métricas
- Estado y estrategia de la Seguridad de la Información.
- Responsabilidad proactiva: principios fundamentales de la privacidad desde el diseño y por defecto.
- Conocimiento en profundidad del ciclo de vida de los Sistemas de Información e integración de la seguridad y la privacidad en los mismos. Control de calidad de los Sistemas de Información.
- Evaluación de Impacto de Protección de Datos (EIPD). Significación, características, alcance y necesidades. Estándares de evaluación.
- Realización de una Evaluación de Impacto. Preparación y organización; análisis de la necesidad de llevar a cabo la

necesidad y consultas previas.

MÓDULO 3: Responsabilidad activa y técnicas de garantía del cumplimiento de la normativa de protección de Datos (4 créditos ECTS).

1) Competencias y resultado del aprendizaje:

- Comprender el significado de una auditoría y sus distintos alcances.
- Adquirir destreza en las implicaciones normativas dependiendo del Cliente que se audite.
- Conocimiento profundo de la normativa de protección de datos personales y sus implicaciones.
- Capacidad para poder medir detectar las deficiencias en una auditoría.
- Capacidad para auditar distintos entornos y alcances.
- Capacidad para poder acometer una auditoría.
- Conocimiento del informe de auditoría y poder llevar a cabo un modelo propio.

Como resultado del aprendizaje el alumno estará capacitado para poder tener en cuenta pautas que les ayuden a afrontar una auditoría de protección de datos personales desde el punto de vista jurídico y técnico, incorporando los aspectos relativos a la seguridad desde el diseño y por defecto.

2) Contenidos:

- La función de la Auditoría en los Sistemas de información.
- Responsabilidad proactiva y auditoría. El proceso de Auditoría: Estándares y Directrices de Auditoría de SI, acometer una auditoría, figuras intervinientes
- Principios de la auditoría y el auditor: independencia, objetividad, deber de secreto, objetividad, transparencia, acuerdo de confidencialidad.
- DPO,AUDITOR, COMPLIANCE OFFICER
- Responsabilidad proactiva vs. auditoría: Comparativa de normas estandarizadas, metodologías de análisis y gestión de riesgos, evaluación de riesgos, seguridad de los datos personales, privacidad desde el diseño y por defecto.
- Diseñar-implementar-eficacia modelo GDPR.
- Auditoría ISO 19011
- ISO 27001 y protección de datos.
- Informe y dictamen de auditoría.
- Violaciones de seguridad y evaluaciones de impacto.
- Sistemas de control de acceso físico y lógicos.
- Sistemas de registros de acceso (datos primarios y secundarios).
- Sistemas de identificación y autenticación (principales plataformas)
- Sistemas de gestión en soportes físicos y virtuales.
- Sistemas de acceso remotos.
- Copias de respaldo y recuperación.
- Tecnologías de cifrado y anonimización.
- Auditar la existencia de Privacy Enchancing Technologies.
- Auditar si los tratamientos cumplen Privacy by Design y Privacy by Default.
- Auditorías de entornos Pay for Privacy.

TRABAJO FINAL (5 créditos ECTS).

Estudio desarrollado por el alumno bajo la tutela de un Profesor con el grado de Doctor, de los que imparten docencia en el Diploma.

El trabajo consistirá en el análisis crítico de un aspecto o problemática relacionados con el programa cursado en el Diploma o bien en la demostración del grado de dominio de una de las competencias relacionadas con los contenidos del Programa del Diploma.

El trabajo será defendido por el alumno ante un Tribunal integrado por Profesores con el grado de Doctor de entre los que imparten docencia en el Diploma distintos del tutor.

5.5 PRÁCTICAS EXTERNAS (CURRICULARES O EXTRACURRICULARES)

Empresa/Entidad	Conven	Nº de plazas	Periodo de realización
-----------------	--------	--------------	------------------------

	io vigente	disponibles			
NO SE CONTEMPLAN EN ESTA EDICIÓN					
5.6. TRABAJO FINAL					
<p>Estudio desarrollado por el alumno bajo la tutela de un Profesor con el grado de Doctor, de los que imparten docencia en el Diploma.</p> <p>El trabajo consistirá en el análisis crítico de un aspecto o problemática relacionados con el programa cursado en el Diploma o bien en la demostración del grado de dominio de una de las competencias relacionadas con los contenidos del Programa del Diploma.</p> <p>El trabajo será defendido por el alumno ante un Tribunal integrado por Profesores con el grado de Doctor de entre los que imparten docencia en el Diploma distintos del tutor.</p> <p>La puntuación del Trabajo Final constituirá un 13,33% de la Calificación final del Diploma</p>					
6. PROFESORADO Y OTROS RECURSOS HUMANOS NECESARIOS PARA LLEVAR A CABO EL PLAN DE ESTUDIOS					
Apellidos	Nombre	Categoría profesional	Institución/ Empresa	Nº ECTS asignados presenciales	Nº ECTS asignados virtuales
Serrano Fernández	María	Catedrática de Universidad (Grado Doctor)	Universidad Pablo de Olavide		2
Díaz Gómez	Manuel Jesús	Profesor Titular de Universidad (Grado Doctor)	Universidad de Huelva		2
Ruiz Tarrias	Susana	Profesora Titular de Universidad (Grado Doctor)	Universidad de Granada		3
López San Luis	Rocío	Profesora Titular de Universidad (Grado Doctor)	Universidad de Almería		2

Valls Prieto	Javier	Profesor Titular de Universidad (Grado Doctor)	Universidad de Granada		2
Sánchez Barrilao	Juan Francisco	Profesor Titular de Universidad (Grado Doctor)			1
Bobo Ruiz	Jesús	Profesor Colaborador Indefinido	Universidad de Granada		1
Orza Linares	Ramón María	Profesor Contratado Doctor (Grado Doctor)	Universidad de Granada		3
López-Vidriero Tejedor	Icár	Licenciada en Derecho	Abogada colegiada del ICAM		2
Margarit	Genís	Ingeniero de Telecomunicaciones e Ingeniero de sistemas electrónicos.	Profesor Universidad Pompeu Fabra e Instructor de las certificaciones EC-Council, Microsoft y Cisco		2
Muñoz Ropa	Antonio	Licenciado en Informática	Universidad de Granada		2
Álvarez Bermejo	José Antonio	Profesor Titular de Arquitectura y Tecnología de Computadores (Grado Doctor)	Universidad de Almería		1
Gómez Romero,	Juan	Profesor Titular de Ciencias de la Computación e IA (Grado Doctor)	Universidad de Granada		2

7. CRONOGRAMA DEL DESARROLLO DEL CURSO

Módulo	Materia/Asignatura	Profesor/a	Nº de ECTS presenciales	Nº de ECTS virtuales	Fecha inicio	Fecha final
Nº1: La protección de datos en el ámbito internacional,	-Contexto normativo. RGPD y LOPDGDD. Fundamentos y principios	Ramón María Orza Linares		14	01/12/2020	12/03/2021

supranacional y nacional. Normativa general y sectorial	-RGPD y LOPDGDD. Legitimación y derechos de los interesados	Rocío López San Luis				
	-El DPD. Designación y competencias	Manuel Jesús Díaz Gómez				
	-Autoridades de control y directrices de interpretación del RGPD	Susana Ruiz Tarrías				
	-Transferencias internacionales de datos. Normativa española y europea con implicaciones en la protección de datos	Susana Ruiz Tarrías				
	-Normativas sectoriales afectadas por la protección de datos	Jesús Bobo Ruiz Juan Francisco Sánchez Barrilao				
	-Procedimientos por vulneración de la normativa de protección de datos y régimen sancionador	María Serrano Fernández				
Nº2: Responsabilidad activa en la protección de datos personales	-Análisis y gestión de riesgos de los tratamientos de datos personales. Metodología y programa de cumplimiento en una organización	Antonio Muñoz Ropa		7	15/03/2021	07/05/2021
	-Seguridad de la información. Marco normativo. Ciberseguridad y gobierno de la SI	Javier Valls Prieto				

	-Puesta en práctica de la SI. Control de calidad. Seguridad por diseño y por defecto	José A. Álvarez Bermejo				
	-Evaluación de Impacto de Protección de Datos (EIPD)	Juan Gómez Romero				
Nº3: Responsabilidad activa y técnicas de garantía del cumplimiento de la normativa de protección de Datos	-La función de la auditoría en los SI. Estándares y directrices de auditoría de SI. -Principios de la auditoría	Icía López-Vidriero Tejedor		4	10/5/2021	2/07/2021
	-La auditoría: técnicas de auditoría	Genís Margarit				
Trabajo Final		Tutor Asignado por la Comisión Académica de entre sus miembros		5	7/7/2021	14/7/2021
8. RECURSOS MATERIALES Y SERVICIOS						
8.1 JUSTIFICACIÓN DE LA ADECUACIÓN DE LOS MEDIOS MATERIALES Y SERVICIOS DISPONIBLES						
<p>La Plataforma virtual permite la impartición del Diploma con carácter 100% virtual, a través de la utilización de recursos como subida de archivos de contenidos, cuaderno de trabajo del estudiante, controles y exámenes tipo test, uso de webinar, chats individuales o de grupo entre los estudiantes y el profesorado, tutorías online, etc.</p>						
8.2 PREVISIÓN DE ADQUISICIÓN DE RECURSOS MATERIALES Y SERVICIOS NECESARIOS, EN SU CASO						
<p>En tanto que el Diploma se plantea 100% on line, no se prevé la necesidad de adquisición de equipamiento. En todo caso, podrán ser requeridos servicios de traducción inglesa de documentos jurídicos internacionales o europeos que no dispongan versión en español.</p>						
8.3 INFORMACIÓN SOBRE ENSEÑANZA VIRTUAL PARA MODALIDAD SEMIPRESENCIAL Y VIRTUAL, EN SU CASO						

<input checked="" type="checkbox"/> Uso del Campus Virtual de la UNIA	
<input checked="" type="checkbox"/> Conozco los mínimos en cuanto a funciones docentes y recursos de aprendizaje en red del modelo de enseñanza-aprendizaje virtual de la UNIA (para más información, consúltese la <u>GUÍA SOBRE ENSEÑANZA-VIRTUAL EN LA UNIA</u>)	
9. PRESUPUESTO DE INGRESOS Y GASTOS	
9.1 VALORES CUANTITATIVOS ESTIMADOS DE INGRESOS	
9.2 VALORES CUANTITATIVOS ESTIMADOS DE GASTOS	
10. RESULTADOS PREVISTOS (valores cuantitativos estimados para los indicadores y su justificación)	
- Tasa de graduación prevista	95 %
- Introducción de nuevos indicadores (en su caso)	
Denominación:	
Definición:	
Valor:	
Justificación de las estimaciones realizadas:	
11. CRONOGRAMA PREVISTO DE IMPLANTACIÓN DEL TÍTULO	
Inicio del plazo de preinscripción:	
Fin del plazo de preinscripción:	30/06/2020
Inicio del plazo de matrícula:	06/07/2020
Fin del plazo de matrícula:	15/09/2020
Inicio del curso:	01/12/2020
Finalización del curso:	Defensa Trabajo Final de Diploma 6/09/2021-10/09/2021
En Granada, a 6 de Marzo de 2020.	
Fdo.: Susana Ruiz Tarrías	

Conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal (Reglamento (UE) 2016/679, de 27 de abril) le informamos que los datos personales que nos ha facilitado pasarán a ser tratados por la UNIVERSIDAD INTERNACIONAL DE ANDALUCÍA como responsable del tratamiento, siendo órgano competente en la materia la Dirección del Área de Gestión Académica (Monasterio Santa María de las Cuevas, C/ Américo Vespucio nº2. Isla de La Cartuja. 41092 Sevilla) ante quien Vd. puede ejercitar sus derechos de acceso, rectificación, limitación, oposición o portabilidad señalando concretamente la causa de su solicitud y acompañando copia de su documento acreditativo de identidad. La solicitud podrá hacerse mediante escrito en formato papel o por medios electrónicos.

Caso de no obtener contestación o ver desestimada su solicitud puede dirigirse al Delegado de Protección de Datos de la Universidad (rgpd@unia.es; Tfno. 954462299) o en reclamación a la Agencia Española de Protección de Datos a través de los formularios que esa entidad tiene habilitados al efecto y que son accesibles desde su página web: <https://sedeagpd.gob.es>. Como responsable, la Universidad le informa que exclusivamente tratará los datos personales que Ud. le facilite para dar cumplimiento a los siguientes fines:

a) Gestión académica y administrativa de:

- Participación en procesos de acceso y admisión a las enseñanzas oficiales (Grado, Máster y Doctorado) o de formación Continua de la Universidad Internacional de Andalucía.
- Inscripción y/o matrícula como alumno en cualquiera de las titulaciones oficiales (Grado, Máster y Doctorado), Formación Continua u otras actividades académicas ofrecidas por la Universidad Internacional de Andalucía.
- Participación en convocatorias de becas y ayudas al estudio de la Universidad Internacional de Andalucía, la Admón. General del Estado o la de las Comunidades Autónomas y de otras entidades públicas o privadas.
- Participación en convocatorias de programas de movilidad de carácter nacional o internacional.
- Obtención y expedición de títulos oficiales, títulos propios y otros títulos académicos.

b) Gestión de su participación como estudiante en prácticas y actividades formativas nacionales o internacionales en instituciones, empresas, organismos o en otros centros.

c) Utilización de servicios universitarios como obtención del carné universitario, bibliotecas, actividades deportivas u otros.

La Universidad se encuentra legitimada para tratar estos datos al ser necesarios para la ejecución de la relación jurídica establecida entre Ud. y la Universidad y para que ésta pueda cumplir con sus obligaciones legales establecidas en la Ley Orgánica 6/2001, de Universidades.

Usted responde de la veracidad de los datos personales que ha proporcionado a la Universidad y de su actualización.

La Universidad comunicará los datos personales que sean indispensables, y nunca en otro caso, a las siguientes categorías de destinatarios:

- A otras Administraciones y organismos públicos para el ejercicio de las competencias que les sean propias y compatibles con las finalidades arriba enunciadas (Así -a modo enunciativo y no limitativo- a Ministerios con competencias en educación y ciencia, a otras administraciones, a otras Universidades o Centros formativos equivalentes para la gestión de traslados, a empresas para la realización de prácticas).
- A entidades bancarias para la gestión de pagos y cobros.
- A organismos públicos o privados en virtud de la celebración de convenios de colaboración o contratos, conforme a lo dispuesto en la legislación vigente en materia de Protección de Datos.
- A los servicios de la propia Universidad que sean adecuados para gestionar la utilización de los servicios universitarios ofertados.

Sus datos de carácter personal se tratarán y conservarán por la Universidad conforme a la legislación vigente en materia de protección de datos, pasando luego a formar parte -previo expurgo- del Archivo Histórico Universitario conforme a lo dispuesto en la legislación sobre Patrimonio Histórico.

La Universidad sólo prevé la transferencia de datos a terceros países en el caso de su participación como alumno en alguno de los programas de formación o becas de carácter internacional. La transferencia se realizará siguiendo las directrices establecidas al respecto por el Reglamento Europeo de Protección de Datos y normativa de desarrollo.

El Servicio de Protección de Datos de la Universidad Internacional de Andalucía cuenta con una página en la que incluye legislación, información y modelos en relación con la Protección de Datos Personales a la que puede acceder desde el siguiente enlace: <https://www.unia.es/protecciondatos>.