



DIPLOMA DE ESPECIALIZACIÓN

**CÓDIGO
0500**

Protección de Datos en la Sociedad Digital

Modalidad Virtual, de 1 de diciembre de 2020 a 10 de septiembre de 2021.

DIRECCIÓN

Dr. Manuel Jesús Díaz Gómez. Univ. de Huelva

Dra. Susana Ruiz Tarrías. Univ. de Granada



Rectorado. SEDE DE LA CARTUJA, Sevilla

@ UNIAuniversidad
#UNIAPOSG

PRESENTACIÓN Y OBJETIVOS

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 “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 (...)”.

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.

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)].

Sin embargo, al mismo tiempo, internet se convierte en un ámbito en el que los derechos de los ciudadanos 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 cualificación 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.

Nº DE PLAZAS

30 plazas

REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

Requisitos de Acceso

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.

Criterios de Admisión

Las solicitudes presentadas para cursar el Diploma de Especialización en 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.

Excepcionalmente, a petición del interesado, la Comisión de Postgrado podrá autorizar una matrícula condicional para aquellos estudiantes que acrediten que han superado el menos el noventa por ciento de los créditos de una de las titulaciones requeridas, excluyendo el Trabajo Fin de Grado y las prácticas externas.

En esta situación la obtención del título queda condicionada a que el solicitante cumpla los requisitos de acceso al título propio de postgrado en un plazo que no podrá ser superior a los dos años contados desde la fecha de terminación de los estudios (Rgtº E. P. y F. C. UNIA)

PROGRAMA ACADÉMICO

30 ECTS, distribuidos en los siguientes Módulos:

Módulo 1. La protección de datos en el ámbito internacional, supranacional y nacional. Normativa general y sectorial (14 ECTS).

01/12/2020 al 12/03/2021

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

15/03/2021 al 07/05/2021

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

10/05/2021 al 02/07/2021

Trabajo Final (5 ECTS)

07/07/2021 a 10/09/2021

PROFESORADO

D. Manuel Jesús Díaz Gómez (Universidad de Huelva)

Dª. Susana Ruiz Tarrias (Universidad de Granada)

Dª. Rocío López San Luis (Universidad de Almería)

D. Javier Valls Prieto (Universidad de Granada)

D. Juan Francisco Sánchez Barrilao
(Universidad de Granada)

D. Jesús Bobo Ruiz (Universidad de Granada)

D. Ramón María Orza Linares (Universidad de Granada)

D^a. Iciar López-Vidriero Tejedor (Abogada colegiada del ICAM)

D. Genís Margarit (Universidad Pompeu Fabra)

D. Antonio Muñoz Ropa (Universidad de Granada)

D. José Antonio Álvarez Bermejo (Universidad de Almería)

D. Juan Gómez Romero (Universidad de Granada)

ADMISIÓN Y MATRÍCULA

Los interesados deberán realizar las siguientes gestiones:

1.- Solicitar la admisión a través de <https://portal.unia.es>

2.- Remitir a la dirección de correo electrónico alumnos.sevilla@unia.es la documentación que se relaciona a continuación:

- Fotocopia del DNI.
- Fotocopia compulsada del Título Académico que da acceso al Programa o resguardo acreditativo de haber abonado los derechos de expedición del mismo, y, en su caso,
- Acreditación de experiencia profesional previa en materia de protección de datos y/o acreditación oficial de la misma.

Una vez que se haya comprobado su solicitud y su documentación, se validará la misma y los admitidos deberán formalizar la matrícula a través del procedimiento on-line disponible en la dirección:

<http://www.unia.es/automatricula>

El plazo para realizar la matrícula finaliza el **15 de noviembre de 2020**.

Una vez que el alumno haya formalizado su matrícula, deberá remitir el justificante de haber abonado la misma a alumnos.sevilla@unia.es

IMPORTE Y PAGO

Precios públicos por servicios académicos y administrativos:

- Matrícula: 450,00 € (15,00 €/crédito).
- Apertura de expediente: 40,00 €.
- Expedición tarjeta de identidad: 4,50 €.

Una vez superados los 30 ECTS, los alumnos podrán solicitar:

- Certificado académico.
- Expedición de Título.

El abono del importe de la matrícula (494,50 €) se podrá realizar en un único pago, al formalizar la matrícula; o fraccionarlo en dos plazos. El primero de ellos, correspondiente al 50% del importe de la matrícula y las tasas administrativas (269,50 euros) en el momento de formalizar la matrícula; el segundo, correspondiente al otro 50% del importe (225,00 euros), antes del 15 de febrero de 2021. El importe de la matrícula podrá abonarse mediante ingreso en efectivo, domiciliación bancaria o mediante transferencia en la cuenta bancaria que se indica a continuación, haciendo constar el nombre y apellidos del alumno y la actividad académica (0500 - Diploma de Especialización en Protección De Datos En La Sociedad Digital)

CUENTA: LA CAIXA:

IBAN:ES7821009166752200074348

SWIFT: CAIXESBBXXX.

Los gastos que generen las operaciones bancarias serán por cuenta de los interesados.



INFORMACIÓN E INSCRIPCIÓN

<https://www.unia.es/>



Universidad Internacional de Andalucía. Sede La Cartuja de Sevilla. Monasterio Santa María de las Cuevas. Isla de la Cartuja 41092. Sevilla. Telf.: (0034) 954 462 299 sevilla@unia.es - www.unia.es