TÍTOLS PROPIS
VNIVERSITAT DE VALÈNCIA

Experto Universitario Online en el Reglamento General de Protección de Datos: Delegado de Protección de Datos en las Administraciones Públicas. 1.ª Edición.
Código: 18223540

DATOS GENERALES

Curso académico	
Tipo de curso	Experto Universitario
Número de créditos	15,00 Créditos ECTS
Matrícula	600 euros (importe precio público)
Requisitos de acceso	Funcionarios Públicos. Estudiantes y Público en general. □ Título oficial español o extranjero que otorgue acceso a enseñanzas oficiales de postgrado □ Estudiantes a los que les quede menos de un 10% para obtener su título de grado, condicionados a la obtención del título en el mismo año académico. □ Profesionales del ámbito
Modalidad	On-line
Lugar de impartición	Aula Virtual
Horario	Aula Virtual

Dirección

Organizador	Facultat de Dret
Colaborador	Institut Valencià d'Administració Pública
Dirección	Ricard Martínez Martínez Dr. Profesor Departamento de Derecho Constitucional, Titular Cátedra Microsoft. Universitat de Valencia. Ha sido Presidente de APEP. Lorenzo Cotino Hueso Catedrático Derecho Constitucional, Universitat de València. Coordinador Red www.derechotics.com, Magistrado TSJ C. Valenciana (2000-19). Consejo Transparencia C. Valenciana.

Plazos

Preinscripción al curso	Hasta 18/10/2018
Fecha inicio	Noviembre 2018
Fecha fin	Abril 2019

Más información

Teléfono	961 603 000
E-mail	informacion@adeituv.es

PROGRAMA

El marco constitucional y europeo de la protección de datos. Normativa general de Proteccion de datos

1.1 La conformación de un derecho fundamental a la protección de datos de los ciudadanos de la Unión Europea por el Tribunal de Justicia.

1.2 Aspectos generales del Reglamento General de Protección de Datos. A) Antecedentes y fundamento de la normativa. B) Conceptos y definiciones. C) Los ámbitos subjetivo, material y territorial de aplicación. Exclusiones.

1.3 Principios de protección de datos. A) La legitimación para el tratamiento: aspectos generales. El consentimiento explícito. Datos sujetos a especial protección. Datos de menores. El contrato. Deberes e intereses públicos; legitimación atribuida por una norma, las administraciones públicas y la concurrencia de interés público. El interés legítimo. B) El principio de finalidad. Uso para fines no incompatibles. El uso de datos personales con fines históricos, estadísticos y de investigación.

1.4 Los derechos del ciudadano. A. Acceso. B. Rectificación. C. Cancelación, supresión y derecho al olvido. D. Limitación del tratamiento. Notificaciones a terceros de la supresión y limitación del tratamiento. E. Portabilidad. F. Oposición al tratamiento. G. Excepciones a los derechos. H. La gestión de los ejercicios de derechos.1.Dominio 1. NORMATIVA GENERAL DE PROTECCIÓN DE DATOS.
(Porcentaje temario: 50%)

1.1. Contexto normativo.
1.1.1. Privacidad y protección de datos en el panorama internacional.

1.1.2. La protección de datos en Europa.
1.1.3. La protección de datos en España.
1.1.4. Estándares y buenas prácticas.
Implica: repaso breve APEC, nuevo convenio 108 y OCDE Privacy Guidelines. Adicionalmente referencias a EEUU y espacio iberoamericano de protección de datos.

1.2. El Reglamento Europeo de Protección de datos y actualización de LOPD. Fundamentos.
1.2.1. Ámbito de aplicación.
1.2.2. Definiciones.
1.2.3. Sujetos obligados.
1.3. El Reglamento Europeo de Protección de datos y actualización de LOPD. Principios

1.3.1. El binomio derecho/deber en la protección de datos.
1.3.2. Licitud del tratamiento
1.3.3. Lealtad y transparencia
1.3.4. Limitación de la finalidad
1.3.5. Minimización de datos
1.3.6. Exactitud

1.4. El Reglamento Europeo de Protección de datos y actualización de LOPD. Legitimación
1.4.1. El consentimiento: otorgamiento y revocación.
1.4.2. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado.
1.4.3. Consentimiento de los niños.
1.4.4. Categorías especiales de datos.
1.4.5. Datos relativos a infracciones y condenas penales.
1.4.6. Tratamiento que no requiere identificación.
1.4.7. Bases jurídicas distintas del consentimiento.
1.5. Derechos de los individuos.
1.5.1. Transparencia e información
1.5.2. Acceso, rectificación, supresión (olvido).
1.5.3. Oposición
1.5.4. Decisiones individuales automatizadas.
1.5.5. Portabilidad.
1.5.6. Limitación del tratamiento.
1.5.7. Excepciones a los derechos.
1.6. El Reglamento Europeo de Protección de datos y actualización de LOPD. Medidas de cumplimiento.
1.6.1. Las políticas de protección de datos.
1.6.2. Posición jurídica de los intervinientes. Responsables, co-responsables, encargados, subencargado del tratamiento y sus representantes. Relaciones entre ellos y formalización.
1.6.3. El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos.
1.7. El Reglamento Europeo de Protección de datos y actualización de LOPD. Responsabilidad proactiva.
1.7.1. Privacidad desde el diseño y por defecto. Principios fundamentales.
1.7.2. Evaluación de impacto relativa a la protección de datos y consulta previa. Los tratamientos de alto riesgo.
1.7.3. Seguridad de los datos personales. Seguridad técnica y organizativa.
1.7.4. Las violaciones de la seguridad. Notificación de violaciones de seguridad.
1.7.5. El Delegado de Protección de Datos (DPD). Marco normativo.
1.7.6. Códigos de conducta y certificaciones.
1.8. El Reglamento Europeo de Protección de datos. Delegados de Protección de Datos (DPD, DPO o Data Privacy Officer).
1.8.1. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses.
1.8.2. Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección.
1.8.3. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones.
1.8.4. Comunicación con la autoridad de protección de datos.
1.8.5. Competencia profesional. Negociación. Comunicación. Presupuestos.
1.8.6. Formación.
1.8.7. Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.
(Inicialmente me planteo si Joaquín Martín Cubas al menos el punto 5 y el 8, hablamos aquí de liderazgo, gestión de proyectos, gestión de equipos).
1.9. El Reglamento Europeo de Protección de datos y actualización de LOPD. Transferencias internacionales de datos

1.9.1. El sistema de decisiones de adecuación.
1.9.2. Transferencias mediante garantías adecuadas.
1.9.3. Normas Corporativas Vinculantes
1.9.4. Excepciones.
1.9.5. Autorización de la autoridad de control.
1.9.6. Suspensión temporal
1.9.7. Cláusulas contractuales1.10. El Reglamento Europeo de Protección de datos y actualización de LOPD. Las Autoridades de Control.
1.10.1. Autoridades de Control.
1.10.2. Potestades.
1.10.3. Régimen sancionador.
1.10.4. Comité Europeo de Protección de Datos.
1.10.5. Procedimientos seguidos por la AEPD.
1.10.6. La tutela jurisdiccional.

1.10.7. El derecho de indemnización.

1.11. Directrices de interpretación del RGPD.
1.11.1. Guías del GT art. 29.
1.11.2. Opiniones del Comité Europeo de Protección de Datos
1.11.3. Criterios de órganos jurisdiccionales.

1.12. Normativas sectoriales afectadas por la protección de datos.
1.12.1. Sanitaria, Farmacéutica, Investigación.
1.12.2. Protección de los menores
1.12.3. Solvencia Patrimonial
1.12.4. Telecomunicaciones
1.12.5. Videovigilancia
1.12.6. Seguros
1.12.7. Publicidad, etc.
1.13. Normativa española con implicaciones en protección de datos.
1.13.1. LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
1.13.2. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
1.13.3. Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica
1.14. Normativa europea con implicaciones en protección de datos.
1.14.1. Directiva e-Privacy: 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 (Directiva sobre privacidad y las comunicaciones electrónicas) o Reglamento e-Privacy cuando se apruebe.
1.14.2. 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.
1.14.3. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

La responsabilidad activa.

2.1 Las posiciones responsables, encargados, corresponsables, responsable no establecido en la UE.
2.2 Diligencia y responsabilidad: la llamada accountability: a. Identificación de los tratamientos y registro de actividades.
b. Protección de datos desde el diseño y por defecto. c. La identificación de riesgos en el tratamiento: análisis de impacto en el derecho fundamental a la protección de datos: principios jurídicos. d. El deber de transparencia. e. Cesiones de datos y deberes específicos.
2.4. El encargado del tratamiento. a. Diligencia en la elección. Códigos de conducta y certificación.
2.5. Deberes de seguridad: la notificación de violaciones.
2.6 Transferencias internacionales. a. País seguro. b. Cláusulas contractuales. c. Binding Corporate Rules. BCR. d. Excepciones a las reglas generales. e. Tutela, cooperación y asistencia mutua entre autoridades de protección de datos personales. f. Funciones de la Comisión.Dominio 2. RESPONSABILIDAD ACTIVA.
(Porcentaje temario: 30%)
2.1.Análisis y gestión de riesgos de los tratamientos de datos personales.
2.1.1.Introducción. Marco general de la evaluación y gestión de riesgos. Conceptos generales.
2.1.2.Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante.
2.1.3.Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible.
2.2. Metodologías de análisis y gestión de riesgos.
2.3. Programa de cumplimiento de Protección de Datos y Seguridad en una organización.
2.3.1. El Diseño y la implantación del programa de protección de datos en el contexto de la organización.
2.3.2. Objetivos del programa de cumplimiento.
2.3.3. Accountability: La trazabilidad del modelo de cumplimiento.
2.4. Seguridad de la información.
2.4.1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos.
2.4.2. Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Seguridad de la Información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI.
2.4.3. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.
2.5. Evaluación de Impacto de Protección de Datos EIPD.
2.5.1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares.
2.5.2. Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas.

Técnicas para garantizar el cumplimiento de la normativa de protección de datos y otros conocimientos (I)

3.1 Las técnicas de protección de datos desde el diseño y por defecto. La implementación de software, procesos y procedimientos basados en privacidad.
3.2 El análisis de riesgos y las evaluaciones de impacto en la protección de datos.
3.3 Los planes de implementación de cumplimiento del Reglamento General de Protección de Datos. Gestión basada en

procesos: el compliance.
3.4 Tecnologías de la información: nociones básicas. A. Los sistemas de información condiciones de desarrollo de bases de datos y entornos informáticos. B. Tecnologías emergentes: Big Data, RFID, Inteligencia Artificial, Block Chain, APPS, Internet de los objetos, Smart Cities.
3.5 Conceptos básicos de seguridad en ficheros y tratamientos. A. Seguridad desde el diseño. B. Estándares normativos de seguridad: del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos al esquema nacional de seguridad.
C. Estándares de seguridad. Códigos de conducta y certificaciones. D. Los roles y deberes en seguridad. E. La gestión de procedimientos de notificación de violaciones de seguridad. F. La Directiva NIS.Dominio 3. TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS.
(Porcentaje temario: 20%)
3.1. La auditoría de protección de datos.
3.1.1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la Auditoría.
3.1.2.Elaboración del informe de auditoría. Aspectos básicos e importancia del informe de auditoría.
3.1.3.Ejecución y seguimiento de acciones correctoras.

3.2.Auditoría de Sistemas de Información.
3.2.1. La Función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices de Auditoría de SI.
3.2.2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoria de protección de datos en la auditoria de SI.
3.2.3. Planificación, ejecución y seguimiento.

3.3. La gestión de la seguridad de los tratamientos.

3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI).
3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación.
3.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres.

3.4. Otros conocimientos.
3.4.1. El cloud computing.
3.4.2. Los Smartphones.
3.4.3. Internet de las cosas (IoT).
3.4.4. Big data y elaboración de perfiles.
3.4.5. Redes sociales
3.4.6. Tecnologías de seguimiento de usuario
3.4.7. Blockchain y últimas tecnologías

Técnicas para garantizar el cumplimiento de la normativa de protección de datos y otros conocimientos (II)

4.1 Delegado de protección de datos. Funciones y capacitación. Las relaciones con la Agencia Española de Protección de Datos.
4.2 Códigos de conducta y certificaciones.
4.3 Tutela de los derechos. Las Autoridades de protección de datos (I). Las autoridades subnacionales. Competencias: a. Potestad de inspección. b. Deber de cooperación. c. Acceso al registro de actividades. d. Violaciones de seguridad. e. Evaluaciones de impacto y autorizaciones previas. f. Transferencias internacionales de datos personales: tutela, cooperación y asistencia mutua. h. Acciones de promoción y sensibilización.
4.3 Tutela de los derechos. Las Autoridades de protección de datos (II). El procedimiento (One Stop Shop). a. Infracciones y sanciones. b. Reclamaciones ante una autoridad. C. Mecanismos de cooperación, asistencia mutua y coherencia.
4.4. El acceso a la Jurisdicción. a. Aspectos procedimentales. b. Derecho de indemnización. c. Recurso frente a resoluciones de una autoridad de control. d. Recurso frente a resoluciones del Comité.
4.5 El Comité. Marco general. Estructura y funciones. a. Composición. b. Independencia. c. Funciones. d. Procedimiento. e. Estructura. f. Mecanismo de coherencia. g. Dictamen del Comité. h. Resolución de conflictos por el Comité. i. Procedimiento de urgencia. j. Intercambio de información. k. Recursos ante el TJUE frente al Comité.
4.6 Competencias de la Comisión Europea. a. Actos de ejecución. b. Informe y revisión del GDPR. c. Otras competencias.

Normativa sectorial: la protección de datos en el sector público

5. 1. Transparencia, acceso a la información pública y reutilización.
5.2 Protección de datos en la administración electrónica.
5.3 Archivo, investigación histórica, estadística y científica.
5.4 Fuerzas y cuerpos de seguridad: videovigilancia.
5.5 Ficheros de salud y servicios sociales.
5.6 Gestión de datos en entornos escolares.
5.7 La gestión de personal.
5.8. Retos de futuro:
a. La gestión de servicios en la nube.
b. Big data. La analítica basada en datos personales. c. Internet de las Cosas y Smart Cities.

PROFESORADO

Mónica Arenas Ramiro

Dra. Profesora de Derecho Constitucional. U. Alcalá. Premio Tesis doctoral por la AGPD 2005

Andrés Boix Palop

Professor Titular de Dret Administratiu. Universitat de València..

Joaquín Cañada González

Diputación Provincial de Valencia

Lorenzo Cotino Hueso

Catedrático de Derecho Constitucional. Coordinador de www.derechotics.com.

Ana María de la Encarnación Valcárcel

Ayudante/a Doctor/a. Departament de Dret Administratiu i Processal. Universitat de València

Joaquín Martín Cubas

Contratado/a Doctor/a. Departament de Dret Constitucional, Ciència Política i de l'Administració. Universitat de València

Ricard Martínez Martínez

Dr. Profesor Departamento de Derecho Constitucional, Titular Cátedra Microsoft. Universitat de Valencia. Ha sido Presidente de APEP.

Consuelo Reyes Marzal Raga

Prof. Titular de Derecho Administrativo. Universitat de València.

Alfonso Ortega Giménez

Dr. Profesor Derecho Internacional Privado, Vicedecano (Facultad de Ciencias Sociales y Jurídicas de Elche). Tesis premiada por la AGPD 2014

Carmen Serrano Durba

Ingeniera Informática U. Politécnica de Valencia, técnico informática de de Seguridad Generalitat Valenciana

Juan Miguel Signes Andreu

Responsable de Seguridad de la información en la Conselleria de Sanitat Generalitat Valenciana. Ha sido residente del capitulo ISACA Valencia

OBJETIVOS

Las salidas profesionales que tiene el curso son:

Delegado de Protección de datos, con especial incidencia en las administraciones públicas.

ª Proveer a las administraciones públicas de profesionales para el desempeño de la función de delegado de protección de datos.
ª Capacitar a los profesionales con un conocimiento profundo 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 (RGPD).
ª Dotar a las personas formadas de las competencias necesarias para el despliegue funcional que define el RGPD:
a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;
d) cooperar con la autoridad de control;
e) actuar como punto de contacto de la autoridad de control;

METODOLOGÍA

Introducir el siguiente texto.
La docencia se estructura en dos bloques y fases básicos, a saber:
Fase 1: Aprendizaje del marco general
Unidad 1. El marco constitucional y europeo de la protección de datos. Normativa general de Protección de datos.
Unidad 2. La responsabilidad activa.
Unidad 5. Normativa sectorial: la protección de datos en el sector público.

Fase 2: Herramientas para el despliegue de las funciones del DPO
Unidad 3. Técnicas para garantizar el cumplimiento de la normativa de protección de datos y otros conocimientos (I).
Unidad 4. Técnicas para garantizar el cumplimiento de la normativa de protección de datos y otros conocimientos (II).
En cada fase se desarrollará el autoaprendizaje del alumnado a partir de los materiales, videos, webinars y cada fase contará los espacios temáticos en el aula con foros de dudas y participación.
De igual modo en cada fase se llevará a cado el sistema de evaluación con test e informe teórico práctico.
Test. La evaluación constará de una parte, de preguntas tipo test alineadas con las de la certificación de la Agencia Española de Protección de Datos. Así, se llevarán a cabo preguntas vinculadas a los tres Dominios temáticos señalados por la AGPD, repartiendo entre preguntas teóricas (75%) así como preguntas con escenario en el que se plantea un caso práctico (25%).
Informe teórico práctico. Además del test, respecto de la primera y segunda parte de la asignatura cada alumno realizará un informe teórico práctico. Dicho informe alcanzará todos los aspectos de las asignaturas, si bien se integrarán en un documento que remitira cada alumno respecto de la primera y segunda parte del curso. Una vez acabado el periodo de entrega se contará con una retroalimentación de la actividad.