NOMBRE DEL CURSO:

Curso Delegado de Protección de Datos

DURACIÓN: 180 HORAS

Director/a

Ainhoa Juárez Carreño

Letrada colegiada en el Ilustre Colegio de Abogados de Madrid, Máster de Práctica Jurídica en Centro de Estudios e Investigaciones Jurídicas Madrid (CEIJ).

Cuenta con una larga experiencia en procesos judiciales de diferentes materias y especialidades.

Experta reconocida por el Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias del Banco de España.

Con amplia experiencia en normativas relativas al cumplimiento normativo empresarial (compliance) y nuevas tecnologías, ha escrito e impartido diversos cursos relativos a estas materias, formando a auditores, consultores y redes comerciales.

Dirige durante años, proyectos de valoración de puestos de trabajo, sucesión en pymes, protocolos en las empresas familiares, fusiones y escisiones de empresas, impartiendo además formación en las citadas materias, formando a formadores.

Destaca su carrera profesional desde hace 15 años en entidades relacionadas con la empresa en el ámbito de la privacidad y las nuevas tecnologías, llegando a ocupar puestos de relevancia en todas ellas.

Su anterior desempeño profesional se desarrolló en la Fundación Española para la Protección de Datos, dirigiendo el departamento jurídico y consultoría técnica.

Posee la certificación IRCA (International Register of Certificated Auditors). Es Delegada de Protección de Datos certificada según el Esquema de la Agencia Española de Protección de Datos.

En materia de Prevención del Blanqueo de Capitales y Financiación del Terrorismo, ha elaborado distintos cursos y desarrollado el primer software específico de aplicación de esta normativa en los sujetos obligados.

Codirige e imparte como ponente la formación de preparación de Delegados de Protección de Datos del Ilustre Colegio de Abogados de Madrid ICAM.

Director/a

Jorge Badiola Guerra

Profesional con más de 20 años de experiencia en el área de gestión y dirección empresarial, realizó sus estudios de Ciencias Empresariales en la Universidad Complutense de Madrid.

Desde el año 1992, comenzó su andadura empresarial en diversos ámbitos hasta que finalmente, se especializó en las nuevas tecnologías, su aplicación normativa y de seguridad de la información.

Pionero desde la entrada de internet en España, en al año 1994 desarrolló su primer sitio web, evolucionando hacia el momento actual en el que se ha centrado completamente en el área de la seguridad de datos y privacidad.

En 2009, fue nombrado presidente de la Fundación Española para la Protección de Datos, a través de la cual, ha desarrollado protocolos de actuación y profesionalización del sector de las nuevas tecnologías, coordinando más de 30 centros y empresas profesionales en toda España.

Relativo a la Prevención del Blanqueo de Capitales y Financiación del Terrorismo, es experto externo reconocido por el Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias del Banco de España.

Colaboró como presidente en la Comunidad de Madrid de ASEBLAC, la primera y más importante Asociación Española de Sujetos Obligados en Prevención del Blanqueo de Capitales.

Actualmente ha fundado y preside la Asociación Española de Delegados de Protección de Datos. Es Delegado de Protección de Datos certificado según el Esquema de la Agencia Española de Protección de Datos.

Autor de varias publicaciones sobre la materia, ha impartido cursos y conferencias en diversos foros profesionales y empresariales difundiendo la normativa y las buenas prácticas en su aplicación.

Codirige e imparte como ponente la formación de preparación de Delegados de Protección de Datos del Ilustre Colegio de Abogados de Madrid ICAM.

ÍNDICE

1.- DATOS GENERALES

Denominación del curso	Curso Delegado de Protección de Datos – 180 h
Horas totales	180 horas
Modalidad	Teleformación

2.- PROFESORADO

Nombre y Apellidos	Ainhoa Juárez
Datos adicionales	Letrada del ICAM – DPD Certificada
Tutorías	Lunes y viernes de 9:00 a 14:00 horas

Nombre y Apellidos	Jorge Badiola
Datos adicionales	Economista– DPD Certificado
Tutorías	Martes y Jueves de 9:00 a 14:00 horas

3.- CONOCIMIENTOS PREVIOS

No es necesario contar con conocimientos previos aunque sí es aconsejable que el alumno o alumna reúna conocimientos del Derecho y la práctica en materia de protección de Datos.

4.- COMPETENCIAS ASIGNADAS Y NIVEL DE ADQUISICIÓN

Proporcionar conocimientos técnicos y prácticos, así como una formación técnica y metodológica para que los alumnos puedan realizar procesos de adaptación, asesoramiento, consultoría y auditoría, en cualquier organización, ya sea de carácter público o privado.

Proporcionar conocimientos teóricos para superar el examen de obtención de la certificación de Delegado de Protección de Datos.

Obtener una visión extendida sobre la materia, facultando al alumno a adquirir las siguientes funciones:

- Informar y asesorar al responsable o 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.
- 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.
- Supervisar la asignación de responsabilidades
- Supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento
- Supervisar las auditorías correspondientes
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos
- Supervisar su aplicación de conformidad con el artículo 35 del Reglamente
- Cooperar con la autoridad de control
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 y
- Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

5. RESULTADOS DEL APRENDIZAJE DEL CURSO

Preparación para el examen de certificación “Delegado de Protección de Datos”

Aplicar la normativa de Protección de Datos en las organizaciones que traten datos de carácter personal

6. INDICADORES DE LOGRO

El Delegado de Protección de Datos será capaz de:

- Recabar información para determinar las actividades de tratamiento
- Analizar y comprobar la conformidad de las actividades de tratamiento
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento
- Recabar información para supervisar el registro de las operaciones de tratamiento
- Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
- Asesorar:
- Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos
- Que metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos
- Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
- Que salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados
- Si se ha llevado a cabo correctamente o no de la evaluación de impacto de la protección de datos
- Si sus conclusiones son conformes con el Reglamento.
- Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
- Asesorar al responsable del tratamiento sobre:
- Que metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos

- Que áreas deben someterse a auditoría de protección de datos interna o externa
- Que actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

7. PRUEBAS DE EVALUCIÓN Y CRITERIOS DE CALIFICACIÓN

La evaluación de los conocimientos y capacidades técnicas o profesionales, se llevará a cabo mediante la realización de un examen, que versará sobre los temas relativos a los conocimientos específicos indicados en el siguiente apartado, de conformidad con los criterios de ponderación establecidos para cada uno de los dominios establecidos por la Agencia de Protección de Datos.

El examen se compone de 150 preguntas tipo test, siendo necesario para su aprobación haber superado el 75% de las mismas. El 20% de las preguntas, es decir, 30 preguntas, describirán un escenario práctico sobre el que versará la pregunta.

Las preguntas estarán distribuidas en cada uno delos correspondientes bloques o dominios del programa conforme a la siguiente ponderación:

Dominio 1-50%	75 preguntas, de ellas 15 con escenario
Dominio 2-30%	45 preguntas, de ellas 9 con escenario
Dominio 3-20%	30 preguntas, de ellas 6 con escenario

Para la aprobación de la prueba, se requiere haber respondido correctamente al menos, a un 50% de las preguntas en cada uno de los bloques o dominios.

Las preguntas tendrán cuatro opciones de respuesta, de las cuales sólo una será válida. Cada respuesta correcta contará como 1 punto. No puntúan las respuestas en blanco.

Se requiere haber obtenido al menos, 113 puntos.

Será necesario para la validación del curso haber presentado los ejercicios prácticos que se planteen en el curso.

8. CONTENIDOS DEL CURSO

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.

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.

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 contractuales

1.10. 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.

2. 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.

3. 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

4. Garantía de Derechos Digitales

5. Ejercicios prácticos –

6. Examen (Dominios 1 a 3)

9. MEDIOS PEDAGÓGICOS

Plataforma de formación y medios audiovisuales.

Ejercicios prácticos

Debates

Tutorización durante toda la duración del curso.