PROGRAMA FORMATIVO

Delegado de protección de datos

Abril 2019

DATOS GENERALES DE LA ESPECIALIDAD

1. Familia Profesional: ADMINISTRACIÓN Y GESTIÓN

Área Profesional: Administración y auditoría

2. Denominación: Delegado de protección de datos

3. Código: **ADGD27EXP**

4. Nivel de cualificación: 3

5. Objetivo general:

Ejercer tareas de consejo, gestión y asesoría al responsable del fichero de la entidad o empresa, sobre el cumplimiento de la normativa de protección de datos, por lo que será el encargado del tratamiento de las obligaciones legales en esta materia.

6. Prescripción de los formadores:

6.1. Titulación requerida:

- Licenciado, ingeniero, arquitecto o el título de grado correspondiente u otros títulos equivalentes.
- Diplomado, ingeniero técnico, arquitecto técnico o el título de grado correspondiente u otros títulos equivalentes.

6.2. Experiencia profesional requerida:

- Mínimo de 24 meses, en los últimos 5 años, en el ámbito de protección de datos o de la seguridad de la información.
- Estar incluido en el registro de Delegados de Protección de Datos (DPD) de la Agencia Española de Protección de Datos.

6.3. Competencia docente:

Será necesario tener formación metodológica o experiencia de 500 horas de impartición, de las cuales 200 horas deberán ser experiencia docente en materias relacionadas con la protección de datos o la seguridad de la información.

7. Criterios de acceso del alumnado:

7.1. Nivel académico o de conocimientos generales:

- Título Bachillerato
- Ciclo Formativo de Grado Superior: Técnico Superior en Administración y Finanzas, o equivalente.
- Además el aspirante al curso demostrará conocimientos suficientes para seguir con aprovechamiento esta formación, a través de una prueba de acceso.

8. Número de participantes:

Máximo 25 participantes para cursos presenciales.

9. Relación secuencial de módulos formativos:

- Módulo 1: Normativa general de protección de datos.
- Módulo 2: Responsabilidad activa.
- Módulo 3: Técnicas para garantizar el cumplimiento de la normativa de protección de datos.

10. Duración:

Horas totales: 250 horas

Distribución horas:
- Presencial: 250 horas

11. Requisitos mínimos de espacios, instalaciones y equipamiento

11.1. Espacio formativo:

- Aula de gestión: Los espacios tendrán que tener un mínimo de 30 m² para grupos de 15 alumnos (2m² por alumno)

Cada espacio estará equipado con mobiliario docente adecuado al número de alumnos, así mismo constará de las instalaciones y equipos de trabajo suficientes para el desarrollo del curso

11.2. Equipamiento:

- Aula de gestión:
  - Mesa y silla para el formador
  - Mesas y sillas para el alumnado
  - Material de aula
  - Pizarra
  - PC instalado en red con posibilidad de impresión de documentos, cañón con proyección e Internet para el formador
  - PCs instalados en red e Internet con posibilidad de impresión para los alumnos
  - Software específico para el aprendizaje de cada acción formativa: Un paquete de software ofimático, con la última actualización disponible del de mayor implantación en el mercado laboral, para el docente y para cada uno de los alumnos.Se deberá disponer de acceso y derecho de uso a:
    - 1 Dominio por curso con subdominios ilimitados y gestión de DNS
    - Espacio web de al menos10 GB
    - Acceso mínimo a 10 FTP
    - MySQL 5 x 1 GB al menos con gestión desde phpMyAdmin
    - Gestión de archivos en Panel de Control
    - Buzones POP3/IMAP4/SMTP 50 x 6 GB
    - Gestión de usuarios y permisos
    - Internacionalización
    - Gestión de clientes y pedidos
    - Redes Sociales
    - Analítica web: Google Analytics, eTracker …
  - Libros de apoyo.
  - Diversos modelos ejemplos de documentos contractuales.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

12. Requisitos oficiales para el ejercicio de la profesión

Este curso prepara para, en su caso, superar las pruebas de certificación "Delegado de Protección de Datos" según marca el Esquema de Certificación de Personas para la categoría de "Delegado de Protección de Datos" de la Agencia Española de la Protección de Datos.

MÓDULOS FORMATIVOS

Módulo nº 1

Denominación: Normativa general de protección de datos

Objetivo: Dominar el cumplimiento normativo del reglamento europeo, normativa nacional, directiva europea sobre ePrivacy. Directrices y guías del GT art.29, etc.

Duración: 125 horas.

Contenidos teórico- prácticos:

- Contexto normativo.
  - Privacidad y protección de datos en el panorama internacional.
  - La protección de datos en Europa.
  - La protección de datos en España.
  - Estándares y buenas prácticas.
- El Reglamento Europeo de Protección de datos y actualización de LOPD. Fundamentos.
  - Ámbito de aplicación.
  - Definiciones.
  - Sujetos obligados.
- El Reglamento Europeo de Protección de datos y actualización de LOPD. Principios
  - El binomio derecho/deber en la protección de datos.
  - Licitud del tratamiento
  - Lealtad y transparencia
  - Limitación de la finalidad
  - Minimización de datos
  - Exactitud
- El Reglamento Europeo de Protección de datos y actualización de LOPD. Legitimación
  - El consentimiento: otorgamiento y revocación.
  - El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado.
  - Consentimiento de los niños.
  - Categorías especiales de datos.
  - Datos relativos a infracciones y condenas penales.
  - Tratamiento que no requiere identificación.
  - Bases jurídicas distintas del consentimiento.
- Derechos de los individuos.
  - Transparencia e información
  - Acceso, rectificación, supresión (olvido).
  - Oposición
  - Decisiones individuales automatizadas.
  - Portabilidad.
  - Limitación del tratamiento.
  - Excepciones a los derechos.
- El Reglamento Europeo de Protección de datos y actualización de LOPD. Medidas de cumplimiento.

    - Las políticas de protección de datos.
    - Posición jurídica de los intervinientes. Responsables, co-responsables, encargados, subencargado del tratamiento y sus representantes. Relaciones entre ellos y formalización.
    - El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos.
- El Reglamento Europeo de Protección de datos y actualización de LOPD.
- Responsabilidad proactiva.
    - Privacidad desde el diseño y por defecto. Principios fundamentales.
    - Evaluación de impacto relativa a la protección de datos y consulta previa. Los tratamientos de alto riesgo.
    - Seguridad de los datos personales. Seguridad técnica y organizativa.
    - Las violaciones de la seguridad. Notificación de violaciones de seguridad.
    - El Delegado de Protección de Datos (DPD). Marco normativo.
    - Códigos de conducta y certificaciones.
- El Reglamento Europeo de Protección de datos. Delegados de Protección de Datos
- (DPD, DPO o Data Privacy Officer).
    - Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses.
    - Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección.
    - Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones.
    - Comunicación con la autoridad de protección de datos.
    - Competencia profesional. Negociación. Comunicación. Presupuestos.
    - Formación.
    - Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.
- El Reglamento Europeo de Protección de datos y actualización de LOPD. Transferencias internacionales de datos.
    - El sistema de decisiones de adecuación.
    - Transferencias mediante garantías adecuadas.
    - Normas Corporativas Vinculantes
    - Excepciones.
    - Autorización de la autoridad de control.
    - Suspensión temporal
    - Cláusulas contractuales
- El Reglamento Europeo de Protección de datos y actualización de LOPD. Las Autoridades de Control.
    - Autoridades de Control.
    - Potestades.
    - Régimen sancionador.
    - Comité Europeo de Protección de Datos.
    - Procedimientos seguidos por la AEPD.
    - La tutela jurisdiccional.
    - El derecho de indemnización.
- Directrices de interpretación del RGPD.
    - Guías del GT art. 29.
    - Opiniones del Comité Europeo de Protección de Datos
    - Criterios de órganos jurisdiccionales.
- Normativas sectoriales afectadas por la protección de datos.
    - Sanitaria, Farmacéutica, Investigación.
    - Protección de los menores
    - Solvencia Patrimonial
    - Telecomunicaciones
    - Videovigilancia
    - Seguros
    - Publicidad, etc.
- Normativa española con implicaciones en protección de datos.
    - LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
    - LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
    - Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica
- Normativa europea con implicaciones en protección de datos.

- 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.
- 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.
- 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.

Módulo nº 2

Denominación: Responsabilidad activa

Objetivo: Capacitar para la evaluación y gestión de riesgos de tratamientos de datos personales; evaluación de impacto de protección de datos, protección de datos desde el diseño, protección de datos por defecto, etc…

Duración: 75 horas.

Contenidos teórico - prácticos:

- Análisis y gestión de riesgos de los tratamientos de datos personales.
  - Introducción. Marco general de la evaluación y gestión de riesgos. Conceptos generales.
  - Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante.
  - Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible.
- Metodologías de análisis y gestión de riesgos.
- Programa de cumplimiento de Protección de Datos y Seguridad en una organización.
  - El Diseño y la implantación del programa de protección de datos en el contexto de la organización.
  - Objetivos del programa de cumplimiento.
  - Accountability: La trazabilidad del modelo de cumplimiento.
- Seguridad de la información.
  - 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.
  - 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.
  - 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.
- Evaluación de Impacto de Protección de Datos “EIPD”.
  - Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares.

- Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas.

Módulo nº 3

Denominación: Técnicas para garantizar el cumplimiento de la normativa de protección de datos

Objetivo: Dominar las diversas técnicas para garantizar el cumplimiento de la normativa de protección de datos: Auditorías de seguridad, auditorías de protección de datos, etc.

Duración: 50 horas.

Contenidos teórico - prácticos:

- La auditoría de protección de datos.
  - El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la Auditoría.
  - Elaboración del informe de auditoría. Aspectos básicos e importancia del informe de auditoría.
  - Ejecución y seguimiento de acciones correctoras.
- Auditoría de Sistemas de Información.
  - La Función de la Auditoría en los Sistemas de Información. Conceptos básicos.
  - Estándares y Directrices de Auditoría de SI.
  - Control interno y mejora continua. Buenas prácticas. Integración de la auditoria de protección de datos en la auditoria de SI.
  - Planificación, ejecución y seguimiento.
- La gestión de la seguridad de los tratamientos.
  - Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI).
  - Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación.
  - Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres.
- Otros conocimientos.
  - El cloud computing.
  - Los Smartphones.
  - Internet de las cosas (IoT).
  - Big data y elaboración de perfiles.
  - Redes sociales.
  - Tecnologías de seguimiento de usuario.
  - Blockchain y últimas tecnologías.