Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

DELEGADO DE PROTECCIÓN DE DATOS

Versión 1

Abril 2026

GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE

SISTEMA NACIONAL DE EMPLEO

IDENTIFICACIÓN DE LA ESPECIALIDAD Y PARÁMETROS DEL CONTEXTO FORMATIVO

Denominación de la especialidad:	DELEGADO DE PROTECCIÓN DE DATOS
Familia Profesional:	ADMINISTRACIÓN Y GESTIÓN
Área Profesional:	ADMINISTRACIÓN Y AUDITORÍA
Código:	ADGD0102
Nivel de cualificación profesional:	3

Objetivo general

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

Relación de módulos de formación

Módulo 1	Normativa general de protección de datos	125 horas
Módulo 2	Responsabilidad activa	75 horas
Módulo 3	Técnicas para garantizar el cumplimiento de la normativa de protección de datos	50 horas

Modalidades de impartición

Presencial
Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	250 horas
Teleformación	Duración total de las tutorías presenciales: 0 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: -Título de Bachiller o equivalente -Título de Técnico Superior (FP de Grado superior) o equivalente
Experiencia profesional	No se requiere
Otros	Se recomiendan los siguientes requisitos mínimos - Conocimientos básicos en materia de protección de datos. - Conocimientos básicos en materia de gestión de la seguridad de la información. - Conocimientos básicos en materia de gestión empresarial.
Modalidad de teleformación	Además de lo indicado anteriormente, los participantes han de tener las destrezas suficientes para ser usuarios de la plataforma virtual en la que se apoya la acción formativa.

Justificación de los requisitos del alumnado
En relación con las Acreditaciones/titulaciones a las que se refiere el apartado de la tabla anterior relativa a “Requisitos de acceso del alumnado”, se especifica lo siguiente: • Técnico Superior FP de familias profesionales de Administración y gestión o equivalente. Para acreditar los requisitos de formación, se documentará con la presentación de los títulos o certificados correspondientes. - Además la Administración deberá comprobar mediante una prueba de acceso que el candidato posee conocimientos generales relacionados con la especialidad indicados anteriormente (en materia de protección de datos, gestión de la seguridad de la información y gestión empresarial).

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: - 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.
Experiencia profesional mínima requerida	- Mínimo de 24 meses, en los últimos 5 años, en el ámbito de protección de datos o de la seguridad de la información.
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.
Otros	- Estar incluido en el registro de Delegados de Protección de Datos (DPD) de la Agencia Española de Protección de Datos.
Modalidad de teleformación	Además de cumplir con las prescripciones establecidas anteriormente, los tutores-formadores deben acreditar una formación, de al menos 30 horas, o experiencia, de al menos 60 horas, en esta modalidad y en la utilización de las tecnologías de la información y comunicación.

Justificación de las prescripciones de formadores y tutores
Para acreditar tanto los requisitos de formación como de experiencia impartiendo formación en las horas mínimas estipuladas, se documentará con la presentación de títulos y certificados oficiales, vida laboral, certificados de empresa o contratos más liquidación (que demuestre que se han ejecutado).

Requisitos mínimos de espacios, instalaciones y equipamientos

Espacios formativos	Superficie m² para 15 participantes	Incremento Superficie/ participante (Máximo 30 participantes)
Aula de gestión	45.0 m²	2.4 m² / participante

Espacio formativo	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 participantes - Software específico para el aprendizaje de cada acción formativa. • Un paquete de software ofimático y lector de pdf. (Versión actualizada).

La superficie de los espacios e instalaciones estarán en función de su tipología y del número de participantes. Tendrán como mínimo los metros cuadrados que se indican para 15 participantes y el equipamiento suficiente para los mismos.

En el caso de que aumente el número de participantes, hasta un máximo de 30, la superficie de las aulas se incrementará proporcionalmente (según se indica en la tabla en lo relativo a m²/participante) y el equipamiento estará en consonancia con dicho aumento.

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

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

Aula virtual

Características
• La impartición de la formación mediante aula virtual se ha de estructurar y organizar de forma que se garantice en todo momento que exista conectividad sincronizada entre las personas formadoras y el alumnado participante así como bidireccionalidad en las comunicaciones. • Se deberá contar con un registro de conexiones generado por la aplicación del aula virtual en que se identifique, para cada acción formativa desarrollada a través de este medio, las personas participantes en el aula, así como sus fechas y tiempos de conexión.
Otras especificaciones
• Garantizar el soporte técnico permanente durante el horario docente del curso por parte del centro. • La plataforma de teleformación que se utilice para impartir acciones formativas deberá alojar el material virtual de aprendizaje correspondiente, poseer capacidad suficiente para desarrollar el proceso de aprendizaje y gestionar y garantizar la formación del alumnado,

permitiendo la interactividad y el trabajo cooperativo, y reunir los requisitos técnicos de infraestructura, software y servicios necesarios.

- El equipamiento que se exige al alumnado para poder seguir el curso en modalidad virtual no podrá ser superior a un i3 con 4G y con una antigüedad máxima de 5 años, teniendo que aportar la empresa adjudicataria máquinas físicas o virtuales con la potencia suficiente en caso de ser necesaria mayor potencia. El alumnado deberá contar con conexión de banda ancha a internet para poder seguir las clases de forma síncrona.

Para impartir la formación en **modalidad de teleformación**, se ha de disponer del siguiente equipamiento.

Plataforma de teleformación

La plataforma de teleformación que se utilice para impartir acciones formativas deberá alojar el material virtual de aprendizaje correspondiente, poseer capacidad suficiente para desarrollar el proceso de aprendizaje y gestionar y garantizar la formación del alumnado, permitiendo la interactividad y el trabajo cooperativo, y reunir los siguientes requisitos técnicos de infraestructura, software y servicios:

- **Infraestructura:**

Tener un rendimiento, entendido como número de alumnos que soporte la plataforma, velocidad de respuesta del servidor a los usuarios, y tiempo de carga de las páginas Web o de descarga de archivos, que permita:

a) Soportar un número de alumnos equivalente al número total de participantes en las acciones formativas de formación profesional para el empleo que esté impartiendo el centro o entidad de formación, garantizando un hospedaje mínimo igual al total del alumnado de dichas acciones, considerando que el número máximo de alumnos por tutor es de 80 y un número de usuarios concurrentes del 40% de ese alumnado.

b) Disponer de la capacidad de transferencia necesaria para que no se produzca efecto retardo en la comunicación audiovisual en tiempo real, debiendo tener el servidor en el que se aloja la plataforma un ancho de banda mínimo de 300 Mbs, suficiente en bajada y subida.

Estar en funcionamiento 24 horas al día, los 7 días de la semana.

- **Software:**

- Compatibilidad con el estándar SCORM y paquetes de contenidos IMS.
- Niveles de accesibilidad e interactividad de los contenidos disponibles mediante tecnologías web que como mínimo cumplan las prioridades 1 y 2 de la Norma UNE 139803:2012 o posteriores actualizaciones, según lo estipulado en el capítulo III del Real Decreto 1494/2007, de 12 de noviembre.
- El servidor de la plataforma de teleformación ha de cumplir con los requisitos establecidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por lo que el responsable de dicha plataforma ha de identificar la localización física del servidor y el cumplimento de lo establecido sobre transferencias internacionales de datos en los artículos 40 a 43 de la citada Ley Orgánica 3/2018, de 5 de diciembre, así como, en lo que resulte de aplicación, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas respecto del tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

- Compatibilidad tecnológica y posibilidades de integración con cualquier sistema operativo, base de datos, navegador de Internet de los más usuales o servidor web, debiendo ser posible utilizar las funciones de la plataforma con complementos (plug-in) y visualizadores compatibles. Si se requiriese la instalación adicional de algún soporte para funcionalidades avanzadas, la plataforma debe facilitar el acceso al mismo sin coste.
- Disponibilidad del servicio web de seguimiento (operativo y en funcionamiento) de las acciones formativas impartidas, conforme al modelo de datos y protocolo de transmisión establecidos en el anexo V de la Orden/TMS/369/2019, de 28 de marzo.

- **Servicios y soporte:**

- Sustentar el material virtual de aprendizaje de la especialidad formativa que a través de ella se imparta.
- Disponibilidad de un servicio de atención a usuarios que de soporte técnico y mantenga la infraestructura tecnológica y que, de forma estructurada y centralizada, atienda y resuelva las consultas e incidencias técnicas del alumnado. Las formas de establecer contacto con este servicio, que serán mediante teléfono y mensajería electrónica, tienen que estar disponibles para el alumnado desde el inicio hasta la finalización de la acción formativa, manteniendo un horario de funcionamiento de mañana y de tarde y un tiempo de demora en la respuesta no superior a 48 horas laborables.
- Personalización con la imagen institucional de la administración laboral correspondiente, con las pautas de imagen corporativa que se establezcan.

  Con el objeto de gestionar, administrar, organizar, diseñar, impartir y evaluar acciones formativas a través de Internet, la plataforma de teleformación integrará las herramientas y recursos necesarios a tal fin, disponiendo, específicamente, de herramientas de:
  - Comunicación, que permitan que cada alumno pueda interaccionar a través del navegador con el tutor-formador, el sistema y con los demás alumnos. Esta comunicación electrónica ha de llevarse a cabo mediante herramientas de comunicación síncronas (aula virtual, chat, pizarra electrónica) y asíncronas (correo electrónico, foro, calendario, tablón de anuncios, avisos). Será obligatorio que cada acción formativa en modalidad de teleformación disponga, como mínimo, de un servicio de mensajería, un foro y un chat.
  - Colaboración, que permitan tanto el trabajo cooperativo entre los miembros de un grupo, como la gestión de grupos. Mediante tales herramientas ha de ser posible realizar operaciones de alta, modificación o borrado de grupos de alumnos, así como creación de «escenarios virtuales» para el trabajo cooperativo de los miembros de un grupo (directorios o «carpetas» para el intercambio de archivos, herramientas para la publicación de los contenidos, y foros o chats privados para los miembros de cada grupo).
  - Administración, que permitan la gestión de usuarios (altas, modificaciones, borrado, gestión de la lista de clase, definición, asignación y gestión de permisos, perfiles y roles, autenticación y asignación de niveles de seguridad) y la gestión de acciones formativas.
  - Gestión de contenidos, que posibiliten el almacenamiento y la gestión de archivos (visualizar archivos, organizarlos en carpetas –directorios- y subcarpetas, copiar, pegar, eliminar, comprimir, descargar o cargar archivos), la publicación organizada y selectiva de los contenidos de dichos archivos, y la creación de contenidos.

- Evaluación y control del progreso del alumnado, que permitan la creación, edición y realización de pruebas de evaluación y autoevaluación y de actividades y trabajos evaluables, su autocorrección o su corrección (con retroalimentación), su calificación, la asignación de puntuaciones y la ponderación de las mismas, el registro personalizado y la publicación de calificaciones, la visualización de información estadística sobre los resultados y el progreso de cada alumno y la obtención de informes de seguimiento.

Material virtual de aprendizaje:

El material virtual de aprendizaje para el alumnado mediante el que se imparta la formación se concretará en el curso completo en formato multimedia (que mantenga una estructura y funcionalidad homogénea), debiendo ajustarse a todos los elementos de la programación (objetivos y resultados de aprendizaje) de este programa formativo que figura en el Catálogo de Especialidades Formativas y cuyo contenido cumpla estos requisitos:

- Como mínimo, ser el establecido en el citado programa formativo del Catálogo de Especialidades Formativas.
- Estar referido tanto a los objetivos como a los conocimientos/ capacidades cognitivas y prácticas, y habilidades de gestión, personales y sociales, de manera que en su conjunto permitan conseguir los resultados de aprendizaje previstos.
- Organizarse a través de índices, mapas, tablas de contenido, esquemas, epígrafes o titulares de fácil discriminación y secuenciase pedagógicamente de tal manera que permiten su comprensión y retención.
- No ser meramente informativos, promoviendo su aplicación práctica a través de actividades de aprendizaje (autoevaluables o valoradas por el tutor-formador) relevantes para la adquisición de competencias, que sirvan para verificar el progreso del aprendizaje del alumnado, hacer un seguimiento de sus dificultades de aprendizaje y prestarle el apoyo adecuado.
- No ser exclusivamente textuales, incluyendo variados recursos (necesarios y relevantes), tanto estáticos como interactivos (imágenes, gráficos, audio, video, animaciones, enlaces, simulaciones, artículos, foro, chat, etc.). de forma periódica.
- Poder ser ampliados o complementados mediante diferentes recursos adicionales a los que el alumnado pueda acceder y consultar a voluntad.
- Dar lugar a resúmenes o síntesis y a glosarios que identifiquen y definan los términos o vocablos básicos, relevantes o claves para la comprensión de los aprendizajes.
- Evaluar su adquisición durante y a la finalización de la acción formativa a través de actividades de evaluación (ejercicios, preguntas, trabajos, problemas, casos, pruebas, etc.), que permitan medir el rendimiento o desempeño del alumnado.

Otras especificaciones

Para que la acción formativa online funcione, debe ser flexible en ritmos y acceso, altamente interactiva (foros, debates, tutorías en vivo) para fomentar la participación, y con un enfoque práctico basado en la aplicación de los conocimientos a problemas reales o simulados.

Vinculaciones con capacitaciones profesionales

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.

Ocupaciones y puestos de trabajo relacionados

- 12111015 DIRECTORES DE DEPARTAMENTO DE ADMINISTRACIÓN Y FINANZAS, EN GENERAL
- 1321 DIRECTORES DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC)
- 13211026 DIRECTORES DE DEPARTAMENTO DE SERVICIOS INFORMÁTICOS, EN GENERAL
- 2511 ABOGADOS
- 25991028 ASESORES JURÍDICOS (SECTOR PRIVADO)
- 26111052 TÉCNICOS SUPERIORES EN CONTABILIDAD Y/O FINANZAS, EN GENERAL
- 27191013 AUDITORES-ASESORES INFORMÁTICOS
- 2721 DISEÑADORES Y ADMINISTRADORES DE BASES DE DATOS
- 28101019 ECONOMISTAS
- 34021022 TÉCNICOS DE APOYO EN AUDITORÍA Y/U OPERACIONES FINANCIERAS
- 3612 ASISTENTES JURÍDICO-LEGALES
- 3711 PROFESIONALES DE APOYO DE SERVICIOS JURÍDICOS Y SERVICIOS SIMILARES
- 37111027 TÉCNICOS DE SERVICIOS JURÍDICOS Y/O SIMILARES
- DELEGADO DE PROTECCION DE DATOS

Requisitos necesarios para el ejercicio profesional

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.

Requisitos oficiales de las entidades o centros de formación

Estar inscrito en el Registro de entidades de formación (Servicios Públicos de Empleo).

Centro Móvil

Es posible impartir esta especialidad en centro móvil.

MÓDULO DE FORMACIÓN 1: 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 Comité Europeo de Protección de Datos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 125 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- 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, y otros.
- 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.

Habilidades de gestión, personales y sociales

- Realizar Evaluaciones de Impacto (EIPD) y determinar las medidas técnicas y organizativas adecuadas según el riesgo.
- Establecer procedimientos para identificar, gestionar y notificar violaciones de seguridad a la autoridad competente.
- Organizar actividades de tratamiento y supervisión de la documentación necesaria para auditorías.
- Actuar sin recibir instrucciones directas sobre cómo realizar sus funciones, manteniendo la neutralidad.
- Manejar de forma íntegra la información sensible y mantener la confidencialidad en todas las operaciones.
- Agilizar a interpretación de la normativa frente a nuevos tratamientos tecnológicos o cambios en la organización.
- Actuar como punto de contacto directo para que los ciudadanos ejerzan sus derechos de forma clara y accesible.
- Generar interlocución constante con las Autoridades de Control y fomento de una cultura de protección de datos dentro de la empresa.
- Concienciar y capacitar al personal sobre las buenas prácticas y principios de licitud y transparencia.

MÓDULO DE FORMACIÓN 2: 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 y protección de datos por defecto, entre otros.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 75 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- 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 NIS2: 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.

Habilidades de gestión, personales y sociales

- Integrar la protección de datos desde la fase de ideación de cualquier proyecto o producto.
- Generar evidencias de cumplimiento (logs, contratos con terceros,

registros) que sean válidas en una auditoría de la Agencia Española de Protección de Datos (AEPD), priorizando amenazas según su probabilidad e impacto y aplicando medidas de seguridad proporcionales.
- Fortalecer la proactividad e Iniciativa para la búsqueda constante de puntos débiles en el tratamiento de datos.
- Cuestionar procesos establecidos y evaluar si realmente respetan la minimización de datos.
- Actualizar los conocimientos continuamente mediante recursos como el EDPB (European Data Protection Board).
- Traducir términos legales complejos (como "interés legítimo") a un lenguaje que el equipo pueda entender y aplicar.
- Capacidad para impartir formación interna y convertir a los empleados en la primera línea de defensa de la privacidad.
- Mediar en la solución de conflictos cuando las necesidades de negocio chocan con los límites de la privacidad, buscando soluciones que no comprometan la legalidad.

MÓDULO DE FORMACIÓN 3: 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, y auditorías de protección de datos, entre otros.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 50 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- 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.

Habilidades de gestión, personales y sociales

- Estructurar el sistema de protección dentro de una organización.
- Mapear el flujo de datos y localizar dónde se almacenan (nube, servidores locales, papel) para aplicar el Registro de Actividades de Tratamiento (RAT).
- Realizar controles periódicos y verificar que las medidas de seguridad técnicas (como el cifrado) y organizativas (políticas de uso) se están cumpliendo.
- Crear manuales de respuesta ante el ejercicio de derechos o ante una brecha de seguridad.
- Atender al detalle para revisar cláusulas en contratos con proveedores y asegurar que cumplen el Artículo 28 del RGPD (Encargados del Tratamiento).
- Desglosar procesos complejos y detectar en qué punto se está vulnerando el principio de minimización de datos.
- Interesarse por comprender las nuevas tecnologías (IA, Big Data) para adaptar las técnicas de protección a los nuevos riesgos.
- Transformar la jerga legal en instrucciones sencillas para que cualquier empleado sepa cómo tratar un correo electrónico o una base de datos.
- Convencer a los departamentos de IT o Marketing de que ciertas prácticas deben cambiar por seguridad, sin bloquear la operatividad del negocio.
- Redactar cláusulas informativas que sean fáciles de entender para el ciudadano, ganando su confianza.

ORIENTACIONES METODOLÓGICAS

Este temario debe estar siempre ajustado a la **versión vigente del esquema de certificación DPD-AEPD de la Agencia Española de Protección de datos** y su contenido deberá estar, actualizado a las normas que sean de aplicación en cada momento.

Tanto las horas presenciales como las on-line:

- Metodología activa y participativa: combinando exposiciones teóricas, estudios de caso, talleres prácticos y trabajo en equipo.
- Recursos didácticos: presentaciones multimedia, documentos normativos, software específico, simuladores y plataformas digitales.
- Tutorías personalizadas: seguimiento y apoyo individual para resolver dudas y orientar el aprendizaje.
- Evaluación continua: mediante pruebas teóricas, resolución de casos prácticos y participación en actividades.

EVALUACIÓN DEL APRENDIZAJE EN LA ACCIÓN FORMATIVA

- La evaluación tendrá un carácter teórico-práctico y se realizará de forma sistemática y continua, durante el desarrollo de cada módulo y al final del curso.
- Puede incluir una evaluación inicial de carácter diagnóstico para detectar el nivel de partida del alumnado.
- La evaluación se llevará a cabo mediante los métodos e instrumentos más adecuados para comprobar los distintos resultados de aprendizaje, y que garanticen la fiabilidad y validez de la misma.
- Cada instrumento de evaluación se acompañará de su correspondiente sistema de corrección y puntuación en el que se explicite, de forma clara e inequívoca, los criterios de medida para evaluar los resultados alcanzados por los participantes.
- La puntuación final alcanzada se expresará en términos de Apto/ No Apto.