PROTECCIÓN DE DATOS

PARA TRABAJADORES

Manual de Formación Oficial

Adaptado al RGPD (UE) 2016/679 y la LOPDGDD 3/2018

Guía AEPD actualizada diciembre 2025

⏱️ **Duración del curso**
20 horas lectivas

🎯 **Nivel**
Básico – Todos los trabajadores

📋 **Modalidad**
Presencial / Teleformación / Mixta

✅ **Certificación**
Diploma oficial empresa / FUNDAE

Normativa de referencia

RGPD (UE) 2016/679 | LOPDGDD Ley Orgánica 3/2018 | Constitución Española Art. 18.4
Estatuto de los Trabajadores | Guía AEPD Relaciones Laborales (dic. 2025) | ENS (RD 311/2022)

Presentación del Curso

El presente manual constituye el material oficial del curso "Protección de Datos para Trabajadores", diseñado para cumplir con las obligaciones de formación y concienciación que establece el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Conforme al principio de responsabilidad proactiva recogido en el artículo 5.2 del RGPD, las organizaciones no solo deben cumplir con la normativa, sino también poder demostrar que la cumplen. La Agencia Española de Protección de Datos (AEPD), en su Guía sobre protección de datos en las relaciones laborales (actualizada en diciembre de 2025), establece que la formación del personal es una medida organizativa esencial, extensible incluso a trabajadores sin acceso directo a sistemas de información, como el personal de limpieza o mantenimiento.

BASE LEGAL DE ESTE CURSO

Artículo 5.2 RGPD (responsabilidad proactiva) · Artículo 24 RGPD (medidas técnicas y organizativas) · Artículo 32 RGPD (seguridad del tratamiento) · Artículo 39 RGPD (funciones del DPO) · Artículo 5 LOPDGDD (deber de confidencialidad) · Guía AEPD Relaciones Laborales, diciembre 2025.

Ficha Técnica del Curso

Denominación	Protección de Datos para Trabajadores
Código de especialidad	ADGD-036 (Protección de Datos)
Duración total	20 horas lectivas
Modalidad	Presencial / Teleformación / Mixta
Nivel de cualificación	Nivel 1 – Básico (todos los trabajadores)
Destinatarios	Trabajadores/as de cualquier sector que traten datos personales en el ejercicio de sus funciones
Normativa base	RGPD (UE) 2016/679 · LOPDGDD 3/2018 · Guía AEPD dic. 2025
Organismo supervisor	Agencia Española de Protección de Datos (AEPD)
Tipo de certificación	Diploma de aprovechamiento de la entidad formativa / Bonificable FUNDAE
Revisión del contenido	Anual o cuando se produzcan cambios normativos relevantes

Índice de Contenidos

TOTAL: 20 horas lectivas

Objetivos del Curso

Objetivo General

Capacitar a los trabajadores para conocer, comprender y aplicar en su actividad diaria los principios y obligaciones que establece la normativa vigente en materia de protección de datos personales, fomentando una cultura de privacidad y responsabilidad en la organización.

Objetivos Específicos

- Conocer el marco legal vigente: RGPD, LOPDGDD y directrices de la AEPD.
- Identificar qué son los datos personales y cuándo se produce un tratamiento.
- Reconocer los derechos de los ciudadanos y cómo atenderlos.
- Comprender las bases jurídicas que legitiman el tratamiento de datos.
- Cumplir con el deber de secreto y confidencialidad profesional.
- Identificar, gestionar y notificar brechas de seguridad.
- Aplicar los derechos digitales laborales: desconexión digital, videovigilancia, etc.
- Documentar adecuadamente la formación recibida para acreditar el cumplimiento.

MÓDULO 1 – Marco Normativo

Duración: 3 horas | Nivel: Básico

1.1. El derecho fundamental a la protección de datos

La protección de los datos personales es un derecho fundamental reconocido en el artículo 18.4 de la Constitución Española de 1978, que dispone que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». España fue pionera en este reconocimiento constitucional.

A nivel europeo, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea reconoce que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan».

1.2. El Reglamento General de Protección de Datos (RGPD)

El RGPD –Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016– es la norma europea de referencia en materia de protección de datos. Es de aplicación directa en todos los Estados miembros desde el 25 de mayo de 2018, sin necesidad de transposición.

Ámbito de aplicación:

- Se aplica a toda organización que trate datos de personas físicas residentes en la UE, independientemente de dónde tenga su sede.
- No distingue entre empresas B2B y B2C: ambas están obligadas a cumplirlo.
- Una dirección de correo profesional es un dato personal a efectos del RGPD.

Principios que consagra (Art. 5 RGPD):

- Licitud, lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva (accountability).

1.3. La LOPDGDD – Ley Orgánica 3/2018

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) adapta el ordenamiento jurídico español al RGPD. Entró en vigor el 6 de diciembre de 2018, sustituyendo a la antigua LOPD de 1999.

Aportaciones principales:

- Refuerza el deber de confidencialidad de las personas que traten datos personales (Art. 5 LOPDGDD).

- Desarrolla la figura del Delegado de Protección de Datos (DPO) en España.
- Introduce el Catálogo de derechos digitales (Título X).
- Regula el tratamiento de datos en el contexto laboral, la videovigilancia y el control del trabajador.

1.4. La Agencia Española de Protección de Datos (AEPD)

La AEPD es la autoridad de control independiente encargada de supervisar el cumplimiento de la normativa de protección de datos en España. Tiene potestad sancionadora y publica guías y recomendaciones de referencia. En diciembre de 2025 actualizó la Guía sobre protección de datos en las relaciones laborales, documento esencial para este curso.

> **PUNTO CLAVE PARA LA INSPECCIÓN**
> *Las inspecciones de la AEPD, Inspección de Trabajo y auditorías internas verificarán que la empresa pueda acreditar documentalmente la formación impartida al personal (fecha, duración, contenido, firma de asistencia y resultado de evaluación).*

MÓDULO 2 – Conceptos Fundamentales

Duración: 3 horas | Nivel: Básico

2.1. ¿Qué son los datos personales?

Según el artículo 4.1 del RGPD, dato personal es «toda información sobre una persona física identificada o identificable». Una persona es identificable cuando puede determinarse su identidad, directa o indirectamente, en particular mediante un identificador como el nombre, número de identificación, datos de localización, identificador en línea u otros elementos propios de su identidad.

Ejemplos de datos personales en el entorno laboral:

- Nombre y apellidos, DNI/NIE, número de la Seguridad Social.
- Dirección postal, correo electrónico personal o profesional, teléfono.
- Imagen (fotografías, vídeo de videovigilancia).
- Datos biométricos usados para control de acceso o jornada.
- Geolocalización de vehículos de empresa asignados a trabajadores.
- Datos de salud o bajas médicas.
- Número de cuenta bancaria para el pago de nómina.

2.2. Categorías especiales de datos

Algunos datos requieren una protección reforzada por su especial sensibilidad. El artículo 9 del RGPD prohíbe su tratamiento con carácter general, salvo excepciones tasadas:

CONCEPTO	DEFINICIÓN
Origen racial o étnico	Información sobre la procedencia racial o étnica de la persona.
Opiniones políticas	Afiliación o simpatía política manifiesta.
Creencias religiosas	Confesión o práctica religiosa o filosófica.
Afiliación sindical	Pertenencia a un sindicato o asociación profesional.
Datos genéticos y biométricos	ADN, huella dactilar, reconocimiento facial (cuando permitan identificar).
Datos de salud	Historial médico, bajas laborales, discapacidades.
Vida u orientación sexual	Datos sobre la vida sexual o preferencias sexuales.
Datos sobre condenas penales	Antecedentes penales o infracciones (Art. 10 RGPD).

2.3. Tratamiento de datos: definición y operaciones

El artículo 4.2 del RGPD define tratamiento como «cualquier operación o conjunto de operaciones realizadas sobre datos personales, con o sin medios automatizados». Incluye:

- Recogida, registro, organización y estructuración.
- Conservación, adaptación o modificación.
- Extracción, consulta, utilización.
- Comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso.
- Cotejo o interconexión, limitación, supresión o destrucción.

2.4. Actores principales del tratamiento

CONCEPTO	DEFINICIÓN
Responsable del tratamiento	Persona física o jurídica que determina los fines y medios del tratamiento. Normalmente, la empresa empleadora.
Encargado del tratamiento	Tercero que trata datos por cuenta del responsable (p. ej., asesoría laboral, empresa de nóminas en la nube).
Interesado	Persona física cuyos datos son objeto del tratamiento (trabajador, cliente, candidato).
Delegado de Protección de Datos (DPO)	Figura que asesora, supervisa y actúa de enlace con la AEPD. Obligatorio en ciertas organizaciones.
Autoridad de control	Organismo público supervisor: la AEPD en España.

MÓDULO 3 – Derechos de los Interesados (ARCO+)

Duración: 2 horas | Nivel: Básico

El RGPD amplía los derechos clásicos ARCO (Acceso, Rectificación, Cancelación, Oposición) con nuevos derechos que forman el denominado conjunto ARCO+:

CONCEPTO	DEFINICIÓN
Derecho de Acceso (Art. 15)	El interesado puede solicitar confirmación de si sus datos son tratados y obtener copia de los mismos.
Derecho de Rectificación (Art. 16)	Corrección de datos inexactos o incompletos.
Derecho de Supresión / 'Al Olvido' (Art. 17)	Eliminación de datos cuando ya no son necesarios, se retira el consentimiento o su tratamiento es ilícito.
Derecho de Limitación (Art. 18)	Restricción del tratamiento mientras se resuelve una impugnación sobre exactitud o licitud.
Derecho de Portabilidad (Art. 20)	Recibir los datos en formato estructurado y transferirlos a otro responsable.
Derecho de Oposición (Art. 21)	Oponerse al tratamiento por motivos relacionados con su situación particular.
Derechos ante decisiones automatizadas (Art. 22)	No ser objeto exclusivo de decisiones basadas en tratamiento automatizado con efectos significativos.

3.1. Plazos y obligaciones de respuesta

- El responsable dispone de 1 mes para responder, ampliable a 3 meses en casos complejos.
- La respuesta debe ser gratuita para el interesado.
- Si no se actúa, el trabajador o ciudadano puede reclamar ante la AEPD.

OBLIGACIÓN DEL TRABAJADOR

Cuando un cliente, usuario o compañero ejercite un derecho ARCO+, debes NUNCA ignorarlo ni resolverlo por tu cuenta sin seguir el procedimiento establecido. Deriva siempre la solicitud al responsable de protección de datos o al DPO de tu organización en el menor tiempo posible.

MÓDULO 4 – Principios del Tratamiento y Bases Jurídicas

Duración: 3 horas | Nivel: Básico

4.1. Principios del tratamiento (Art. 5 RGPD)

- Licitud, lealtad y transparencia: los datos se deben tratar de forma lícita y transparente para el interesado.
- Limitación de finalidad: los datos se recogen para fines determinados, explícitos y legítimos.
- Minimización: solo se deben tratar los datos estrictamente necesarios.
- Exactitud: los datos deben ser correctos y, si es preciso, actualizados.
- Limitación del plazo de conservación: no se guardan más tiempo del necesario.
- Integridad y confidencialidad: protección contra accesos no autorizados, pérdida o destrucción.
- Responsabilidad proactiva: el responsable puede demostrar en todo momento el cumplimiento.

4.2. Bases jurídicas del tratamiento (Art. 6 RGPD)

Todo tratamiento de datos personales debe sustentarse en una base jurídica válida. Las seis bases reconocidas son:

CONCEPTO	DEFINICIÓN
Consentimiento (Art. 6.1.a)	Libre, específico, informado e inequívoco. En el entorno laboral, raramente es válido por la relación de dependencia.
Contrato (Art. 6.1.b)	Tratamiento necesario para la ejecución de un contrato del que es parte el interesado (p. ej., nómina).
Obligación legal (Art. 6.1.c)	Cumplir una obligación legal (p. ej., cotización a la Seguridad Social, IRPF).
Intereses vitales (Art. 6.1.d)	Proteger la vida del interesado u otra persona física.
Interés público (Art. 6.1.e)	Misión realizada en interés público o en ejercicio de poderes públicos.
Interés legítimo (Art. 6.1.f)	Intereses del responsable o tercero, siempre que no prevalezcan los del interesado.

4.3. El Registro de Actividades de Tratamiento (RAT)

El artículo 30 del RGPD obliga a mantener un Registro de Actividades de Tratamiento (RAT) que recoja, para cada tratamiento:

- Nombre y datos de contacto del responsable y del DPO (si existe).
- Finalidades del tratamiento.
- Categorías de interesados y de datos tratados.

- Destinatarios o categorías de destinatarios.
- Transferencias internacionales (si aplica) y garantías adoptadas.
- Plazos previstos de supresión.
- Medidas técnicas y organizativas de seguridad.

MÓDULO 5 – Obligaciones del Trabajador: Secreto y Seguridad

Duración: 2 horas | Nivel: Básico

5.1. Deber de confidencialidad y secreto

El artículo 5 de la LOPDGDD establece que «los responsables y encargados del tratamiento, así como todas las personas que intervengan en cualquier fase del mismo están sujetas al deber de confidencialidad». Este deber:

- Es de carácter permanente: se mantiene incluso después de finalizar la relación laboral.
- Abarca a todos los trabajadores, incluidos aquellos sin acceso directo a sistemas informatizados.
- La AEPD considera que debe extenderse al personal de limpieza o mantenimiento si pueden exponer datos accidentalmente.

> **RECUERDA: EL SECRETO PROFESIONAL NO TIENE FECHA DE CADUCIDAD**
> *La obligación de guardar secreto sobre los datos personales a los que hayas tenido acceso durante tu trabajo persiste incluso tras la extinción de tu contrato, cualquiera que sea su causa.*

5.2. Buenas prácticas obligatorias del trabajador

1. No acceder a datos sin autorización ni para fines distintos a los de tu puesto.
2. No compartir contraseñas ni dejar sesiones abiertas en equipos desatendidos.
3. Bloquear el equipo cuando te ausentes del puesto (Win+L / Ctrl+Cmd+Q).
4. No enviar datos personales por canales no seguros o no autorizados (WhatsApp personal, correo no corporativo, etc.).
5. No imprimir documentos con datos personales innecesariamente; si se imprimen, destruirlos adecuadamente (trituradora).
6. No guardar datos personales en dispositivos extraíbles no autorizados (USB, disco externo).
7. Comunicar de inmediato cualquier sospecha de brecha de seguridad o pérdida de datos.
8. Seguir en todo momento los procedimientos internos de la empresa en materia de protección de datos.

5.3. Política de mesas limpias y pantallas limpias

La política de "mesa limpia" obliga a no dejar documentación con datos personales visible cuando se abandona el puesto. La política de "pantalla limpia" implica bloquear siempre el equipo al ausentarse. Estas medidas son exigidas por el Esquema Nacional de Seguridad (ENS, RD 311/2022) y recomendadas por la AEPD.

5.4. Uso correcto del correo electrónico y herramientas digitales

- Utiliza solo las cuentas corporativas para comunicaciones con datos personales.

- Antes de reenviar un correo, verifica que no contiene datos innecesarios.
- Los correos masivos con datos de clientes o empleados deben enviarse en CCO (copia oculta).
- Desconfía de correos sospechosos (phishing): pueden ser la puerta de entrada a una brecha de datos.

MÓDULO 6 – Protección de Datos en el Entorno Laboral

Duración: 2 horas | Nivel: Básico

6.1. Datos del trabajador en la relación laboral

La empresa puede tratar los datos del trabajador cuando resulten necesarios para la relación laboral. El principio de minimización impone que solo se recopilen los estrictamente precisos. La AEPD, en su Guía de relaciones laborales (dic. 2025), recuerda que el empleador no puede recoger más datos de los necesarios en ninguna fase de la relación laboral.

Datos que pueden tratarse legítimamente:

- Identificativos: nombre, DNI, número de afiliación a la Seguridad Social.
- Económicos: cuenta bancaria para nómina, datos fiscales para el IRPF.
- De salud (limitados): confirmación de baja médica, grado de discapacidad reconocida a efectos de cotización o adaptación del puesto.
- Control de presencia: registro de jornada (obligatorio por el Estatuto de los Trabajadores, Art. 34.9).

6.2. Selección y contratación de personal

- Durante la selección, la empresa debe informar a los candidatos del tratamiento de sus datos.
- No está legitimado pedir acceso a perfiles privados de redes sociales ni solicitar "amistad" para acceder a contenido personal.
- Los perfiles públicos en redes sociales pueden consultarse, pero el candidato debe ser informado de ello y existir una base jurídica válida.
- Los currículums y datos de candidatos no seleccionados deben suprimirse o anonimizarse tras el proceso de selección, salvo consentimiento para conservarlos.

6.3. Videovigilancia y sistemas de control en el trabajo

El artículo 89 de la LOPDGDD y la Guía AEPD regulan el uso de cámaras de videovigilancia en el lugar de trabajo:

- El empleador puede instalar cámaras para la seguridad del centro o el control laboral, siempre que exista proporcionalidad y necesidad.
- Es obligatorio informar a los trabajadores mediante el cartel identificativo homologado por la AEPD.
- Las imágenes no pueden conservarse más de 30 días, salvo que sean prueba de un incidente o delito.
- No está permitida la videovigilancia en zonas de descanso, vestuarios o baños.

6.4. Geolocalización de empleados

El uso de sistemas GPS en vehículos de empresa o dispositivos móviles del trabajador está regulado por el artículo 90 LOPDGDD:

- Es necesario informar previamente al trabajador y a los representantes sindicales.
- La finalidad debe ser legítima (control de flotas, seguridad) y no puede usarse para vigilancia continua e injustificada.
- La geolocalización fuera del horario de trabajo (en el domicilio o en tiempo libre) es, por regla general, desproporcionada e ilícita.

6.5. Control del uso de dispositivos corporativos e internet

El artículo 87 LOPDGDD reconoce el derecho a la intimidad del trabajador en el uso de los dispositivos digitales de la empresa. El empleador puede establecer protocolos de uso y verificar su cumplimiento, pero debe:

- Establecer una política de uso aceptable y comunicarla al trabajador.
- Informar de los controles que se podrán realizar y sus consecuencias.
- Garantizar la proporcionalidad: no se puede acceder al contenido de los correos personales del trabajador aunque se usen equipos de la empresa.

6.6. Sistemas internos de denuncia (Whistleblowing)

La Ley 2/2023 de protección de informantes obliga a muchas empresas a disponer de un canal de denuncias interno. La AEPD recuerda que:

- Tanto denunciante como denunciado deben ser informados del tratamiento de sus datos.
- Los datos deben suprimirse a los 3 meses si no se ha iniciado investigación, salvo que deban conservarse como evidencia de un sistema de prevención penal.

MÓDULO 7 – Seguridad, Brechas y Notificación de Incidentes

Duración: 2 horas | Nivel: Básico

7.1. Medidas de seguridad obligatorias

El artículo 32 del RGPD exige al responsable del tratamiento aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Entre ellas:

- Seudonimización y cifrado de los datos personales.
- Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas.
- Capacidad de restaurar la disponibilidad y el acceso a los datos en caso de incidente físico o técnico.
- Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas.

7.2. ¿Qué es una brecha de seguridad?

El artículo 4.12 RGPD define una brecha de seguridad como «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos».

Ejemplos frecuentes:

- Pérdida o robo de un ordenador portátil, móvil o memoria USB con datos de clientes o empleados.
- Envío accidental de un correo con datos personales a un destinatario incorrecto.
- Ataque de ransomware que cifra los sistemas y hace inaccesibles los datos.
- Acceso no autorizado a una base de datos por parte de un ex-empleado.
- Destrucción accidental de documentación con datos personales sin procedimiento establecido.

7.3. Obligación de notificación

> **PLAZO MÁXIMO: 72 HORAS**
> *Cuando se produce una brecha de seguridad, el responsable del tratamiento debe notificarla a la AEPD en un plazo máximo de 72 horas desde que tenga conocimiento de ella (Art. 33 RGPD). Si la brecha puede suponer un alto riesgo para los derechos y libertades de las personas, también deberá comunicarse a los propios afectados (Art. 34 RGPD).*

¿Qué debes hacer tú como trabajador?

9. Detecta el incidente: cualquier acceso no autorizado, pérdida de datos o comportamiento inusual del sistema.
10. Comunícalo de inmediato a tu supervisor o al responsable de protección de datos de la empresa.

11. No intentes resolver la situación por tu cuenta ni ocultes el incidente.
12. Conserva toda evidencia disponible (correos, capturas, dispositivos afectados).
13. Colabora con la investigación interna que se ponga en marcha.

7.4. Evaluación de Impacto en Protección de Datos (EIPD / DPIA)

El artículo 35 del RGPD obliga a realizar una Evaluación de Impacto en la Protección de Datos (DPIA) cuando un tipo de tratamiento, en particular si utiliza nuevas tecnologías, pueda suponer un alto riesgo para los derechos de las personas. Es obligatoria, entre otros casos, en:

- Tratamiento sistemático y extensivo basado en elaboración de perfiles.
- Tratamiento a gran escala de categorías especiales de datos.
- Observación sistemática a gran escala de zonas de acceso público.

MÓDULO 8 – Derechos Digitales en el Trabajo

Duración: 1 hora | Nivel: Básico

El Título X de la LOPDGDD incorpora un catálogo de derechos digitales que afectan directamente al entorno laboral. Es fundamental que los trabajadores los conozcan:

8.1. Derecho a la desconexión digital (Art. 88 LOPDGDD)

Los trabajadores tienen derecho a no responder comunicaciones digitales de trabajo fuera del horario laboral establecido. La empresa debe elaborar una política interna de desconexión digital y negociarla con los representantes de los trabajadores. Este derecho no impide la guardia o turno de disponibilidad pactados expresamente.

8.2. Derecho a la intimidad en el uso de dispositivos digitales (Art. 87 LOPDGDD)

Los trabajadores tienen derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por la empresa. El empleador puede acceder a los contenidos derivados del uso con fines laborales, pero debe informar previamente de los criterios de utilización y de los controles que podrá efectuar.

8.3. Derecho a la intimidad ante videovigilancia y grabación de sonidos (Art. 89 LOPDGDD)

Los empleadores solo pueden tratar imágenes obtenidas mediante sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores en los términos previstos en el Estatuto de los Trabajadores, siempre en el marco de sus funciones legales y con los límites inherentes a ellas.

8.4. Derecho a la intimidad ante la utilización de sistemas de geolocalización (Art. 90 LOPDGDD)

Los empleadores pueden tratar los datos obtenidos a través de sistemas de geolocalización para el control de los trabajadores cuando se cumplan los requisitos de información previa, proporcionalidad y limitación de finalidad.

8.5. Derechos digitales ante la inteligencia artificial y la toma de decisiones automatizadas

En 2025 la AEPD ha publicado guías específicas sobre IA agéntica y protección de datos. Los trabajadores no pueden ser objeto de decisiones con efectos jurídicos significativos basadas únicamente en el tratamiento automatizado, sin intervención humana, salvo excepciones legalmente previstas.

Régimen Sancionador

El incumplimiento de la normativa de protección de datos puede acarrear sanciones de enorme cuantía tanto para la organización como, en determinados casos, para los propios trabajadores responsables:

TIPO DE INFRACCIÓN	CONDUCTA EJEMPLO	SANCIÓN MÁXIMA
Muy grave (Art. 83.5 RGPD)	Tratamiento sin base jurídica. Violación de datos especialmente protegidos.	**20.000.000 € o 4% facturación anual**
Grave (Art. 83.4 RGPD)	No atender derechos de los interesados. Falta de acuerdo con encargado.	**10.000.000 € o 2% facturación anual**
Leve (Art. 74 LOPDGDD)	Incumplimiento de principio de transparencia. No notificar brechas menores.	**40.000 € (puede reducirse por atenuantes)**

IMPORTANTE

Las sanciones de la AEPD son públicas y pueden afectar gravemente a la reputación de la empresa. La responsabilidad del trabajador puede también derivar en acciones disciplinarias internas, incluyendo el despido disciplinario, e incluso responsabilidad penal en los supuestos más graves (Arts. 197 y ss. del Código Penal).

MÓDULO 9 – Evaluación Final y Registro de Formación

Duración: 1 hora | Nivel: Básico

9.1. Evaluación de conocimientos

Al finalizar el curso, cada participante realizará una prueba de evaluación de conocimientos con las siguientes características:

- Formato: cuestionario de respuesta múltiple (20 preguntas).
- Tiempo máximo: 30 minutos.
- Puntuación mínima para superar el curso: 70% de respuestas correctas (14/20).
- Los participantes que no superen la prueba podrán realizar una segunda convocatoria.

9.2. Documentación para acreditar el cumplimiento

Para que la formación pueda ser invocada ante una inspección de la AEPD, de la Inspección de Trabajo o en el marco de una auditoría interna o externa, la empresa debe conservar:

- Programa del curso (este manual) con indicación de contenidos y número de horas.
- Hoja de asistencia firmada por cada participante con fecha, nombre, DNI y firma.
- Resultado de la evaluación de cada participante.
- Diploma o certificado de aprovechamiento entregado a cada asistente.
- Evidencia de la entidad o persona que impartió la formación.

RECOMENDACIÓN DE LA AEPD

Según la Guía de relaciones laborales de la AEPD (dic. 2025), la formación debe estar alineada con los tratamientos reales de la empresa, ser periódica y documentarse de forma que pueda acreditarse ante la autoridad de control. Se recomienda repetirla con periodicidad mínima anual o cuando se produzcan cambios normativos o en los tratamientos de la organización.

9.3. Hoja de Asistencia y Firma

Nº	Nombre y Apellidos	DNI/NIE	Firma
1			
2			
3			
4			
5			
6			
7			
8			

9			
10			

Docente/Responsable del curso: _____ Fecha: _____ Firma: _____

Referencias Normativas y Documentales

Normativa europea:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD).
- Carta de Derechos Fundamentales de la Unión Europea – Art. 8.

Normativa española:

- Constitución Española, Art. 18.4.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). BOE-A-2018-16673.
- Real Decreto Legislativo 2/2015 – Estatuto de los Trabajadores (Arts. 20.3, 34.9, 87-91).
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas.
- Real Decreto 311/2022, de 3 de mayo – Esquema Nacional de Seguridad (ENS).
- Ley 30/2015, de 9 de septiembre, por la que se regula el Sistema de Formación Profesional para el Empleo en el ámbito laboral.

Guías y documentos de la AEPD:

- Guía sobre la protección de datos en las relaciones laborales – AEPD (diciembre 2025). Disponible en: aepd.es
- Guía sobre control de presencia mediante sistemas biométricos – AEPD (en revisión 2025).
- Guía sobre inteligencia artificial agéntica desde la perspectiva de la protección de datos – AEPD (2025).

Organismos de referencia:

- Agencia Española de Protección de Datos (AEPD): www.aepd.es
- Comité Europeo de Protección de Datos (CEPD/EDPB): edpb.europa.eu
- Fundación Estatal para la Formación en el Empleo (FUNDAE): www.fundae.es
- Servicio Público de Empleo Estatal (SEPE): www.sepe.es

AVISO LEGAL

Este manual ha sido elaborado con fines formativos. El contenido refleja la normativa vigente en el momento de su redacción (2025-2026). La empresa u organización que lo utilice es responsable de actualizar el contenido ante cambios normativos y de adaptarlo a su actividad concreta.

Revisión recomendada: anual o ante cualquier modificación relevante del RGPD, la LOPDGDD o las guías de la AEPD.