3. Normativa que protege los datos personales (LOPD)

La normativa que protege los datos personales, comúnmente referida por sus siglas **LOPD**, constituye el marco legal diseñado para garantizar y proteger el derecho fundamental de las personas físicas a su honor e intimidad personal y familiar en relación con el tratamiento de su información. Esta legislación no solo regula cómo las empresas y organismos públicos deben recolectar, almacenar y utilizar los datos para asegurar su confidencialidad e integridad, sino que también otorga a los ciudadanos el poder de control sobre su propia información.

Aunque históricamente se basó en la Ley Orgánica 15/1999, en la actualidad este marco jurídico ha evolucionado hacia la **Ley Orgánica 3/2018 (LOPDGDD)** y el **Reglamento General de Protección de Datos (RGPD)** europeo, estableciendo un sistema más estricto donde la prioridad es la seguridad proactiva de los ficheros para evitar el uso indebido, la alteración o el acceso no autorizado a la información sensible de los individuos.

3.1 Protección de datos a nivel Profesional y Personal

La protección de datos se estructura como una relación de correspondencia obligatoria entre dos vertientes complementarias: la profesional (deberes) y la personal (derechos). En el **ámbito profesional**, la normativa convierte a las empresas, autónomos e instituciones en "responsables del Tratamiento". Estos tienen el deber jurídico, bajo el principio de "responsabilidad proactiva", de aplicar las medidas técnicas y organizativas necesarias como el cifrado, el control de accesos o las copias de seguridad para garantizar que la información no sufra alteraciones, pérdidas o accesos no autorizados. El incumplimiento de estas obligaciones, que incluye el deber de secreto y la notificación de brechas de seguridad, puede derivar en graves sanciones administrativas y económicas.

Como contrapartida, en el **ámbito personal**, la legislación sitúa al ciudadano en el centro como el dueño legítimo de sus datos (el "interesado"). Esto le otorga el poder de controlar su información mediante el ejercicio de los derechos fundamentales (Acceso, Rectificación, Supresión, Oposición, Portabilidad y Limitación), garantizando así que su privacidad e intimidad sean respetadas frente al uso tecnológico y automatizado de sus datos personales.

3.2 Medidas de Seguridad: Evolución y Clasificación de Niveles

Para garantizar la integridad y confidencialidad de la información, la normativa establece un marco de medidas de seguridad que las organizaciones deben implementar obligatoriamente.

Históricamente, este sistema se regía por el **Real Decreto 1720/2007**, que clasificaba los ficheros en tres niveles rígidos (Básico, Medio y Alto) dependiendo de la sensibilidad de los datos. Sin embargo, es fundamental destacar el cambio de paradigma introducido con la aplicación efectiva del **RGPD** en mayo de 2018 y la **LOPDGDD 3/2018**. La normativa actual eliminó la obligatoriedad de estos niveles preestablecidos y los sustituyó por el principio de "análisis de riesgos". No obstante, la Agencia Española de Protección de Datos (AEPD) sigue recomendando utilizar las medidas del antiguo reglamento como guías de buenas prácticas y estándares de seguridad válidos para cumplir con la ley vigente.

El Nivel Básico constituye el escalón fundamental de seguridad y se aplica a ficheros que contienen datos identificativos o personales que no revelan aspectos sensibles de la personalidad ni de la economía (por ejemplo: nombre, DNI, dirección, teléfono o número de cuenta bancaria simple). En este nivel, las medidas de seguridad se centran en la gestión operativa: es obligatorio disponer de un documento de seguridad actualizado, establecer mecanismos de identificación y autenticación de usuarios (contraseñas), gestionar las incidencias y realizar copias de seguridad (backups) con una periodicidad mínima semanal para garantizar la recuperación de los datos.

El Nivel Medio se aplica cuando el tratamiento de datos ofrece una visión sobre la personalidad o el comportamiento del individuo, incluyendo datos relativos a la solvencia patrimonial, crédito, infracciones administrativas o penales, y datos tributarios o de la Seguridad Social. Al aumentar el riesgo, las medidas de seguridad se endurecen respecto al nivel anterior. Es obligatorio designar a un responsable de Seguridad específico y restringir el acceso físico a los servidores donde se alojan los datos. Además, se introduce una medida de control clave: la obligación de realizar una auditoría de seguridad, interna o externa, al menos cada dos años, para verificar el cumplimiento de la normativa.

El Nivel Alto se reserva para la información especialmente protegida o sensible, cuyo uso indebido podría causar discriminación o daños graves al ciudadano. Esto incluye datos de ideología, religión, creencias, origen racial, vida sexual, violencia de género y, muy especialmente, datos de salud. Las medidas técnicas en este nivel son críticas: la información debe viajar cifrada (encriptada) a través de redes de telecomunicaciones y en dispositivos portátiles. Asimismo, es obligatorio mantener un registro de accesos exhaustivo que identifique qué usuario accedió a qué dato concreto y en qué momento, y conservar una copia de seguridad

en una ubicación física diferente a la del centro de procesamiento de datos principal para prevenir desastres.

El cambio sustancial se produjo con la entrada en vigor del Reglamento Europeo (RGPD). La ley exige a la empresa realizar una "Evaluación de Impacto". La organización debe analizar qué riesgos específicos tiene su sistema y decidir qué medidas aplica. Si el riesgo es alto, acabará aplicando cifrado y auditorías (similares al antiguo Nivel Alto), pero la responsabilidad de decidirlo recae sobre la empresa, no sobre una lista cerrada de la ley.

Nivel de Seguridad	**Tipo de Datos (Datos de los ficheros)**	**Características y Medidas de Seguridad**
NIVEL BÁSICO	**Datos identificativos y generales:** • Nombre y apellidos. • Dirección, teléfono, email. • DNI / NIF. • Datos bancarios simples (nº cuenta). • Cualquier dato que no entre en los niveles superiores.	**Gestión básica:** • **Identificación y Autenticación:** El personal debe tener usuario y contraseña propios. • **Copias de Seguridad (Backup):** Obligatorio realizarlas periódicamente (mínimo semanalmente) y verificar que funcionan. • **Gestión de incidencias:** Tener un registro de cualquier problema de seguridad. • **Actualización:** Mantener el software actualizado.
NIVEL MEDIO	**Datos sobre personalidad o economía:**	**Control y Auditoría:** • **Responsable de Seguridad:** Nombrar a una persona encargada.

	• Infracciones administrativas o penales. • Solvencia patrimonial o crédito. • Datos de Hacienda o Seguridad Social. • Datos que evalúen la personalidad o comportamiento de los individuos.	• **Auditoría:** Realizar una auditoría interna o externa cada 2 años obligatoriamente. • **Control de acceso físico:** Restringir el acceso a las salas donde están los servidores. • **Gestión de soportes:** Control estricto de entrada/salida de discos duros o USBs.
NIVEL ALTO	**Datos Especialmente Protegidos (Sensibles):** • Ideología, religión y creencias. • Origen racial. • **Salud** (historiales médicos) y vida sexual. • Violencia de género. • Datos policiales sin consentimiento.	**Seguridad Crítica:** • **Cifrado (Encriptación):** Los datos deben viajar cifrados por la red y en dispositivos portátiles. • **Copias de respaldo externas:** Una copia de seguridad debe guardarse en un edificio diferente al de los servidores. • **Registro de accesos:** Se debe guardar un "log" (registro) de *quién* accedió, *cuándo* y a *qué dato* concreto accedió.

Bibliografía

- **Para las Obligaciones Profesionales (responsable del tratamiento):**

- *Fuente:* Agencia Española de Protección de Datos (AEPD).
- *Enlace:* https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes.

- **Para las Medidas de Seguridad en Empresas (INCIBE):**
  - *Fuente:* Instituto Nacional de Ciberseguridad (INCIBE) - Guía RGPD para empresas.
  - *Enlace:* https://www.incibe.es/empresas/te-ayudamos/rgpd-para-pymes.

- **Para los Derechos Personales (Ciudadanos):**
  - *Fuente:* Agencia Española de Protección de Datos (AEPD).
  - *Enlace:* https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos.

- **Texto Legal Consolidado:**
  - *Fuente:* BOE (Ley Orgánica 3/2018).
  - *Enlace:* https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673.

- **Fuente de los Niveles (Básico, Medio, Alto):**
  - *Fuente:* Real Decreto 1720/2007 (Reglamento de desarrollo de la LOPD).
  - *Enlace:* https://www.boe.es/buscar/act.php?id=BOE-A-2008-979 (Ver Título VIII).

- **Fuente del Cambio de Normativa (Situación Actual):**
  - *Fuente:* AEPD - Guía del Reglamento General de Protección de Datos.
  - *Enlace:* https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf

- **Fuente sobre Ciberseguridad y Medidas Técnicas:**
  - *Fuente:* INCIBE - Protección de la información.
  - *Enlace:* https://www.incibe.es/empresas/guias/proteccion-datos