1. Evolución y Objetivo de la Normativa

El objetivo de la LOPD es regular cómo las empresas y organismos recolectan y usan los datos, asegurando su confidencialidad y otorgando el control al ciudadano sobre su información.

• **Evolución:** Aunque históricamente se basaba en la Ley Orgánica 15/1999, el marco actual se rige por el **RGPD** (europeo) y la **LOPDGDD 3/2018** (española).

• **Enfoque actual:** Se ha pasado de un sistema rígido a uno de **seguridad proactiva**, donde la prioridad es evitar accesos no autorizados y usos indebidos mediante un análisis de riesgos continuo,.

2. Doble Vertiente: Profesional y Personal

La normativa estructura la protección de datos en una relación de derechos y deberes entre dos figuras clave:

• **Ámbito Profesional (El Responsable del Tratamiento):**

◦ Empresas, autónomos e instituciones tienen la obligación de aplicar la **"responsabilidad proactiva"**. Esto implica implementar medidas técnicas (cifrado, copias de seguridad) para evitar alteraciones o pérdidas de datos.

◦ El incumplimiento de estas medidas o del deber de secreto puede conllevar graves sanciones.

• **Ámbito Personal (El Interesado):**

◦ El ciudadano es el dueño de sus datos y posee derechos fundamentales para controlarlos: **Acceso, Rectificación, Supresión, Oposición, Portabilidad y Limitación**.

3. Clasificación de las Medidas de Seguridad

Aunque la normativa actual (RGPD) sustituyó los niveles rígidos por el principio de "análisis de riesgos" y la "Evaluación de Impacto",, la Agencia Española de Protección de Datos (AEPD) sigue recomendando utilizar la clasificación clásica como guía de buenas prácticas.

Los niveles se dividen según la sensibilidad de los datos tratados:

A. Nivel Básico (Datos identificativos)

• **Tipo de datos:** Nombre, DNI, dirección, teléfono, nº de cuenta bancaria simple,.

• **Medidas obligatorias:**

◦ Documento de seguridad actualizado.

◦ Identificación y autenticación (usuarios y contraseñas propios),.

◦ **Copias de seguridad (Backups):** Mínimo una vez a la semana,.

◦ Gestión de incidencias y actualización de software.

B. Nivel Medio (Datos de personalidad o economía)

• **Tipo de datos:** Infracciones administrativas/penales, solvencia patrimonial (crédito), datos tributarios, seguridad social o análisis de comportamiento/personalidad,.

• **Medidas adicionales (sumadas a las básicas):**

◦ Nombrar un **Responsable de Seguridad**,.

◦ **Auditoría:** Obligatoria cada 2 años (interna o externa),.

◦ Control de acceso físico a los servidores y gestión estricta de la entrada/salida de soportes (USBs, discos duros),.

C. Nivel Alto (Datos especialmente protegidos/sensibles)

• **Tipo de datos:** Ideología, religión, origen racial, vida sexual, violencia de género y, especialmente, **datos de salud**,.

• **Medidas críticas:**

◦ **Cifrado (Encriptación):** La información debe viajar cifrada por la red y en dispositivos portátiles,.

◦ **Registro de accesos:** Un "log" exhaustivo que guarde quién accedió, cuándo y a qué dato concreto,.

◦ **Copia de respaldo externa:** Una copia de seguridad debe guardarse en una ubicación física (edificio) diferente a la de los servidores principales para prevenir desastres,.

Una analogía para entender los niveles de seguridad

Para visualizar mejor la clasificación de seguridad que explica el texto, imagina que estás guardando objetos de valor:

• **Nivel Básico (Tu casa):** Guardas tu correspondencia y facturas. Necesitas una llave para entrar (usuario/contraseña) y de vez en cuando haces fotocopia de los papeles importantes (copia de seguridad semanal).

• **Nivel Medio (Un banco):** Guardas dinero e historial financiero. Ya no basta con una llave; necesitas un guardia de seguridad (Responsable de Seguridad), cámaras y controles estrictos de quién entra a la cámara acorazada (control físico), además de inspecciones regulares (auditorías).

• **Nivel Alto (Un laboratorio de alta seguridad):** Guardas secretos de estado o expedientes médicos vitales. La información es tan delicada que si sale del edificio va en un maletín blindado (cifrado), se registra cada huella dactilar de quien toca un archivo (registro de accesos) y se guarda una copia idéntica en un búnker en otra ciudad por si el edificio principal se incendia (copia externa).