






**SOLUCIONES INTEGRALES EN
PROTECCIÓN DE DATOS DE
CARÁCTER PERSONAL**

Descripción de servicio

MARCO NORMATIVO LEGAL BÁSICO:

La siguiente legislación configura, básicamente, el actual marco normativo nacional de obligado cumplimiento para las organizaciones (tanto públicas como privadas), en materia de protección de datos.

-  **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)**
-  **Sentencia del Tribunal Constitucional 292/2000** (que define el derecho a la Protección de Datos personales como un derecho fundamental independiente)
-  **RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** (en adelante, Reglamento de desarrollo de la LOPD o RLOPD)

CONCEPTO DE DERECHO A LA PROTECCION DE DATOS:

- ◎ *“...El contenido del Derecho fundamental a la protección de datos consiste en un **poder de disposición y de control** sobre los datos personales que faculta a la persona para **decidir** cuáles de éstos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo **saber quién posee esos datos** personales **y para qué, pudiendo oponerse a esa posesión o uso...**”*

¿Por qué adaptarse a la LOPD?

- La información que manejan las empresas y el tratamiento que realiza de la misma, está sujeta a una legislación estricta: Ley Orgánica de Protección de Datos (LOPD)
- La adaptación a la LOPD es de obligado cumplimiento para todas las empresas que traten automatizadamente datos de carácter personal (de clientes, proveedores, empleados, potenciales, etc.)
- Es un primer paso para la adopción en la empresa de una política de seguridad que establezca unos principios mínimos de gestión de la seguridad interna y mejora la calidad en la gestión administrativa de procesos basados en las TIC.
- Permite exonerar de responsabilidad a la empresa ante posibles acciones ilegales de sus empleados y evita riesgos de denuncia de junto a desprestigio institucional respecto a la actividad desarrollada (servicios tecnológicos)

¿Por qué adaptarse a la LOPD?

- El régimen sancionador es el más duro de Europa, junto con Grecia.

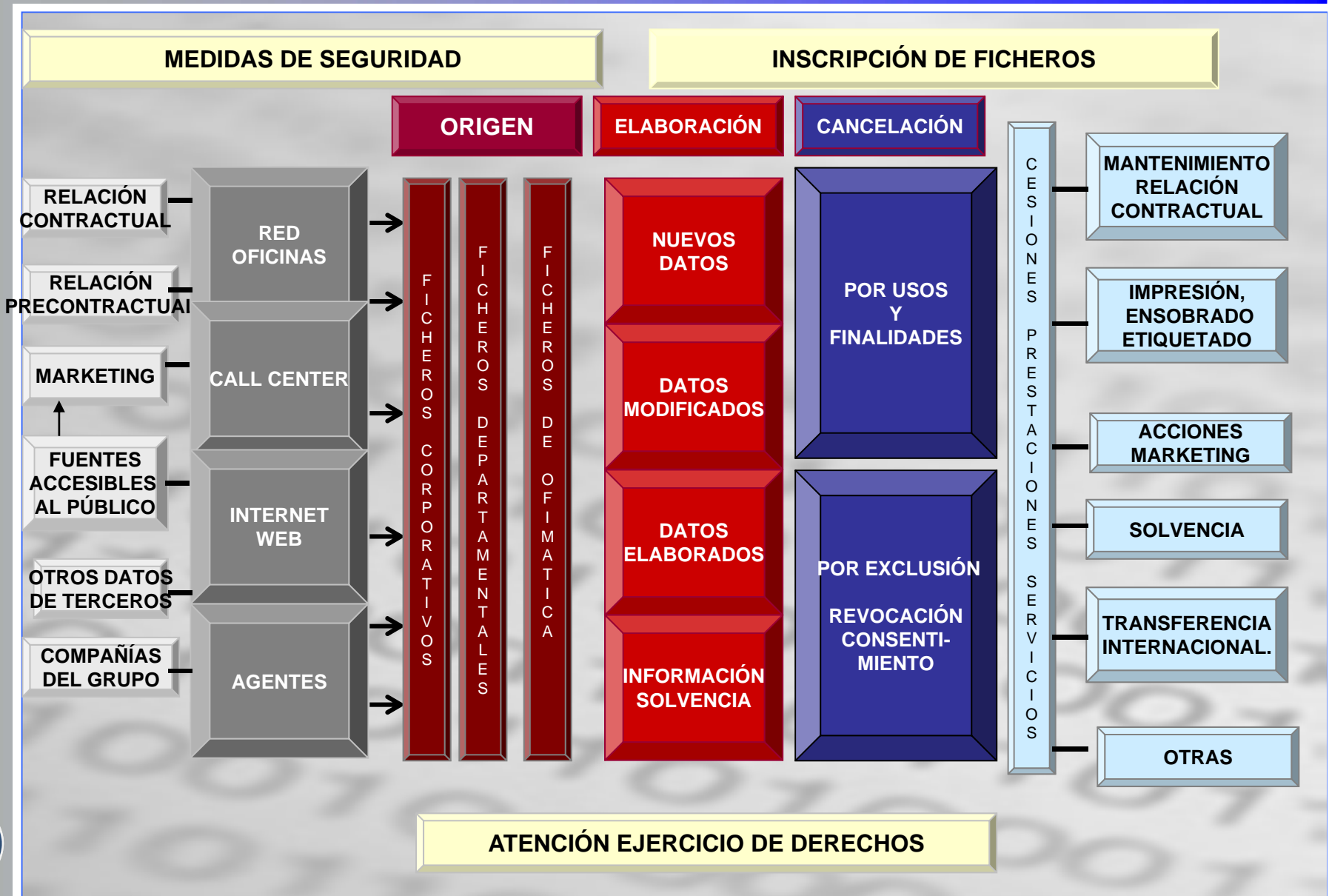
<u>Infracciones (art. 44 LOPD)</u>	<u>Sanciones (art. 45 LOPD)</u>
Infracción Leve	de 601,01 a 60.101,21 €
Infracción Grave	de 60.101,21 a 300.506,05 €
Infracción Muy Grave	de 300.506,05 a 601.012,10 €
- Además de implicar un elevado riesgo económico por sanción, supone una potencial pérdida de imagen institucional, de difícil valoración, ya que las sanciones se hacen públicas en la página web (www.agpd.es) del órgano de control: La Agencia Española de Protección de Datos (AEPD).
- **La cuantía total de las sanciones impuestas por la AEPD a entidades privadas en 2009 asciende a 24,8 millones de euros.**
- Las organizaciones más sensibilizadas en la materia han aprovechado la adecuación a la citada normativa para convertir su cumplimiento en un elemento diferenciador y de valor añadido, respecto a la competencia del sector.



- Establecer medidas para **prevenir** riesgos y **apoyo** en las tomas de decisión de riesgos asumidos.
- **Explotar** la información de forma rentable y legal.
- **Control** y **prevención** de incumplimientos y actuaciones conflictivas.
- **Cobertura** para realizar acciones presentes y futuras.
- Es un primer paso (obligatorio) para establecer un adecuado **sistema de gestión de la seguridad** de la información en la organización.

- **Inscripción de ficheros** en el Registro General de Protección de Datos (Art. 25 y 26 LOPD; Título V: arts. 52 al 62 RD 1720/2007).
- **Elaboración del Documento de Seguridad** de los datos (Art. 9 LOPD; Título VIII – arts. 79 a 114 RD 1720/2007), donde se recogen los diferentes niveles de medidas de seguridad obligatorias, atendiendo a la tipología de datos tratados.
- **Adaptación de los procesos internos** en todo lo relativo a tratamiento de datos de carácter personal (cesiones de datos, prestaciones de servicios por terceros) e inclusión de cláusulas contractuales en cualquier documento que recabe datos de carácter personal. Inclusión de un módulo de revisión de las obligaciones de la LSSI-CE (Internet). Estos servicios pueden ser globales o departamentales, atendiendo al alcance acordado.
- **Atención al ejercicio de los derechos** de los afectados.
- **Formación** de personal en materia de protección de datos
- **Soporte y mantenimiento continuos** (revisión de la implantación de las medidas, informes jurídico-técnicos, defensa ante inspección de la AEPD, auditoría bienal, etc)

- ⦿ Previamente a la presentación de la oferta, se efectúa una toma de datos para elaborar un presupuesto personalizado y adecuado a la empresa/sector/área o departamento.
- ⦿ Documentación de arranque del proyecto (kick-off) con revisión de la planificación, objetivos, definición de interlocutores
- ⦿ Identificación de todos los ficheros con datos de carácter personal para su clasificación y agrupación con arreglo a criterios lógicos
- ⦿ Entrevistas con Responsables de Departamento con el fin de recabar información sobre los procesos de los distintos departamentos (Recursos Humanos, Informática, Comercial, Marketing) y detectar deficiencias respecto de los requerimientos LOPD
- ⦿ Elaboración de Entregables: preparación de la documentación para la transferencia de conocimientos al cliente (propuesta de inscripción de ficheros, informe técnico de riesgos y recomendaciones, documento de seguridad, etc)
- ⦿ Procedimiento centralizado para la atención al ejercicio de los derechos
- ⦿ Formación, en caso de ser solicitada al personal de la empresa
- ⦿ Servicio de mantenimiento: para el seguimiento y soporte de la actividad de la empresa después de la implantación (incluida la defensa de procedimientos sancionadores o tutelas de derecho incoados por la AEPD)



Obligación adicional para entidades que desarrollan software

- ◉ Desde abril de 2008, el Reglamento de desarrollo de la LOPD (RD 1720/2007, de 21 de diciembre) establece expresamente en su Disposición adicional única:

“Productos de software. Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento”.

Es decir, el RLOPD determina que todo software comercializado debe tener implementadas con carácter obligatorio, como mínimo, las medidas de seguridad que establece la normativa.

Recordar que esta Ley no solo establece condiciones legales para tratar datos personales, sino que también establece las medidas de seguridad (tecnico-organizativas) que necesariamente deben proteger a dicha información.