

Practica Seguridad La Ley Orgánica de Protección de Datos (LOPD)



1. Leyes de protección de datos que han existido en la historia reciente de España.....	3
1.1 LEY ORGÁNICA 5/1992.....	3
1.2 LA LEY ORGÁNICA 15/1999.....	3
1.3 CONFIGURACIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS POR PARTE DEL TRIBUNAL CONSTITUCIONAL.....	3
a) La Sentencia 254/1993, de 20 de julio de 1993 (RTC 1993, 254) del Tribunal Constitucional. Recurso de Amparo n.º 1827/1990: El Tribunal Constitucional otorga el amparo contra la denegación presunta por parte de la Administración Pública de información acerca de la existencia, contenido y finalidad de ficheros automatizados de titularidad pública en los que consten datos personales del actor y contra las dos decisiones judiciales que confirmaron aquella denegación.....	3
1.4 LA LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (LOPDGDD).....	4
2. Legislación actual y organismos básicos.....	4
2.1 Legislación actual.....	4
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD).....	4
Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)5	
Ley Orgánica 7/2021.....	6
2.2 Organismos básicos.....	6
Agencia Española de Protección de Datos (AEPD).....	6
Comité Europeo de Protección de Datos (CEPD).....	6
Organismos de otras comunidades.....	7
3. Normativa que protege los datos personales (LOPD).....	7
3.1 Protección de datos a nivel Profesional y Personal.....	7
3.2 Medidas de Seguridad: Evolución y Clasificación de Niveles.....	8
4. Normativa de los sistemas de información y comercio electrónico - LSSI-CE (Ley 34/2002)..	12
5. Bibliografía.....	15
Punto 1:.....	15
Punto 2:.....	15
Punto 3:.....	15
Punto 4:.....	16

1. Leyes de protección de datos que han existido en la historia reciente de España

1.1 LEY ORGÁNICA 5/1992.

Primera ley de protección de datos en España, limita el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

1.2 LA LEY ORGÁNICA 15/1999

Regula el tratamiento de los datos de carácter personal y los ficheros donde se contenían, sin importar el soporte en el cual fueran tratados; regular con detalle los derechos de las personas y las obligaciones de aquellos que creaban ficheros y trataban datos, ya fuera como responsables o encargados del tratamiento de los mismos.

1.3 CONFIGURACIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS POR PARTE DEL TRIBUNAL CONSTITUCIONAL.

- a) *La Sentencia 254/1993, de 20 de julio de 1993 (RTC 1993, 254)* del Tribunal Constitucional. *Recurso de Amparo n.º 1827/1990:* El Tribunal Constitucional otorga el amparo contra la denegación presunta por parte de la Administración Pública de información acerca de la existencia, contenido y finalidad de ficheros automatizados de titularidad pública en los que consten datos personales del actor y contra las dos decisiones judiciales que confirmaron aquella denegación.
- b) *La Sentencia del Tribunal Constitucional 94/1998, de 4 de mayo:* Sentencia posterior del TC, nos informa con claridad que nos encontramos ante un derecho fundamental, por el cual se garantiza a la persona la protección de sus datos, el control sobre sus propios datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados.
- c) *La Sentencia 292/2000, de 30 de noviembre del 2000 (RTC 2000, 292)* del Tribunal Constitucional: Establece un marco normativo robusto para el control de los datos personales, ampliando la protección más allá de la intimidad y garantizando un control efectivo sobre su uso, dándole al individuo el derecho a negarse a compartir sus datos, controlarlos, saber quién los maneja o controlarlos.

1.4 LA LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (LOPDGDD).

Adapta la normativa española al *Reglamento General de Protección de Datos (RGPD)* de la UE y completa sus disposiciones. Esta ley también garantiza los derechos digitales de la ciudadanía, como el derecho al olvido, la portabilidad de datos, la desconexión digital en el ámbito laboral, y establece normas para menores de edad y el tratamiento de datos de fallecidos.

2. Legislación actual y organismos básicos

2.1 Legislación actual

En la actualidad, la legislación informática de protección de datos se basa en dos leyes principales: el *Reglamento General de Protección de Datos (RGPD)* y la *Ley Orgánica 3/2018 (LOPDGDD)*.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

La *RGPD* es la normativa europea más estricta del mundo que protege los datos personales de los ciudadanos y les da mayor control sobre cómo se usan. Entró en vigor en 2018 y afecta a todas las empresas que estén en la UE o que ofrezcan servicios a las personas de la UE. Esta normativa establece derechos para las personas y obligaciones estrictas para las empresas, con sanciones muy altas en caso de incumplimiento.

Sus funciones principales son:

- a) Protege la privacidad de las personas en la era digital.
- b) Regula el tratamiento de datos personales, regulando cómo se recogen, almacenan, usan y transfieren.
- c) Otorga control a los ciudadanos sobre sus datos, permitiéndoles decidir cómo se utilizan.
- d) Impone obligaciones a empresas y organizaciones para garantizar un uso seguro y transparente.

Al estar sujetos a esta ley, las personas tienen derecho a saber qué datos tienen las empresas sobre ellos, a corregir datos que estén incorrectos y a pedir que se eliminen los datos. Además, podrán

solicitar trasladar sus datos a otro proveedor y oponerse a que se usen sus datos en ciertos contextos para beneficio de las empresas.

Las empresas, por otra parte, tendrán que avisar a los usuarios y pedir una autorización clara para poder usar sus datos, y tendrán que informar de cómo se van a usar sus datos exactamente. Tendrán que aplicar medidas para proteger totalmente la información, y caso de fuga de datos se tendrá que avisar a la autoridad y a los afectados. También estarán obligadas a documentar cómo se tratan los datos.

Si no se respetan estas normas, las empresas pueden tener sanciones muy elevadas.

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)

La *LOPDGDD* es la norma española que complementa al *RGPD* europeo. Se aprobó en diciembre de 2018, y se diseñó para adaptar la normativa española a la europea (*RGPD*) de una manera novedosa. Esta normativa ha añadido un bloque específico sobre derechos digitales, por ejemplo la desconexión laboral o el uso de datos en el ámbito educativo y laboral.

Sus funciones principales son:

- a) Adaptar el *RGPD* al contexto español, aclarando y desarrollando aspectos que el reglamento europeo deja abiertos.
- b) Reconocer los derechos generales de las personas, como el derecho a la seguridad o educación digital, o el derecho a la neutralidad de la red.
- c) Regular el tratamiento de datos personales,
- d) Establecer el régimen de protección de menores, fijando la edad mínima de consentimiento en 14 años.
- e) Definir las competencias de la *AEPD*, como atender reclamaciones de ciudadanos y supervisar el cumplimiento de la normativa.
- f) Regular el procedimiento sancionador en España, clasificando las infracciones y estableciendo sanciones económicas por gravedad y por el tamaño de la organización.
- g) Concretar cómo deben actuar empresas y administraciones en el tratamiento de datos personales en España.

Respecto a los derechos de los ciudadanos, se mantienen los anteriores impuestos por el *RGPD*, y se añaden derechos como a la desconexión laboral, a la educación digital, a la neutralidad de la red o la regulación del uso de dispositivos de videovigilancia y geolocalización. Además, establece en 14 años la edad mínima para que sus datos puedan ser tratados.

Respecto a las empresas, el *LOPDGDD* detalla cuándo es obligatorio nombrar un Delegado de Protección de Datos, cómo debe de gestionarse el bloqueo de datos cuando los datos no puedan ser eliminados, y más reglas específicas. Además, regula específicamente el ámbito laboral, como el uso de sistemas de vigilancia en el trabajo.

Ley Orgánica 7/2021

Aunque el *RGPD* y la *LOPDGDD* son las leyes principales en materia de protección de datos, la *Ley Orgánica 7/2021* también está presente porque se encarga específicamente del tratamiento de datos en el ámbito penal. Esta norma regula cómo deben manejarse los datos relacionados con infracciones, investigaciones y actuaciones de las autoridades policiales y judiciales. Así, complementa al *RGPD* y a la *LOPDGDD*, garantizando que incluso en contextos de seguridad y justicia se respeten los derechos y la protección de la información personal.

2.2 Organismos básicos

Agencia Española de Protección de Datos (AEPD)

La *AEPD* es el organismo público encargado de garantizar que en España se cumpla la normativa de protección de datos, tanto el *RGPD* como la *LOPDGDD*. Su función principal es proteger los derechos de las personas sobre sus datos personales.

Sus funciones principales son:

- a) Supervisar que empresas, administraciones y organizaciones traten los datos de forma legal.
- b) Atender y resolver reclamaciones de ciudadanos.
- c) Imponer sanciones cuando se incumple la normativa.
- d) Ofrecer guías, informes y recomendaciones para ayudar a cumplir la ley.
- e) Colaborar con autoridades europeas dentro del Comité Europeo de Protección de Datos.

Comité Europeo de Protección de Datos (CEPD)

El *CEPD* es el organismo que coordina la aplicación del *RGPD* en toda la Unión Europea. Está formado por todas las autoridades nacionales de protección de datos incluida la *AEPD* y garantiza que las normas se interpreten igual en todos los países.

Sus funciones principales son:

- a) Supervisar cómo aplican el *RGPD* las autoridades de cada país.
- b) Emitir directrices y recomendaciones para aclarar cómo aplicar el *RGPD*.
- c) Coordinar los casos transfronterizos entre distintos países.
- d) Tomar decisiones vinculantes cuando hay conflictos entre autoridades.

- e) Promover una protección de datos uniforme en toda la UE.

Organismos de otras comunidades

Hay comunidades en las que tienen autoridades específicas en las regiones en las que tienen competencia. Por ejemplo, en Cataluña tienen la *APDCAT* (Autoridad Catalana de Protección de Datos), en el País Vasco tienen la *AVPD* (Agencia Vasca de Protección de Datos) y en Andalucía tienen el *CTPDA* (Consejo de Transparencia y Protección de Datos de Andalucía).

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	<p>Datos identificativos y generales:</p> <ul style="list-style-type: none"> • Nombre y apellidos. • Dirección, teléfono, email. • DNI / NIF. • Datos bancarios simples (nº cuenta). • Cualquier dato que no entre en los niveles superiores. 	<p>Gestión básica:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• Infracciones administrativas o penales.• Solvencia patrimonial o crédito.• Datos de Hacienda o Seguridad Social.• Datos que evalúen la personalidad o comportamiento de los individuos.	Control y Auditoría: <ul style="list-style-type: none">• Responsable de Seguridad: Nombrar a una persona encargada.• 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	<p>Datos Especialmente Protegidos (Sensibles):</p> <ul style="list-style-type: none"> • Ideología, religión y creencias. • Origen racial. • Salud (historiales médicos) y vida sexual. • Violencia de género. • Datos policiales sin consentimiento. 	<p>Seguridad Crítica:</p> <ul style="list-style-type: none"> • 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 <i>quién accedió, cuándo y a qué dato concreto accedió</i>.
-------------------	---	--

4. Normativa de los sistemas de información y comercio electrónico - LSSI-CE (Ley 34/2002)

Las siglas *LSSI-CE* se refieren a “*Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*”. La extraordinaria expansión de las redes de comunicaciones electrónicas y en especial de Internet así como la incorporación de esta última a la vida económica y a la actividad comercial, hacen necesario establecer un marco jurídico adecuado que genere en todos los actores intervenientes la confianza necesaria para el empleo de este nuevo medio. Es la principal ley de los sistemas de información y comercio electrónico y se encarga de regular los servicios y transacciones electrónicas en España. Su principal objetivo es crear un marco legal que garantice la transparencia y seguridad en las actividades comerciales por internet, desde la venta de productos hasta el envío de newsletters.

Se ha incorporado como resultado de la promulgación de la Directiva 2000/31/CE, del Parlamento Europeo que a su vez incluye determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio

electrónico). Se promulgó el día 11 de julio del año 2002, siendo introducida en el *BOE* (Boletín Oficial del Estado) el día siguiente.

Esta ley no se aplica solamente a las tiendas online. Cualquier empresa o usuario en internet que cumple cualquiera de las siguientes condiciones puede verse afectada por la *LSSI-CE* (*Ley 34/2002*):

- a) Tener una página web corporativa con formularios de contacto.
- b) Enviar correos electrónicos comerciales o newsletters.
- c) Publicar contenidos promocionales.
- d) Recibir ingresos por publicidad online.
- e) Ofrecer productos o servicios a través de internet.

Para cumplir con esta ley se deben respetar los siguientes aspectos:

- a) Tener aviso legal en la página o el servicio que se ofrece en internet.
- b) Tener y enseñar política de privacidad y de cookies.
- c) Tener y avisar de los términos y condiciones de uso.
- d) Enviar la información solamente cuando se tenga consentimiento expreso.
- e) Identificar al remitente y permitirle darse de baja.
- f) Informar y obtener consentimiento para las cookies.

El cumplimiento de la *LSSI* es fundamental para cualquier empresa o profesional que ofrezca servicios online en nuestro país. No cumplir con esta ley puede tener graves consecuencias legales, incluyendo multas y sanciones, así como la pérdida de confianza de los clientes.

En octubre de 2019, una clienta realizó una reclamación a la *Agencia Española de Protección de Datos (AEPD)* porque al consultar la página web de la aerolínea no aparecía la opción de rechazar las cookies. La usuaria se vio obligada a aceptar las cookies para seguir navegando y poder contratar un vuelo. En ese momento, decidió denunciar la situación a la *AEPD* que requirió información a la compañía respecto al asunto; sin embargo, la empresa no contestó hasta enero de 2020. Por su parte, Iberia alegó que su banner de cookies estaba siendo modificado en el momento en el que se produjo la denuncia y considera no hay base suficiente para abrir un expediente sancionador. “Llevaba trabajando desde junio de 2019 en el diseño de la solución de adaptación de la política de cookies a las exigencias del *Reglamento General de Protección de Datos y la Nueva Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales* siguiendo, las guías de buenas prácticas emitidas por las autoridades de control y muy especialmente la emitida por la Agencia el pasado mes de noviembre de 2019”. No obstante, la Agencia intentó verificar la información suministrada por Iberia y «se comprobó que además de seguir sin ofrecer la opción de rechazar todas las cookies, tal y

como se denunciaba, (...) varios puntos de la política de cookies de la página no se ajustaban a las recomendaciones».

El titular del sitio web es el responsable de los contenidos propios publicados y de los enlaces a terceros que puedan resultar ilícitos o engañosos.

Las funciones de supervisión, control y las actuaciones inspectoras se llevan a cabo por el Ministerio de Energía, Turismo y Agenda Digital, aunque la potestad sancionadora corresponde a la *Agencia Española de Protección de Datos*.

También cabe mencionar la regulación que trae esta ley a la prestación de servicios de la sociedad de la información, que no requiere autorización previa y se realiza en libre prestación si proviene de países de la UE/EEE. Solo pueden imponerse restricciones cuando el servicio afecte al orden público, la seguridad, la salud, la protección de consumidores, la dignidad o los menores. Las medidas deben ser proporcionadas, respetar los derechos fundamentales y, en ciertos casos, requerir intervención judicial. Si el servicio procede de otro Estado de la UE/EEE, antes de restringirlo se debe coordinar y notificar a dicho Estado y a la Comisión Europea, salvo urgencia.

La LSSI-CE(*Ley 34/2002*) se ha introducido en un momento en el que solamente el 17% de los hogares de España tenían Internet. El gobierno de aquel entonces había anticipado el éxito que iba a tener el Internet, así que ha decidido implementar esta ley para no tener que enfrentarse a ciertos problemas en el futuro. Se puede decir que impulsar esta ley fue un gran éxito, ya que en el año 2005, solamente 3 años después de impulsar la ley, el 50,6% de los hogares contaban con internet, en 2014 se trataba de un porcentaje de 74,4% y hoy en día se trata de un porcentaje cercano al 90%.

5. Bibliografía

Punto 1:

- **Para la Historia de la Protección de Datos:**
 - Fuente: Alba Legal.
 - Enlace: <https://www.albalegal.es/historia-de-la-proteccion-de-datos/>
 - **Para la Asistencia en la Generación de Contenido:**
 - Fuente: Google Gemini (IA).
 - Enlace: <https://gemini.google.com/>
-

Punto 2:

- **Para la Guía Completa del RGPD:**
 - Fuente: Imagina Formación.
 - Enlace: <https://imagineformacion.com/tutoriales/que-es-el-rgpd-guia-completa>
 - **Para el Reglamento de Protección de Datos de la UE:**
 - Fuente: Consejo de la Unión Europea (Consilium).
 - Enlace: <https://www.consilium.europa.eu/es/policies/data-protection-regulation/>
 - **Para la Ley Orgánica de Protección de Datos (LOPDGDD):**
 - Fuente: Boletín Oficial del Estado (Referencia a la Ley 3/2018).
-

Punto 3:

- **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>.
- **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>.
-

Punto 4:

- **Legislación LSSI (Ley 34/2002):**
 - Fuente: Boletín Oficial del Estado (BOE).
 - Enlace: <https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758>
- **Normativa Europea (Directiva 2000/31/CE):**
 - Fuente: Diario Oficial de la Unión Europea.
 - Enlace: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295>
- **Información sobre Obligaciones y Cambios 2025:**
 - Fuente: Global Suite Solutions.
 - Enlace:
<https://www.globalsuitesolutions.com/es/lssi-que-es-obligaciones-cambios-2025/>
- **Portal Oficial de la LSSI:**
 - Fuente: Ministerio para la Transformación Digital.
 - Enlace: <https://lssi.digital.gob.es/lssi>
- **Recurso Audiovisual (Video explicativo):**
 - Fuente: YouTube.
 - Enlace: <https://www.youtube.com/watch?v=RDbYDya0oio>
- **Guía de Comercio Electrónico en España:**
 - Fuente: Stripe Resources.
 - Enlace: <https://stripe.com/es/resources/more/ecommerce-law-in-spain-lssi>
- **Estadísticas de Acceso a Internet en Hogares (2025):**
 - Fuente: 21 Noticias.
 - Enlace:
<https://21noticias.com/2025/12/01/el-84-de-los-hogares-espanoles-tienen-ordenador-y-el-97-acceso-a-internet/>
- **Caso Práctico (Multas por Cookies):**
 - Fuente: Conversia.
 - Enlace:
<https://www.conversia.es/iberia-multada-por-incumplir-con-la-politica-de-cookies/>