

➤ *¿Qué es la LOPD?*

La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999 de 13 de diciembre (LOPD), tiene por objeto proteger y garantizar las libertades y los derechos fundamentales de las personas físicas, su honor e intimidad personal y familiar.

La LOPD establece unas obligaciones en relación a la protección de datos de carácter personal contenidos en ficheros automatizados y no automatizados (en papel) que poseen empresas y administraciones públicas, y que son tratados por éstas con diferentes finalidades: gestión de personal, proveedores, clientes, campañas de marketing, etc.

Obligaciones básicas de las empresas

En definitiva, todas las empresas deberán:

Declarar los ficheros automatizados (informáticos) y no automatizados (en papel) con datos de carácter personal a la Agencia de Protección de Datos.

Legitimar los datos personales de que dispone mediante el cumplimiento de los siguientes principios de la LOPD:

- Principio del **consentimiento del afectado**.
- Principio de **información al afectado**.
- Principio de **calidad de los datos**.

Proteger los ficheros automatizados y no automatizados para preservar la confidencialidad, integridad y disponibilidad de los datos siguiendo lo establecido en el Reglamento de Seguridad.

Como aspectos básicos se requiere:

- Disponer de un **Documento de Seguridad**.
- Definir e implantar los **Procedimientos** requeridos.
- Nombrar un **Responsable de Seguridad** (si se dispone de datos de nivel medio o alto).
- **Formar y concienciar** en materia de seguridad de la información a todo el personal que gestione datos personales.

➤ ***Tipos y niveles de datos***

Los datos de carácter personal se clasifican en tres niveles atendiendo a su naturaleza y finalidad. A cada nivel le corresponden unas medidas de seguridad, siendo las de nivel alto las más estrictas:

✓ **Nivel básico**

Todos los datos de carácter personal estarán, como mínimo, en este nivel.

A todos los ficheros con datos personales se les deberán aplicar las medidas de seguridad de nivel básico.

✓ **Nivel medio**

En general, los datos relativos a infracciones administrativas o penales, sobre solvencia patrimonial o crédito, sobre servicios financieros, y aquellos que permitan determinar un perfil de las personas.

A estos datos será de aplicación las medidas de nivel básico y las de nivel medio.

✓ **Nivel alto:**

En general, los datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

A estos datos se les aplicarán las medidas definidas para el nivel básico, el medio y el alto.

➤ ***¿A qué obliga la LOPD en materia de backup y recuperación de datos?***

NIVEL BAJO, MEDIO Y ALTO

Se deberán garantizar la restauración de los datos al momento anterior a producirse la pérdida. Realización de copias de backup al menos con una frecuencia semanal. (art.94.1 del Reglamento de Desarrollo de la LOPD (RLPOD), RD 1720/2007)

NIVELES MEDIO Y ALTO

Necesaria **autorización** para la ejecución de procedimientos de restauración de datos. (RLOPD art.100.2)

NIVEL ALTO

Almacenamiento externo de copias y procedimientos de restauración de datos. (RLOPD art.102).

➤ **Qué dice exactamente la normativa**

Art. 101.2. Cifrado de los datos La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos garantizando que dicha información no sea vista ni manipulada durante su transporte. Para la encriptación se recomienda un cifrado de 128 bits.

Art. 103. Registro de accesos El administrador no tiene acceso a los datos salvo autorización expresa del cliente. En el caso de necesitar ejecutar una recuperación en el data-center, el usuario debe proporcionar su clave de seguridad. El acceso queda registrado.

Art. 102. Copias de respaldo en un lugar diferente a aquél en que se encuentran los equipos informáticos que los tratan Es la funcionalidad principal de nuestras herramientas de backup online. Obligatorio en las copias para la protección de datos de alto nivel.

Art. 104. Transmisión de datos por redes de Telecomunicaciones Los datos se transmiten, cifrados y comprimidos, bajo un protocolo de comunicación seguro SSL (https).

Art. 94.2. Verificación periódica de la copia El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

 <p>MAST STORAGE MAST BACKUP ONLINE TÉRMINOS Y CONDICIONES DE USO</p> <p>El presente documento (en adelante, el "Contrato") constituye un contrato legalmente vinculante suscrito por usted y Mast Storage S.L. por el que se registrá la utilización, por parte de usted, del SERVICIO DE ALMACENAMIENTO INFORMÁTICO (BACKUP REMOTO), denominado MAST BACKUP ONLINE, en base a los siguientes:</p> <p>ANTECEDENTES:</p> <p>I.- El cliente es usuario de equipos informáticos, en los que es aconsejable disponer de medidas para seguridad del archivo de la información.</p> <p>II.- MAST dispone del software y demás medios precisos para prestar el servicio de almacenamiento remoto (backup) de la información, garantizando su seguridad y la total confidencialidad, a través de un procedimiento que permite el encriptado de dicha información, la cual sólo puede tratarse mediante una clave de encriptación de la que dispondrá únicamente el cliente tras personalizarla.</p> <p>III.- El objeto del presente contrato es la regulación de las condiciones de prestación del servicio de backup remoto por MAST al cliente.</p> <p>IV.- A los efectos de este contrato, las palabras que seguidamente se indican tendrán en el mismo, el significado que, asimismo, se especifica a continuación:</p> <p>ALMACENAMIENTO, O SERVICIO DE ALMACENAMIENTO (BACKUP): Custodia de la información remitida por el cliente, en equipos remotos de los que dispone MAST -a fin de garantizar al máximo la conservación de tal información-. Comprende no sólo la recepción de la información y su custodia sino los medios para facilitar el acceso por parte del cliente, para recuperar la información por vía informática.</p> <p>ID DE USUARIO: Nombre de usuario de acceso a la cuenta entre el cliente y MAST para la identificación de éste por vía informática; será expedida por MAST.</p> <p>CONTRASEÑA: Clave de acceso a la cuenta de usuario, asignada inicialmente por MAST, y personalizable por el cliente.</p> <p>CLAVE DE ENCRYPTACIÓN: El programa permite su personalización de forma que solo el cliente sea conocedor de ella; ello comporta que solo el cliente es responsable de que, en caso de su pérdida, no sea posible desencriptar la información.</p> <p>CLIENTE: El receptor de los servicios regulados en este contrato.</p> <p>1</p>	 <p>CERTIFICADO DE APROBACIÓN</p> <p>Certificamos que el Sistema de Gestión de Calidad de:</p> <p>OGIC INFORMATICA, S.L. ADAM DATACENTER C/ Travessera de Gràcia 342, 3ª planta 08025 Barcelona España</p> <p>ha sido aprobado por Lloyd's Register Quality Assurance de acuerdo con las siguientes Normas de Sistemas de Gestión de Calidad:</p> <p>ISO 9001:2008</p> <p>El Sistema de Gestión de Calidad es aplicable a:</p> <p>Servicios de ISP: housing, hosting y los servicios de comunicaciones asociados.</p> <table><tr><td>Aprobación</td><td>Aprobación Original:</td><td>23 Febrero 1998</td></tr><tr><td>Certificado No: SGI 3958507/11B</td><td>Certificado en Vigor:</td><td>09 Enero 2013</td></tr><tr><td></td><td>Caducidad del Certificado:</td><td>08 Enero 2016</td></tr></table> <p> Emitido por: LRQA, Ltd. Operaciones España</p>  <p><small>Este documento está sujeto a los términos y condiciones que aparecen al dorso 71 Fenchurch Street, London EC3A 4BS United Kingdom. Registration number 1893370. Este certificado está condicionado a que la compañía mantenga el sistema de calidad con los términos establecidos, lo que será manifestado por LRQA En caso de la falta de Actualización UKAS indica Anulación del certificado a menos que el cliente actualice su sistema por el Certificado de Acreditación UKAS.</small></p>	Aprobación	Aprobación Original:	23 Febrero 1998	Certificado No: SGI 3958507/11B	Certificado en Vigor:	09 Enero 2013		Caducidad del Certificado:	08 Enero 2016
Aprobación	Aprobación Original:	23 Febrero 1998								
Certificado No: SGI 3958507/11B	Certificado en Vigor:	09 Enero 2013								
	Caducidad del Certificado:	08 Enero 2016								