

**Usuarios Registrados**Usuario Contraseña [¿Olvidó su contraseña?](#)
**Registro**
**Periodistas:**
[Regístrese para ver sus contenidos personalizados](#)
**Comunicadores:**
[Regístrese para publicar notas y convocatorias](#)
**Información**

- Cursos de Verano de APIE
- Agenda APIE 2007
- Estudio sobre Periodistas, Empresas, Instituciones
- Notas de Prensa
- Convocatoria eventos
- Teletipos

**Documentación**

- Prensa on-line
- Fuentes Estadísticas
- Papeles de Trabajo
- Empresas
- Admón. pública

**Servicios APIE**

- Estatutos de APIE Leg.
- Alta en APIE
- Bolsa de trabajo
- Formación periodistas
- Publicaciones APIE
- Ofertas socios

**Carpetas de Prensa**

Si necesita información sobre empresas consulte nuestras carpetas de prensa

A-B-C-D-E-F-G-H-I-J  
K-L-M-N-O-P-Q-R-S  
T-U-V-W-X-Y-Z

**Buscar por texto**

[Click for Live Support!](#)

## La Ley de Protección de Datos y la Seguridad Informática

**Además de registrar los ficheros en la Agencia Española de Protección de Datos y garantizar a los ciudadanos los ejercicios de sus derechos, las organizaciones deben establecer importantes medidas de seguridad informática que en muchos casos no son cumplidas.**

La Ley Orgánica de Protección de Datos, más conocida como LOPD, exige que las organizaciones establezcan una serie de medidas jurídicas y organizativas que garanticen el correcto tratamiento de los datos que son diariamente recogidos de sus clientes, proveedores y colaboradores.

Debido a las importantes labores realizadas por la Agencia Española de Protección de Datos en los últimos años, podemos constatar que casi la totalidad de las grandes empresas españolas y multinacionales que poseen sedes en nuestro país demuestran un grado muy importante de cumplimiento de la LOPD. No obstante, existen estudios que comprueban que pasados 10 años de la implantación de la Ley de Protección de Datos, casi el 90% de las PYMES no la cumplen, o en el mejor de los casos, la cumplen parcialmente.

Existen algunos factores que conllevan a las grandes organizaciones a cumplir con la normativa de forma más amplia:

- Participan constantemente de licitaciones públicas que exigen el cumplimiento de una serie de normativas, inclusive la LOPD;
- Recogen diariamente una cantidad ingente de datos que les incrementa de forma importante el riesgo de pérdida de información, y que les acaba obligando a adoptar mecanismos de tratamiento más rígidos;
- Disponen de condiciones financieras que les permite mantener un personal dedicado exclusivamente al mantenimiento de las normas;
- Están muy expuestas al público y consecuentemente, más vulnerables a eventuales denuncias.

La Ley de Protección de Datos está compuesta actualmente de 49 artículos que deben ser cumplidos integralmente por cualquier organización que recoja y realice tratamientos de información que contenga datos de carácter personal.

Sin embargo, un ciudadano común no tiene condiciones de saber si la empresa que maneja sus datos cumple integralmente con la normativa. La única forma visible de saberlo es a través de una consulta pública a la página de la Agencia de Protección de Datos, donde se puede verificar si la empresa realmente tiene sus ficheros registrados.

Además, cuando una empresa dispone de cupones o formularios de recogida de datos, normalmente estos documentos traen en el pie de página un texto legal en que se informa de la existencia de un fichero y de los derechos que el ciudadano tiene de acceder, rectificar o cancelar sus datos. Y nada más...

No obstante, existe un detalle que el ciudadano común y muchas organizaciones desconocen: Que La LOPD es complementada por el Real Decreto 994/99 de 11 de junio, que establece las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Para empezar, toda organización deberá confeccionar y mantener actualizado un Documento de Seguridad de obligado cumplimiento cuya inexistencia conlleva a importantes sanciones. A la hora de plantearnos la elaboración del Documento de Seguridad, empiezan a surgir las dificultades derivadas de la dificultad del cumplimiento de determinadas medidas de nivel alto.

Muchas organizaciones se limitan a confeccionar un Documento de Seguridad en líneas generales, que es prácticamente una copia literal de los artículos del reglamento. De esta forma, estarán cumpliendo únicamente con una obligación formal, mientras que lo que realmente importa es que se establezcan en la práctica medida que de hecho aseguren la confidencialidad y la integridad de los datos recogidos de sus clientes y colaboradores.

Algunos de los procedimientos de seguridad informática más importantes exigidos por la normativa son:

- **Procedimientos de Acceso Lógicos:** La organización debe establecer una relación actualizada de los usuarios que tienen autorización de acceso al sistema de información de la empresa. Esta autorización de acceso se da a través de un mecanismo de autenticación de usuarios y contraseñas que deberán ser cambiadas con la periodicidad determinada por el Responsable de

### Seguridad de la Empresa.

- **Procedimiento de Control de Accesos Físicos:** Los servidores, carpetas y armarios en que es almacenada toda la información de carácter personal de la empresa, deben estar acondicionados en un espacio protegido y restringido al personal autorizado.
- **Procedimiento de Accesos a Datos a través de Redes de Comunicaciones:** Un número importante de empresas españolas dispone de redes de comunicación muy amplias, como son las intranets y la propia Internet. Es a través de estos medios por donde circula toda la información de la empresa, y por esta razón es importante que se establezcan los medios que proporcionen un nivel de seguridad adecuado.
- **Procedimiento del Régimen de Trabajo fuera de los locales de la ubicación del fichero:** Las nuevas tecnologías están permitiendo que cada día más trabajadores puedan desarrollar sus actividades a distancia, accediendo a la información de la empresa a través de sus portátiles, PDA's y blackberries que no siempre cuentan con una protección adecuada. Para poder mantener este flujo bajo control, es importante que todo el trabajo realizado fuera del local de trabajo cuente con una autorización del Responsable del Tratamiento, que además debe aportar los medios necesarios para que el trabajador disponga de equipos protegidos de amenazas externas.
- **Procedimiento de Gestión de Soportes:** Actualmente las empresas generan, reciben y transmiten una cantidad ingente de información, que en muchos de los casos se pierden o no se controlan como es debido. Para aportar un control efectivo de toda esta información, la organización debe establecer un sistema de registro de entrada y salida de soportes. La normativa entiende como soporte, cualquier medio que pueda almacenar una cantidad importante de datos (carpetas, ordenadores, cajas, etc). Estos soportes deben ser organizados a través de etiquetas que los identifiquen de manera sencilla, inventariados y almacenados en un local cuyo acceso será limitado al personal autorizado.
- **Procedimiento de Desecho y Reutilización de Soportes:** Cada vez son mas frecuentes las noticias sobre aparición de documentos tirados en la calle. En muchos de los casos, se trata de información de historiales médicos, cuyos datos son considerados de nivel alto. Normalmente, se suelen tirar al contenedor cintas, discos, disquetes y mucho papeleo, sin que se tomen las debidas precauciones. En muchos de los casos, toda esta información puede ser recuperada y utilizada de forma fraudulenta. El reglamento en su artículo 20, punto 3, determina que se deben tomar las medidas de seguridad pertinentes para impedir cualquier tipo de recuperación de la información que va a ser desechada o reutilizada. Las formas más eficaces de destrucción de la información es el uso de maquinas destructoras de papel y desmagnetizadores en el caso de que se traten de soportes magnéticos.
- **Procedimiento de Notificación, Gestión y Respuesta ante las Incidencias:** El Real Decreto 994/99 en que se aprueban el reglamento de medidas de seguridad para los ficheros de carácter personal, describe como incidencia, en el artículo 2, punto 9 como "cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos". Es decir, cualquier evento o circunstancia que ponga en riesgo la seguridad, la integridad o la confidencialidad de los datos de la empresa. El artículo 10 del reglamento exige que se adopte la utilización de un libro de incidencias en que hagan constar: a) el tipo de incidencia; b) El momento en que se produce; c) La persona que realiza la notificación; d) A quién se le comunica; e) Los efectos que se deriven de la incidencia. Además, la empresa deberá adoptar también procedimientos prevención de incidencias y de respuesta efectiva en el caso que se produzcan.
- **Procedimiento de Copias de Respaldo:** Independientemente de la normativa, este es un procedimiento que debería ser tomado muy en serio por todas las organizaciones que manejan información. La pérdida de datos puede ocasionar trastornos importantes a una empresa que podría perder su base histórica de datos, conllevando a pérdida de operaciones importantes. En el caso de las copias de respaldo, la ley trata de formalizar este procedimiento, que muchas veces es realizado sin que exista documentación alguna y que es gestionado de forma oral sin un monitoramento constante. Además, la copia debe de ser realizada de forma periódica (preferentemente a diario) y su recuperación debe ser capaz de reconstruir toda la base dañada antes de la incidencia.
- **Procedimiento de Registro de Accesos (NIVEL ALTO):** Se trata de uno de lo procedimientos más difíciles de cumplir, sobretodo por la dificultad de aplicar en todos los sistemas de tratamiento de datos y por el masivo almacenamiento de información que conlleva la puesta en marcha de esta medida. El procedimiento de registro de accesos (aplicable solamente a empresas que realizan tratamientos en ficheros de nivel alto) establece que cada acceso que se realice a un fichero, sea registrado en un "log" que identifique el usuario que ha accedido el fichero, la fecha y hora que ha realizado el acceso, que fichero ha accedido, que tipo de operación ha sido realizada (modificación, supresión, etc.) y si el acceso ha sido autorizado o denegado. Estos registros deben tener una revisión periódica y deben conservarse durante un periodo mínimo de dos años.
- **Procedimiento de Cifrado (NIVEL ALTO):** Este procedimiento que hace algunos años también resultaba difícil de cumplir, es actualmente una medida sencilla de ser llevada a cabo, sobretodo por la oferta de aplicaciones informáticas disponibles en el mercado, que realizan cifrados de datos de forma sencilla y eficaz. La norma establece que todos los soportes que contengan datos de carácter personal de nivel alto deberán estar cifrados cuando sean distribuidos, evitando que la información contenida no sea inteligible ni manipulada durante su transporte.

Además de estos procedimientos, el Documento de Seguridad deberá mantener una serie de anexos que deberán estar siempre actualizados. Entre los anexos más importantes están los inventarios de hardware y software de la empresa, la utilización de un libro de incidencias, el listado nominal del personal y de los terceros autorizados para acceder y tratar los datos de la

empresa y las políticas de seguridad en que se determinan las funciones y obligaciones de todo el personal.

Son muchas las implicaciones legales que pueden afectar a las empresas por el incumplimiento de todas estas medidas, una vez que tratan una cantidad ingente de datos personales, y por esta razón, adaptarse a la normativa es algo además de prudente, obligatorio. Cada vez más la Agencia Española de Protección de Datos recibe denuncias por violación a la normativa y es muy importante que las empresas estén en día con el integral cumplimiento de la ley.

La Agencia Española de Protección de Datos es el órgano responsable pela aplicación y verificación del cumplimiento de la ley que actúa de manera independiente a las Administraciones Publicas.

Implantar las normas de la LOPD no es un trabajo extremadamente complicado; sin embargo, es muy recomendable hacerlo asistido por alguna consultoria especializada. Existe una serie de interpretaciones sobre muchos artículos de la ley, son muchos los detalles implícitos y un consultor especializado además de asegurar una implantación adecuada, podrá ofrecer una serie recomendaciones que serán de gran valía para el empresario.

J. Eduardo Caamaño Justo, PMP  
Project Manager  
Mega Software y Comunicaciones  
www.megasyc.com

 **Archivos adjuntos:**

**No hay archivos adjuntos**

[Enviar por correo](#)

© APIE. Todos los derechos reservados. ¿Quiénes somos?

[Aviso legal](#)

powered by:  
 **acceso.com**