

# LOPD más que un puro tramite administrativo



## Análisis legal y técnico de la protección de datos

Todas las organizaciones que cuenten con datos de personas deben cumplir la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal (LOPD), por lo tanto podríamos decir que afecta a todas las empresas de nuestro país, en esta Ley se trata del derecho de las personas a que se requiera el previo consentimiento para la recogida y uso de sus datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar, cancelar u oponer se a la utilización de los mismos.

El cumplimiento de las obligaciones legales exige que se deban conjugar los derechos de los ciudadanos respecto a su uso, difusión y tratamiento, con la adecuada protección de los mismos en el seno de la empresa mediante medidas organizativas y técnicas apropiadas.

## Análisis de los datos

La primera actuación que debemos hacer es saber que datos de los que poseemos están afectados por la Ley, como están organizados estos datos y cuál es su soporte para poder estudiarlos y clasificarlos en el nivel correspondiente señalado por la Ley.

Una vez conocidos el primer requisito es darlos de alta ante la Agencia de Protección de Datos pasando inmediatamente a la aplicación de las medidas de seguridad establecidas para ese tipo de ficheros para garantizar su seguridad y confidencialidad, evitando su difusión, pérdida, alteración o tratamiento no autorizado.

## Medidas de seguridad

Dentro de las medidas de seguridad que se deberán establecer, figuran la redacción de un Documento de Seguridad donde figuraran las medidas a aplicar, quienes son los responsables, y las funciones y obligaciones del personal.

Según el nivel de los ficheros se pondrán en marcha en la empresa todas las medidas señaladas en el Reglamento de desarrollo de la Ley (RD 1720/2007) registro de incidencias, custodia de los soportes, control en el acceso, custodia y distribución de soportes, almacenamiento de la información etc.

## Cuál es la realidad con que nos encontramos

Cuando acudimos a una empresa, generalmente es porque la empresa cree que tiene un problema de seguridad con información importante o porque alguien les ha puesto el miedo en el cuerpo con el anuncio de terribles sanciones o inspecciones en el caso de incumplimiento legal.

Cuando hablamos con los responsables, casi todos nos dicen que ya tienen realizada la adaptación de su empresa a la LOPD, pero cuando se le pregunta qué importancia cree que tiene para su empresa esta adaptación la mayoría contestan que muy poca o nula y constatamos que efectivamente es así, pues han tomado esta adaptación no como un reto para proteger su información importante, para hacer que sus trabajadores tomen conciencia de las consecuencias de divulgar información o tratarla inadecuadamente, para disponer de unos mecanismos de acceso y control apropiados para lograr una información totalmente confidencial, íntegra y disponible, sino como un mero trámite administrativo, que lo único que les ha reportado es un gasto.

## En qué consiste nuestro trabajo

Tengan o no la inscripción de los ficheros realizada, dispongan o no de documentos, nuestro trabajo comienza por examinar los datos que poseen, determinar los ficheros donde se encuentran, examinar la inscripción realizada y modificarla en los casos en que sea incorrecta o haya habido variaciones respecto a la inscripción o en los casos en que no esté realizada realizarla apropiadamente.

Examinamos la circulación de datos y donde se encuentran

Examinamos la organización del personal, funciones, flujos de trabajo, responsabilidades

Examinamos los documentos que la empresa posee, Documento de seguridad, Contratos con el personal, Contratos con terceros, documentos de captura de datos, documentos de cesión de datos...

Examinamos la política, normas, procedimientos, reglas y estándares puestos en marcha en la empresa.

Controlamos accesos y permisos

Analizamos los equipos informáticos realizando una auditoría de los mismos.

Analizamos las redes de comunicaciones y hábitos de navegación

Analizamos el correo electrónico, intranet y página web

Averiguamos que conocimientos tiene el personal sobre los procesos de notificación

Analizamos la seguridad de los datos afectados respecto a una posible eventualidad importante.

Una vez que tenemos un mapa exacto de la situación de la empresa, se redacta un documento de auditoría completo, con un informe jurídico y otro técnico, en el que se describe la situación encontrada y en caso de no cumplimiento redactar las medidas para paliar dichas disconformidades.

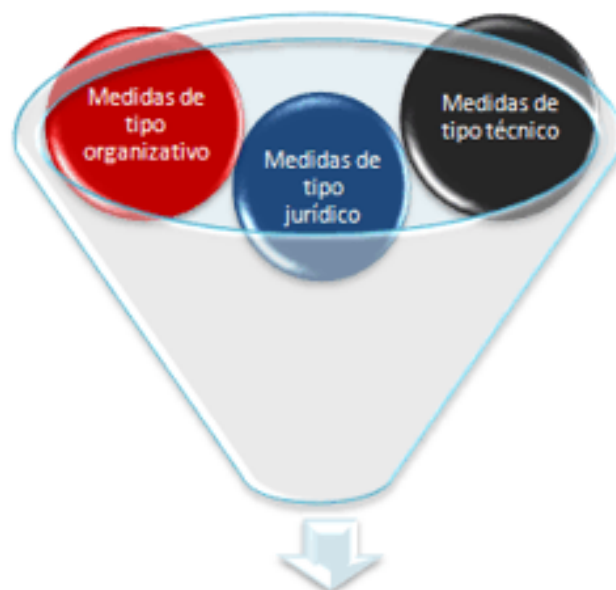
## Tras la auditoria la protección

Concluida la primera fase, pasamos a ayudar a la empresa a cubrir las no conformidades a redactar los documentos necesarios para securizar toda la información que la empresa decida proteger incluida la Legal, (como el documento de seguridad, los documentos de compromiso del personal, los documentos para terceros que tengan relación con los ficheros, los documentos de captura de datos etc.)

Se desarrolla la política de la empresa respecto a la seguridad.

Se describen los procedimientos de trabajo y normas de ejecución para el personal.

Se realiza la formación del personal y se asiste a la empresa en todo el proceso de implantación.



Sobre Locales, Equipos, Programas, Personas...