La auditoría de protección de datos, la gran desconocida (I).

Un 44% de las empresas españolas ve inevitable la pérdida de datos

¿Qué se entiende por cumplir con la Ley Orgánica de Protección de Datos (LOPD)? Todos oímos hablar de la protección de datos, del derecho al honor y del derecho a preservar nuestra intimidad. Derechos que han encaminado a que aquellos que disponen y tratan datos de carácter personal a tener que cumplir con una serie de obligaciones según los requerimientos de las distintas normativas.

La concienciación sobre la obligación de cumplir con la LOPD cada vez es más palpable por parte de las empresas. Sin embargo, el concepto de cumplimiento parece no estar del todo claro. La mayor parte de las organizaciones interpretan erróneamente que cumplir con la ley radica simplemente en registrar sus bases de datos o ficheros ante la Agencia Española de Protección de Datos.

Un gran índice de adaptaciones realizadas podríamos decir que tan solo se han limitado a esta tarea. Por lo que se podría decir que el índice de incumplimiento normativo es todavía más preocupante de lo que ya anunciaba la AEPD en su última memoria donde se podía extraer que **tan solo un escaso 33% de las empresas españolas cumplían supuestamente con la normativa** teniendo en cuenta que contaban con ficheros inscritos.

El registro de ficheros no deja de ser la punta del iceberg, ya que, como sabemos, **una correcta adaptación se da cuando una organización cumple con los principios básicos de la normativa e implementa las medidas de seguridad pertinentes** en función de los datos tratados.

Obviamente no podremos pensar que datos como los relativos a nuestra salud deberán contar con las mismas medidas de seguridad que datos como nuestra dirección postal, correo electrónico o incluso DNI. Estamos hablando de datos especialmente protegidos que deberán contar con unas medidas de seguridad de nivel alto.

En este sentido, como veremos, **todas las empresas que trabajan con ficheros con un nivel de seguridad medio o alto están obligadas a realizar cada dos años una auditoría**. Auditoría que deberá llevarse a cabo para verificar que los sistemas de información e instalaciones de tratamiento y almacenamiento de datos funcionan de manera correcta.

Se trata de una exigencia de la normativa, por lo que no cumplir con ella podrá suponer una sanción económica.

Llegados a este punto, ¿podemos decir que las empresas en nuestro país están cumpliendo con la ley? **Debemos tener en cuenta que en muchas ocasiones las organizaciones se verán obligadas a acreditar la auditoría de sus sistemas de seguridad por motivos de calidad**.

Actualmente es bastante difícil pensar en una actividad empresarial en la que no se lleguen a tratar datos de carácter personal y que para ello no se utilicen tecnologías de la información. Para desempeñar su labor, las organizaciones echan mano de tecnologías como ordenadores, smartphones, tabletas, etc. dispositivos que han agilizado el flujo desmesurado de datos a través de la red.

Sin embargo, estos mismos datos son en muchas ocasiones la columna vertebral de una empresa por lo que incorporar medidas que aseguren su integridad es una tarea primordial.

Esta seguridad de la información supone un requisito básico que, en último término, puede llegar a asegurar la continuidad de un negocio. La realidad es que un 90% de las empresas que se ve afectada por una pérdida importante de datos acaba desapareciendo en un plazo de dos años, tal y como acaba de concluir un estudio de la Cámara de Comercio de Londres. Por otro lado, Iron Mountain en un reciente informe sobre cómo abordan esta situación las empresas españolas ha constatado que **el 44% de las empresas de nuestro país considera que la pérdida de datos es algo inevitable**. Y es que una pérdida en muchas ocasiones viene ocasionada principalmente por una catástrofe, un error humano, cortes de luz, errores propios de sistemas informáticos o ataques externos.

Así, casos como el acontecido en 2005 en Madrid con el incendio de la torre Windsor, empresas como Deloitte o Garrigues tuvieron que poner a prueba sus planes de continuidad ante un desastre de tal calibre. Es por ello que contar con un sistema de seguridad de la información aparte de ser una obligación por parte de distintas normativas se nos antoja como una necesidad fundamental.

La propia normativa de protección de datos ya establece la necesidad de asegurar la disponibilidad y seguridad de la información a través de la incorporación de una serie de medidas que deberán ser auditadas en función de los datos tratados.

De esta forma, **una empresa se verá obligada al menos cada dos años a realizar una auditoría cuando exista un tratamiento de datos de nivel medio o alto**. Así lo establecen los artículos 96 y 110 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprobaba el Reglamento de desarrollo de la LOPD.

Su intención no es otra que garantizar la seguridad de los datos evitando que puedan ser alterados, perdidos o tratados de forma incorrecta. **El incumplimiento por parte de una empresa de esta obligación supondría ante la AEPD una infracción grave de la LOPD punible con una sanción que oscilaría entre los 60.000 y los 300.000 euros**.