



Un nuevo mercado de auditoría obligatoria



José de la Peña Sánchez

No parece mala cosa el que continuemos dándole vueltas al Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, puesto que desde el pasado 25 de junio, se supone que en todas las organizaciones concernidas ya están implantadas las medidas del nivel medio, incluida la contenida en el Artículo 16 («Responsable de seguridad»).

Pero no es esa medida en la que nos vamos a centrar en esta entrega, sino en la prevista en el artículo siguiente, el 17, titulado «Auditoría». Desde la referida fecha ya ha empezado a correr el plazo de dos años (en tanto que período máximo que terminará el 24 de junio de 2002) para someter a una auditoría (interna, externa...) a los sistemas de información e instalaciones de tratamiento de datos personales. Interesante.

CAMBIOS RELEVANTES

La primera consideración sobre el plazo máximo bienal, aparece al analizar el Artículo 8.3 (nivel básico), en el que se dice que «El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo».

Según la RAE/XXI/1992, relevante se define como: «2- Importante, significativo». Habida cuenta de que en líneas generales el «Relevantómetro» suele estar roto o fuera de servicio en la mayoría de entidades, no resulta baladí determinar con la mayor precisión posible el momento más adecuado para realizar la auditoría.

Si no atinamos, podría quedar obsoleto el Informe pre-cambio relevante, con lo que no cumpliría o podría no cumplir ni con el fondo ni con la forma del Reglamento en sus artículos 17.2 y 17.3, sobre todo considerando que las posibles y recomendadas medidas co-

rrectoras adecuadas que quedarán a disposición de la Agencia de Protección de Datos no representarían la actualidad.

Otro aspecto digno de tenerse en cuenta es el alusivo a los «Planes Sectoriales de oficio que realiza la Agencia de Protección de Datos para comprobar el grado de adecuación de los ficheros de las Administraciones Públicas y ficheros privados a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal», según la Memoria 1999 del organismo. Quizá se esté iniciando la aplicación de una suerte o variedad de *benchmarking*.

Habida cuenta de que en líneas generales el «Relevantómetro» suele estar roto o fuera de servicio en la mayoría de entidades, no resulta baladí determinar con la mayor precisión posible el momento más adecuado para realizar la auditoría del Reglamento

En opinión de quien esto escribe, el tipo de auditoría que nos ocupa es multidisciplinar, además de obligatoria, interna o externa, pública (Administraciones Públicas) o privada, de alcance total y con el objeto definido por la seguridad de ficheros automatizados con datos personales.

Consecuentemente, el auditor podrá ser una persona o un equipo, esto es, el auditor responsable del grupo de auditores, expertos técnicos y su apoyo correspondiente. No entramos en la forma jurídica del grupo, ni en las relaciones que unan a sus componentes, puesto que el abanico de posibilidades dentro de la legalidad vigente es amplio.

Sí, sin embargo, es interesante considerar, en el marco de la libertad de elección previsto en el Artículo 17.1 del Reglamento, el grado de independencia del auditor a seleccionar: ¿externo?, ¿interno externalizado?... Recordemos que la Unión Europea todavía no se ha

pronunciado al respecto de lo que tiene que pronunciarse. De alguna manera, «Cabe entender que el cliente (el auditado), en cierto modo, adquiere o alquila la reputación del auditor». Arruinada *dixit*.

ALGUNAS IDEAS

La existencia de un Comité de Auditoría, además, puede convertir «La auditoría en un mecanismo de supervisión». Desde que el Reglamento apareció en el BOE/25-6-1999, han sucedido muchas cosas, algunas tan significativas como el casi olvidado y temido Efecto 2000, resuelto con éxito pero con

una especie de morbo y desilusión. Y hoy nos encontramos saboreando la temprana miel del panal feliz de la «Nueva Economía» y la *Web*, entorno de jugosas promesas en el que ya se han divulgado algunos casos sonados que han merecido la atención de la Agencia. Más se verán, seguro.

Parece como si el cultivo de la desmemoria fuera el modelo de praxis vital imperante, olvidándose en mi opinión el fundamento pragmático de los sistemas expertos, y como se dice: quien no conoce la historia, vuelve otra vez a vivirla, lo mismo pero años después.

Creo conocer lo que ha sucedido con la generación «baby boom» (los que ahora tienen entre 35 y 45 años). Aquella explosión demográfica española de la época del 600 (Seat, por supuesto) en la que primero no había colegios, después no había plazas universitarias, luego no había viviendas... Y así, todo ello ornamentado con periodos de vacas gordas y vacas flacas.

Ahí queda lo dicho y algo más: que hubo una época con exceso de oferta de empleo, resuelta de forma, diremos, pudorosamente inadecuada. Aquella fue la época en la que se gestó el Efecto 2000. Actualmente vivimos en otro tiempo en el que la escasez de profesionales en TIC ha provocado que «en la política actual de fichajes» imperen «los salarios desorbitados y los trasvases de equipos enteros de una empresa a otra», o sea, taifas informáticas «golondrina». Se dan casos curiosos, en los que quienes buscan empleo -a veces el primero- seleccionan a la compañía que quieren que les contrate. Desde luego, quien disponga de buenos profesionales en cualquier disciplina, especialmente en seguridad de la información, tiene oro.

Y de este modo, entre peticiones de pactos entre sindicatos, empresarios y políticos para la Ley Básica de Empleo y el previsto cambio de la Ley de Extranjería, avanzamos todos por la autopista de la «Nueva economía», mientras continúan las prejubilaciones y el electrocardiograma bursátil dibuja perfiles infernales.

Si metemos todo lo dicho en la máquina de las predicciones arriesgadas y pedimos un vaticinio aplicado al mundo de las TIC, bien pudiera salir algo así como: «¡Cuidado, si no se controla el cambio pueden desaparecer las funcionales catedrales informáticas y ser sustituidas por modestas chozas de aficionados!» Y no hay cosa más peligrosa que los aficionados en el mundo de la aplicación de las TIC a los negocios, en el de la seguridad informática (que ya es vieja; no ha nacido hoy), y en el de control y auditoría. (Aclaro: una cosa es ser un informático que debe adquirir experiencia, y otra muy distinta un aficionado a la informática).

Como final de esta florido encadenamiento de reflexiones, pasadas por el tamiz de la experiencia profesional de un modesto servidor, quizá convenga volver al asunto inicial: la auditoría del Reglamento, que viene en tiempos de cambio. Hay que hacerla, y hay que procurar hacerla bien. Por muchas razones. ■

JOSÉ DE LA PEÑA SÁNCHEZ

Auditor Censor Jurado de Cuentas y Licenciado en Informática
Correo-e: coda2@jet.es