



Consideraciones sobre la auditoría prevista en el reglamento



José de la Peña Sánchez

En cuestiones informáticas, y más si afectan a la seguridad informática, hay que tener en cuenta esa verdad tópica de que «lo urgente, desplaza lo importante», ya que el paso del tiempo hace urgente lo importante. La auditoría prevista en el Reglamento (RD 994/1999, de 11 de junio, Art. 17) para los niveles medio y alto de medidas de seguridad, necesita un amplio y pormenorizado estudio, por lo que resulta procedente una primera aproximación. En tanto en cuanto el Director de la Agencia de Protección de Datos no considere oportuno emitir instrucciones al respecto, parece adecuado iniciar la búsqueda de la normativa aplicable, que deberá girar alrededor de los sistemas de información y su seguridad.

El análisis de las normativas ISACA/OAI, IFAC/ICAC e ISO/AENOR, entre las más destacadas, debería orientarse a intentar que afloren sus aspectos básicos y no los específicos, con el objetivo de fijar unos 'Principios Generalmente Aceptados', tanto en la auditoría interna como en la externa.

Habría que tener en especial consideración los siguientes puntos:

El contrato de auditoría, carta propuesta o carta de encargo.

- El conocimiento de la actividad de la entidad a auditar.

- Las declaraciones de la Dirección de la entidad a auditar.

- Los fraudes y los errores

- La utilización del trabajo de terceros:

. Otro auditor externo.

. El auditor interno.

. El experto independiente.

Además -y esto hay que valorarlo adecuadamente-, el caso que nos ocupa es lo que se conoce como «Primera Auditoría», que podría estar afectada por el grado de conocimiento de la actividad de la entidad a auditar, por lo que ha de considerarse como una actividad iniciática creadora de *know how*.

También conviene determinar que la auditoría solo se realiza para cumplir con el RD 994/1999, y no para otro fin, así como quienes son los destinatarios del Informe. Esto tiene un especial interés, ya que podría evitar problemas post-auditoría.

Es preciso señalar la no existencia de limitaciones que impidan la realiza-

ción de pruebas necesarias en opinión del auditor para la obtención de EVIDENCIA suficiente, adecuada, fiable y relevante. Igualmente, se precisa evaluar el CONTROL INTERNO y el RIESGO DE AUDITORÍA.

Todas estas consideraciones, inherentes desde hace muchos años al campo profesional de referencia (la auditoría), nos llevaría a la denominada AUDITORÍA DEFENSIVA, que busca la hiperseguridad en la evidencia obtenida vía información dura: observable y verificable, desechando la información blanda: observable y no verificable, asunto que merece un estudio monográfico.

FICHEROS PREEXISTENTES

Antes de finalizar esta pincelada inicial sobre la auditoría aplicada al Reglamento, quizá convenga mencionar que la nueva Ley de datos ya está vigente desde el 14 del pasado enero. Esta nueva legislación incluye una 'Disposición adicional primera' («Ficheros preexistentes»), con rango de orgánica, que fija un plazo máximo de adaptación de ficheros y tratamientos inscritos o no en el Registro General de Protección de Datos de ¡tres años! (14 de enero de 2003). No puede calificarse dicho plazo de urgente. Pero, en fin, si acudimos a 1978, fecha del mandato constitucional del que han emanado las leyes de protección de datos españolas (la viva y la muerta), pues todo hace pensar que dos décadas y pico no son nada. Se verá.

En posteriores entregas se continuará profundizando en aspectos de la auditoría (RD 994/1999), haciendo hincapié en las sinergias y el valor añadido que pudieran reportar a las entidades y a sus sistemas de información, que deben estar siempre en permanente disposición de mejora.

Mientras tanto, el mundo sigue su marcha, incluso el próximo Informe Olivencia, el 2, con sus recomendaciones y sus comisiones delegadas de auditoría (incluso las auditorías internas y externas), que quizá cristalice en la instauración de normas de obligado cumplimiento. ■

JOSÉ DE LA PEÑA SÁNCHEZ

Auditor Censor Jurado de Cuentas y Licenciado en Informática