Rubén PÉREZ BAILE
Abogado

• **ENUNCIADO:**

SIMANCAS, S.A. de acuerdo con la obligatoriedad legal de implantar un documento de seguridad a tenor de lo dispuesto en la Ley 15/1999 de Protección de Datos de Carácter Personal y, teniendo en cuenta lo dispuesto en el Real Decreto 994/1999 por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de personal, encargó a un Abogado la redacción e implantación del documento de seguridad, así como la inscripción de los ficheros ante la Agencia de Protección de Datos.

Transcurridos dos años desde su implantación le surgen algunas dudas jurídicas sobre la Protección de Datos. Por ello, acude al Despacho del Abogado para que le asesore sobre las siguientes cuestiones.

• **CUESTIONES PLANTEADAS:**

1. ¿Debe realizar una Auditoría de los Sistemas de Información?

2. La empresa pretende crear un fichero temporal. ¿Qué nivel de seguridad debe aplicar a dicho fichero?

3. La empresa pertenece a un grupo de empresas. ¿Puedo ceder los datos a las otras empresas del grupo?

4. Nuestra matriz en Alemania nos ha solicitado la cesión de una serie de datos para la evaluación de personal. ¿Debe la Agencia de Protección de Datos autorizarnos a trasladar el tratamiento a Alemania?

• **SOLUCIÓN:**

1. El Reglamento establece que el «documento de seguridad» debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

Dado el estado actual de la técnica y que, en el nivel medio de seguridad, se exige que la auditoría informática se realice al menos cada dos años, la revisión del documento no debería tener una periodicidad mayor de dos años.

Consiguientemente, el documento de seguridad deberá establecer un sistema periódico de auditoría interna. Y, podrá disponer que se realice una auditoría anual externa para mayor garantía de los datos que se tratan.

El objetivo de ambas auditorías no es más que certificar que se cumplen los requisitos exigidos en las medidas de seguridad requeridas en los niveles correspondientes que recoge el Real Decreto 994/1999.

El artículo 17 del Reglamento determina, pues que:

«Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.»

En definitiva, creemos que lo coherente es realizar una auditoría interna, al menos, una vez al año; y siempre que se produzcan hechos relevantes, en ese mismo momento, independientemente del tiempo transcurrido.

En nivel medio y alto se deberá realizar la auditoría interna o externa, como mínimo una vez cada dos años, a tenor de lo dispuesto en el Reglamento.

2. La respuesta se recoge en el artículo 7.º del Real Decreto 994/1999, en el sentido de que los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento. Asimismo, todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

3. El criterio de la Agencia de Protección de Datos a este respecto es uniforme, entendiendo que la vinculación que puede existir entre las sociedades que integran un grupo empresarial no afecta al régimen de cesión de datos.

Otra cuestión son las implicaciones fiscales y mercantiles que determinan la creación de los grupos de empresas; pero desde el punto de vista de la protección de datos las empresas integradas en el mismo tienen su plena independencia jurídica, su propia personalidad jurídica, de tal forma que lo único que comparten son las acciones o participaciones de las sociedades en cuestión.

La respuesta es que no pueden cederse los datos al grupo de empresas.

4. El concepto de transferencia internacional de datos aparece por primera vez en la norma primera de la Instrucción 1/2000 relativa a las normas por las que se rigen los movimientos internacionales de datos:

«Se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.»

El artículo 33 de la Ley de Protección de Datos exige como regla general que para realizar una transferencia internacional de datos «se obtenga autorización previa del Director de la Agencia de Protección de Datos», con las excepciones que señala el artículo 34 de la Ley de Protección de Datos y que detallamos:

- Que se efectúe con destino a países que proporcionan un nivel de protección equiparable al existente en España.
- Que resulten de la aplicación de tratados o convenios en los que sea parte España.
- (...).
- Que el afectado haya dado su consentimiento.
- (...).

Por tanto, en aplicación de la Ley nuestra transferencia internacional de datos a nuestra matriz en Alemania no debe ser autorizada por el Director de la Agencia de Protección de Datos, por entrar dentro de las excepciones del artículo 34 de la Ley (postura que avala igualmente la Directiva comunitaria al respecto).

Ahora bien, hay que tener en cuenta otras circunstancias para realizar la transferencia internacional de datos, si bien no es precisa la autorización del director de la Agencia de Protección de Datos, si debemos cumplir los requisitos que nos exige el artículo 12 de la Ley de Protección de Datos:

«... La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9.º de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.»

Las medidas de seguridad aplicables serán las establecidas en la normativa española, concretamente para los tratamientos automatizados que contengan datos de carácter personal, recogidos en el Real Decreto 994/1999, 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad.

• SENTENCIAS, AUTOS Y DISPOSICIONES CONSULTADAS:

- **Ley Orgánica 15/1999 (Protección de Datos de Carácter Personal), arts. 9.º, 12, 33 y 34.**
- **RD 994/1999 (Medidas de Seguridad), art. 17.**
- **Instrucción 1/2000 (Protección de Datos de Carácter Personal).**