SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Alvaro Gómez Vieites
Socio-Director de SIMCe Consultores
Prof. de la Escuela de Negocios Caixanova

Recibido: 30/5/05
Aceptado: 27/7/05

Nadie cuestiona hoy en día la importancia adquirida por la Seguridad informática y la Protección de datos de carácter personal en el ámbito de las organizaciones. La progresiva informatización de los procesos administrativos y de negocio, el tratamiento automatizado de datos de carácter personal, el acceso a Internet y el desarrollo de nuevos servicios online son algunos de los factores que explican la creciente preocupación por garantizar la Seguridad en los Sistemas de Información y en la conexión corporativa a Internet.

La información constituye un recurso que, en muchos casos, no se valora adecuadamente por su intangibilidad (cosa que no ocurre con los equipos informáticos, la documentación o las aplicaciones) y, además, las medidas de seguridad no influyen en la productividad del sistema, sino, más bien, al contrario, por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

Con la proliferación de las redes de ordenadores, la información de las empresas ha pasado de concentrarse en los grandes sistemas (sistemas centralizados) a distribuirse por los ordenadores y servidores ubicados en los distintos departamentos y grupos de trabajo. Por este motivo, en la actualidad, muchas organizaciones no conocen la información que hay en los puestos de trabajo (generalmente, ordenadores personales de la propia organización), ni los riesgos que tienen de ataques y desastres, ni cómo la propia organización utiliza esa información.

Otro aspecto importante, que muchas veces se olvida, es que, más del 75 % de los problemas inherentes a la seguridad se producen por fallos de los equipos o por un mal uso por parte del personal.

Además, el entorno legal que ha entrado en vigor en estos últimos años en nuestro país en materia de *Protección de Datos de Carácter Personal* (LOPD) y *Prestación de Servicios de la Sociedad de la Información* (LSSI) plantea nuevos retos técnicos y organizativos para los responsables de la Seguridad Informática.

Así, la Ley Orgánica 15/1999, de 13 de diciembre, sobre *Protección de Datos de Carácter Personal* (LOPD) obliga a la implantación de importantes medidas de seguridad informática a las empresas que hayan creado ficheros con datos personales.

Sin embargo, la mayoría de las empresas todavía incumplen muchas de estas obligaciones, por lo que se exponen a importantes multas (las más elevadas de la **Unión Europea**), que podrían alcanzar los 600.000 euros para las infracciones consideradas como muy graves.

De hecho, en un estudio sobre Seguridad Informática realizado en 2003 en Galicia en el marco del *Proyecto Observatorio TIC* (www.observatoriotic.org), patrocinado por la **Consellería de Innovación, Industria y Comercio**, se pudo constatar que sólo el 50 % de las empresas de Galicia reconocían poseer ficheros con datos de carácter personal, cuando en realidad prácticamente el 100 % de las organizaciones maneja hoy en día en sus aplicaciones de gestión algún dato de carácter personal: personas de contacto en el fichero de clientes, proveedores o contactos comerciales; datos personales de los empleados para la confección de las nóminas, el control de presencia o la gestión de recursos humanos; retenciones a profesionales externos (abogados, notarios, consultores...); *curriculum vitae* de candidatos a empleo; etc.

Asimismo, de este estudio se extraía el preocupante dato de que sólo el 7 % de las empresas había procedido a registrar sus ficheros con datos de carácter personal en el Registro General de Protección de Datos, y en un porcentaje similar (7 %) se afirmaba haber elaborado el Documento de Seguridad exigido por el *Reglamento de Medidas de Seguridad de los Ficheros Automatizados.* El hecho de no haber realizado la inscripción de los ficheros de datos de carácter personal es contemplado como una infracción leve por la LOPD, salvo en el caso de los datos de nivel medio o de nivel alto, en cuyo caso se considerará como infracción grave, pudiendo ser objeto la empresa u organización de una sanción por parte de la APD de entre 60.101 € y 300.506 €.

En este último año podemos considerar que la situación ha mejorado bastante debido a una mayor concienciación por parte de las empresas y las Administraciones Públicas, si bien la situación todavía es preocupante debido al alto grado de incumplimiento de la formativa vigente en España, y que es común a toda la **Unión Europea** (cabe recordar que la LOPD es el fruto de la transposición a nuestro ordenamiento jurídico de la Directiva 95/46/CE del **Parlamento Europeo**, y que por ello todos los países de nuestro entorno cuentan con una legislación similar para proteger la intimidad personal y familiar de sus ciudadanos).

Por lo tanto, veamos a continuación, de forma resumida, cuáles son los principales pasos que debería dar una empresa para cumplir con los requisitos de la LOPD:

- En primer lugar, se debe notificar a la **Agencia de Protección de Datos**, Organismo responsable de ve-

lar por el cumplimiento de la LOPD, la existencia en la empresa de bases de datos o ficheros que incluyan datos de carácter personal, especificando la finalidad a que obedece el fichero y el nivel de medidas de seguridad que se van a adoptar. Se trata de un trámite sencillo, pero imprescindible, ya que el plazo para realizar la inscripción de los ficheros ya existentes en una empresa expiró el 15 de enero de 2003, por lo que desde esa fecha se pueden imponer sanciones importantes a aquellas empresas que utilicen ficheros con datos de carácter personal y no los hayan declarado ante la **Agencia de Protección de Datos**.

- Por otra parte, las empresas también deben informar a los interesados de la recogida de datos personales, mediante las correspondientes cláusulas informativas que se deberían incluir en todos los impresos en papel o formularios electrónicos utilizados para recabar sus datos. El incumplimiento de esta obligación se considera una infracción leve de la LOPD, por lo que puede ser sancionada con una multa que oscila entre los 601 y los 60.101 euros.

- Asimismo, la empresa debe tener en cuenta que los interesados pueden ejercer su derecho de acceso para obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Por otra parte, los interesados también podrían solicitar la rectificación o eliminación de datos personales sometidos a tratamiento por la empresa, o ejercer su derecho de oposición al tratamiento de dichos datos. La empresa debería responder en los plazos previstos a las peticiones que pudiera recibir de los ciudadanos interesados.

- Otra cuestión de especial relevancia en materia de protección de datos es la cesión de datos personales a terceros. La LOPD prohíbe expresamente la comunicación o cesión de datos a terceros sin el consentimiento expreso de los afectados. Por este motivo, en caso de compartir ficheros que pudieran tener datos personales con otras personas jurídicas (aunque se encuentren integradas en el mismo grupo empresarial) será necesario obtener el consentimiento de los afectados, para evitar las sanciones más elevadas previstas por la LOPD, ya que este tipo de operaciones no consentidas se consideran infracciones muy graves con multas que pueden oscilar entre los 300.506 y los 601.012 euros.

- Igualmente, la empresa debe tener en cuenta que si el fichero pierde la finalidad originaria, la LOPD no permite su reutilización para otras actividades por lo que sus datos deberán ser destruidos, notificándose la destrucción del fichero a la propia **Agencia de Protección de Datos**.

- De acuerdo con lo estipulado en el artículo 9 de la citada LOPD, las empresas e instituciones con ficheros de titularidad privada deben implantar todas las medidas de índole técnica y organizativa que permitan garantizar la seguridad de los datos de carácter personal, y eviten su alteración, pérdida, tratamiento o acceso no autorizado. El *Reglamento de Medidas de Seguridad de los Ficheros Automatizados* (Real Decreto 994/1999, de 11 de junio), que entró en vigor el 26/06/99, determina cuáles han de ser las medidas de índole técnica y organizativa que garanticen la integridad y seguridad de ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas, así como de las personas que intervengan en el tratamiento automatizado de los datos.

En el citado Reglamento se establecen tres *"Niveles de seguridad"* para los datos de carácter personal:

- **Nivel básico;** de aplicación a todos los ficheros de datos de carácter personal.

- **Nivel medio;** de aplicación a los ficheros que contengan datos relativos a la comisión de infracciones, Hacienda Pública, servicios financieros. Asimismo, se consideran dentro de este nivel aquellos ficheros que contengan un conjunto de datos de carácter personal que permitan obtener una evaluación de la personalidad del individuo. Así, por ejemplo, también estarían incluidos en el Nivel Medio los ficheros de *curriculum vitae* de candidatos a empleo enriquecidos con los resultados de pruebas psicotécnicas, o los datos obtenidos sobre los patrones de consumo y el comportamiento de los clientes a través de herramientas de *"inteligencia de negocio"*.

- **Nivel alto;** de aplicación a los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales. Hay que tener en cuenta que la Agencia de Protección de Datos considera que si se registra en un fichero información sobre posibles minusvalías de las personas (grado de minusvalía de los empleados a efectos del cálculo de la retención del IRPF, minusvalías de clientes a efectos de proporcionar un mejor servicio, etc.), este dato debe ser tenido en cuenta como relativo a la salud del interesado, por lo que el fichero en cuestión debe cumplir todas las medidas correspondientes al **Nivel alto**.

Las medidas de seguridad mínimas que se han de adoptar en el Nivel básico, y que también son de aplicación en los niveles medio y alto, han de contemplar los siguientes aspectos:

• Elaboración de un Documento de Seguridad que incluya la siguiente información:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

- Medidas, normas y procedimientos para garantizar el nivel de seguridad.

- Funciones y obligaciones del personal.

- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

- Procedimiento de notificación y gestión de incidencias

- Procedimientos de realización de copias de seguridad.

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.

• Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal esta-

rán claramente definidas y documentadas.

• Gestión de incidencias: el procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

• Se ha de establecer un sistema de identificación y autenticación de los usuarios con acceso a los datos de carácter personal:

- Relación de usuarios con acceso autorizado.

- Política de contraseñas (con el correspondiente procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad).

• Se ha de establecer un sistema de control de acceso a los datos de carácter personal, con los mecanismos necesarios para impedir que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

• Se deberá llevar a cabo una gestión correcta de los soportes informáticos que contengan datos de carácter personal:

• Identificación e inventariado de los soportes, que deberán almacenarse en un lugar con acceso restringido al personal autorizado.

• La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en los que esté ubicado el fichero únicamente podrá ser autorizada por el responsable del fichero.

- Los procedimientos establecidos para la realización de copias de seguridad de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En lo que se refiere a las medidas de seguridad adicionales que se han de adoptar en el Nivel medio, debemos tener en cuenta los siguientes aspectos:

• El Documento de Seguridad deberá contener, además de lo dispuesto en las medidas del Nivel básico, la siguiente información:

- Identificación del responsable o responsables de la seguridad.

- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

- Las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

• Responsable de seguridad: el responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad.

• Auditoría de la seguridad: los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento de las medidas, procedimientos e instrucciones vigentes en materia de seguridad de datos. Esta auditoría tendrá lugar al menos una vez cada dos años.

• Identificación y autenticación: será necesario establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información de la empresa.

• Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

• Gestión de soportes: será necesario establecer un sistema de registro de entradas y salidas de soportes informáticos que permita conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega o recepción que deberá estar debidamente autorizada. Asimismo, cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en el mismo. Por último, cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada.

• En el registro de incidencias se anotarán todos los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso y cuáles han sido los datos restaurados.

• Copias de seguridad: será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

• Pruebas con datos reales: las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

Por último, las medidas de seguridad adicionales que se han de adoptar en el **Nivel alto** deben tener en cuenta los siguientes aspectos:

• Los datos de los soportes que vayan a ser distribuidos deberán estar convenientemente encriptados.

• La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará encriptando dichos datos, para garantizar que la información no sea inteligible ni manipulada por terceros.

• En lo que se refiere al control de los accesos al sistema de información, se deberá registrar cada intento de acceso, especificando la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Asimismo, en caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. Este registro de control de los accesos deberá conservarse durante un período mínimo de dos años.

• Copias de seguridad: estas copias deberán conservarse en un lugar diferente de aquél en que se encuentren los equipos informáticos que contienen los datos de carácter personal.

El incumplimiento de estas medidas de seguridad se considera una infracción grave de la LOPD, por lo que la empresa puede ser objeto de una sanción de entre 60.101 y 300.506 euros ■