Implantación de la Ley Orgánica de Protección de Datos

Implementation of the Data Protection Law

J. L. Rivas, J. E. Arés y V. A. Salgado

Resumen

Vamos a describir cómo aplicar la legislación vigente referente a la protección de datos de carácter personal en aquellos centros públicos que imparten cursos propios tales como: masters de postgrado, de extensión universitaria, etc. Para ello utilizaremos como ejemplo la impartición de un máster en Prevención de Riesgos Laborales, viendo el sistema informático empleado para su gestión.

Palabras clave: LOPD, Real Decreto 994/1999, D.E. 95/46, Bases de Datos

Summary

It will be explained the application of the legislation in force regarding personal data protection in public centres where courses such as postgraduate and universitary extension masters are given. In order to do this we will use as example a Master in Labour Risk Prevention considering the whole computer system used for its management.

Keywords: LOPD, Royal Decree 994/1999, D.E. 95/46, Database

La LOPD fundamentalmente tiene el objetivo de proteger a las personas físicas respecto al tratamiento que se puede realizar de sus datos por parte de distintos sujetos, ya sean públicos o privados

1.- Introducción

La LOPD es la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal. Esta Ley fundamentalmente tiene el objetivo de proteger a las personas físicas respecto al tratamiento que se puede realizar de sus datos por parte de distintos sujetos, ya sean públicos o privados. Dicha Ley surge por la gran capacidad de tratamiento y transmisión de la información que ofrecen actualmente las nuevas tecnologías; por tanto existe la necesidad de proteger los derechos del individuo.

Además de la LOPD se tendrá que aplicar el Real Decreto 994/1999, de 11 de junio, que será el Reglamento de las Medidas de Seguridad que deben cumplir los ficheros con datos de carácter personal. Dicho Real Decreto, aunque se aprobó en el desarrollo de la LORTAD (ley predecesora de la LOPD), no ha sido derogado.

Dentro del Reglamento de Medidas de Seguridad, existen tres niveles de seguridad distintos:

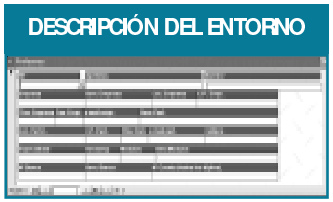
- El *nivel básico* será aplicable a todos los sistemas con datos personales en general. Según el artículo 3, apartado a) de la LOPD se define como: "cualquier información concerniente a personas físicas identificadas o identificables".
- El *nivel medio* será aplicable a: datos de comisión de infracciones administrativas o penales, datos de hacienda pública, datos de servicios financieros, datos sobre solvencia patrimonial y crédito o cualquier conjunto de datos de carácter personal suficiente que permita obtener una evaluación de la personalidad del individuo.
- El *nivel alto* se aplicará a aquellos datos referidos a: ideología, religión, creencias, origen racial, salud o vida sexual y por último los datos recabados para fines policiales.

Estas medidas se aplican de forma acumulativa: así el nivel alto de seguridad deberá cumplir también las reguladas para el nivel medio y el nivel bajo, como muestra la siguiente figura.

Se han inscrito tres ficheros de nivel básico en la Agencia de Protección de Datos cuyo responsable es la propia universidad en la persona de su representante legal y como responsable de seguridad el administrador del sistema

2.- Descripción del entorno

Un área de una universidad imparte un máster de prevención de riesgos laborales (PRL). El máster está dirigido por un profesor titular del área, así como la subdirectora que es profesora asociada perteneciendo a otro departamento. Además, dicho máster tiene contratados los servicios de una secretaria. Para la gestión del curso se ha elaborado: una base de datos para la gestión tanto de los alumnos como de los profesores, ficheros de contabilidad, así como documentos de Word (cartas para los alumnos, memorias, etc.). Todo el sistema informático usado trabaja en un entorno Windows XP Professional y será utilizado por las tres personas antes mencionadas. A continuación se muestran algunos de los tipos de ficheros y pantallas que se emplean.



3.- Medidas a adoptar

Según lo descrito anteriormente, se han inscrito tres ficheros de nivel básico en la Agencia de Protección de Datos (APD): el fichero de contabilidad, ficheros con datos de alumnos/profesores y fichero de acceso al sistema. En los tres el responsable del fichero es la propia universidad en la persona de su representante legal y como responsable de seguridad el administrador del sistema, que en este caso es el subdirector por sus conocimientos técnicos.

Además de inscribirles en la APD habrá que hacerlo por medio de disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente.

Creación, modificación o supresión por disposición general en BOE, DOGA o BOP indicando:

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a terceros países.

- Los órganos de las Administraciones responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Dado el nivel bajo se deben implementar las siguientes medidas:

- Deberá redactarse un documento de seguridad, permanentemente actualizado, en el que se indique el ámbito de aplicación del documento y los recursos protegidos, y en el que constarán:
  - las funciones y obligaciones del personal.
  - la estructura de los ficheros con datos de carácter personal.
  - las normas y procedimientos de seguridad (sistema informático, sistema operativo, aplicaciones de acceso a los ficheros, salvaguarda del sistema y protección de las contraseñas personales).
  - Un registro de incidencias y procedimiento de respuesta delimitado ante las mismas (tipo de incidencia, fecha hora, personas que la detectan, medidas tomadas...).
  - Relación actualizada de usuarios.
  - El nombramiento de un responsable de seguridad que será el encargado de verificar el cumplimiento de lo acordado en el documento periódicamente.
  - Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- El establecimiento de una correcta política de seguridad en la que se realizarán copias de respaldo y recuperación de datos, de manera que permita la reconstrucción en el mismo estado en que se encontraban en el momento de producirse la pérdida; debe habilitarse un local donde se puedan guardar las copias de seguridad situado en un lugar diferente de donde se encuentre el equipo informático.
- El establecimiento de medidas tendentes a garantizar la seguridad de los datos en caso de desecho y reutilización de las copias.
- Se debe habilitar un sistema de login y un password individual y distinto para cada usuario, que limite el acceso a la información sólo a aquellas partes de la aplicación que sea necesaria para el desarrollo de sus funciones. Se recomienda que este control de acceso esté estructurado en grupos, sobre la base de unas políticas basadas en los perfiles de la actividad de los usuarios, de forma que cada usuario esté asignado al grupo que corresponde a su actividad y sólo tenga acceso a los datos que necesite para la misma.
- Habilitar copias externas de respaldo y recuperación "backup" (u otro sistema) de los ficheros. Dichas copias deberán estar debidamente etiquetadas e identificadas con fecha y nombre del sistema en caso de que existieran varios sistemas. Las copias se podrán almacenar en la ubicación de la información original. La periodicidad de la copia de seguridad debe ser tal que permita la recuperación total de la información en caso de pérdida de los datos originales, pero dependerá de la cantidad de información, su variabilidad y del método y los sistemas que se estén utilizando. Se recomienda como mínimo una copia diaria, bien completa o incremental, y al menos una copia completa semanal.
- Considerando que el ordenador del máster dispone de impresora para emitir los correspondientes informes y que éstos pueden contener datos personales de los alumnos y/o profesores, tales informes en soporte papel, que son archivados en carpetas, no son objeto de regulación mediante la LOPD 15/99 en cuanto a las medidas de seguridad aplicables hasta el año

Se debe habilitar un sistema de login y un password individual y distinto para cada usuario, que limite el acceso a la información sólo a aquellas partes de la aplicación que sea necesaria para el desarrollo de sus funciones

Hoy en día no sólo hay que tener en cuenta, en el diseño de los sistemas de gestión de la información, cuestiones técnicas, sino que hay que tener muy presente la legislación vigente

2007, momento en que también deberán cumplir las medidas previstas para el nivel correspondiente a los datos personales que contienen, que como se ha dicho antes será de nivel básico.

4.- Conclusiones

Hoy en día no sólo hay que tener en cuenta, en el diseño de los sistemas de gestión de la información, cuestiones técnicas, sino que hay que tener presente la legislación vigente. Por este motivo habrá que prestar atención a qué datos se están tratando para saber el nivel de seguridad que se debe implementar.

5.- Bibliografía

[1] APD: http://www.agenciaprotecciondatos.es

[2] Virtualey: http://www.virtualey.com

[3] Varios autores: *Hackers procedimientos frente a sus ataques*, Virtualibro (http://www.virtualibro.com).

[4] Pintos & Salgado: http://www.pintos-salgado.com

[5] Área I.P.F.: http://www.ipf.uvigo.es

José Luis Rivas López
(jlrivas@uvigo.es)
Área I.P.F. Universidad de Vigo
José Enrique Arés Gómez
(enrares@uvigo.es)
Área I.P.F. Universidad de Vigo
Víctor Alberto Salgado Seguín
(vsalgado@pintos-salgado.com)
abogado del bufete Pintos & Salgado