Gestión académica y protección de datos

Xavier Canaleta, David Vernet
Dpto. de Informática
Enginyeria i Arquitectura La Salle
Universidad Ramon Llull
08022 Barcelona
e-mail: {xavic, dave}@salleurl.edu

Resumen

En esta ponencia pretendemos analizar si los métodos y acciones que son práctica habitual en la evaluación y la gestión académica del alumnado están afectados por la Ley Orgánica de Protección de Datos de Carácter Personal [1] (en adelante LOPD) y la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico [2] (en adelante LSSICE).

Con ello pretendemos realizar un análisis de la gestión que nos permita identificar las acciones que conllevan un claro incumplimiento de los reglamentos vigentes, incidiendo especialmente en aquellas que pueden ser tipificadas como faltas graves o muy graves. Pero, además, queremos sugerir posibles actuaciones a llevar a cabo para ajustarse a la normativa y evitar así posibles sanciones de los organismos pertinentes.

Pudiera parecer que ciertos aspectos aquí tratados son más propios del área de Derecho que del ámbito de las Tecnologías de la Información. Pero el camino recorrido desde la entrada en vigor de la LOPD hasta la actualidad, nos hace ver que es imprescindible la colaboración de profesionales de ambos sectores para una correcta interpretación y aplicación de esta legislación que tiene un marcado carácter interdisciplinar.

1. Antecedentes

Antes de proceder al desarrollo de los temas centrales de la ponencia, creemos necesario hacer una breve descripción cronológica de la normativa relacionada con la protección de datos.

El primer referente legal en el estado español sobre protección de datos lo hallamos en la Ley Orgánica 5/1992 [3], de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal, más conocida como LORTAD. La legislación española iba con cierto retraso respecto al resto de los países de Europa. Recordemos que el Convenio 108 del Consejo de Europa (donde se recogían una serie de principios para la protección de las personas en la utilización de sus datos personales incluidos en los diversos ficheros automatizados) es del año 1981; y países como Alemania, Austria, Francia e Inglaterra desarrollaron leyes sobre protección de datos e informática a finales de los años 80.

En 1994 aparece, en el Real Decreto 1332/1994 de 20 de junio [4], un reglamento donde se desarrollan ciertos aspectos de la LORTAD, exceptuando uno muy importante: la seguridad y las medidas a adoptar.

El 24 de octubre de 1995 se publica la Directiva Europea 95/46/CEE [5], donde, en su artículo 17, se recogen una serie de obligaciones respecto al tratamiento de datos de carácter personal realizado por terceros. Estas van desde el establecimiento en un contrato que detalle esta responsabilidad hasta la implantación de las medidas técnicas que garanticen la seguridad de dichos datos.

Y no es hasta 1999, concretamente el 25 de junio, cuando sale publicada en el BOE el Real Decreto 994/1999 de 11 de Junio [6], por el cual se aprueba el Reglamento de medidas de seguridad de ficheros automatizados que contengan datos de carácter personal. Este reglamento es una pieza clave ya que hace que la LORTAD sea operativa.

Y el 14 de diciembre del mismo año, se publica la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) que deroga la LORTAD. Esta ley es una actualización de la

NIVEL	TIPO DE DATOS	MEDIDAS A ADOPTAR
Básico	• Nombre y apellidos • Direcciones (física y electrónica) • Teléfono (fijo y móvil)	• Documento de Seguridad • Registro de incidencias • Identificación y autenticación de usuarios • Control de acceso • Gestión de soportes • Copias de respaldo y recuperación
Medio	• Información de Hacienda Pública • Infracciones administrativas • Infracciones penales • Información financiera	• Medidas de seguridad de nivel básico • Creación del Responsable de Seguridad • Auditoría bianual • Medidas adicionales de autenticación • Medidas adicionales de identificación
Alto	• Ideología y creencias • Religión • Origen racial • Salud	• Medidas de nivel básico y medio • Seguridad en la distribución de soportes • Registro de accesos • Cifrado en las telecomunicaciones

Tabla 1. Niveles de protección de datos y medidas de seguridad

antigua LORTAD. Quizás la novedad más importante en relación a la LORTAD es la extensión en su ámbito de aplicación a los ficheros no automatizados. Otro aspecto a tener en cuenta es la diferenciación en tres niveles de protección de datos, dependiendo de la naturaleza de los mismos, y la descripción de las medidas de seguridad a adoptar en cada caso (véase Tabla 1). Y finalmente recordar que la LOPD no deroga el Reglamento de la LORTAD sino al contrario: en su disposición transitoria tercera explicita la subsistencia de las normas preexistentes a la LOPD que no la contradigan.

La consecuencia de lo expuesto en el párrafo anterior es la vigencia de los plazos de implantación de las medidas de seguridad que el Real Decreto 994/1999 establecía: 26 de diciembre de 1999 para las medidas de nivel básico, 26 de junio de 2000 para las de nivel medio y 26 de junio de 2001 para las de nivel alto.

En relación a estos plazos cabe mencionar que el Real Decreto 195/2000 [7], de 11 de febrero, amplía el plazo para implantar las medidas de seguridad para el nivel básico. La nueva fecha pasa a ser el 26 de marzo de 2000. Y la Resolución de 22 de junio de 2001 [8] acaba fijando la fecha definitiva para la implantación de medidas de nivel alto el 26 de junio de 2002.

Y la última Ley española relacionada con los sistemas de información y la protección de datos sale publicada en el BOE número 166, de 12 de julio de 2002. La Ley 34/2002 es la que se conoce como la LSSICE: Ley de servicios de la sociedad de la información y comercio electrónico. Esta Ley pretende regular jurídicamente ciertos aspectos que se derivan del uso de las nuevas tecnologías de la información, en especial Internet, y muy directamente lo que se conoce como el comercio electrónico. La LSSICE, además de cubrir un vacío jurídico evidente en lo que se refiere a legislación informática en Internet, pretende dar protección de los intereses de los consumidores en el comercio electrónico.

2. Análisis del entorno académico

En primer lugar vamos a definir nuestro entorno de trabajo para poder determinar así en qué situación nos encontramos y qué normas nos afectan.

Queremos desvincular, en una aproximación inicial, el entorno académico del entorno administrativo. Por entorno académico nos referiremos a los datos relacionados con los alumnos y su currículum universitario. De este modo, podríamos enumerar ciertos contenidos que pueden ser considerados información académica. Esta lista no pretende especificar todos los datos

exhaustivamente sino dar una idea descriptiva del tipo de contenidos de esta información:

- Datos personales del alumno: como pueden ser el nombre y apellidos, la fecha de nacimiento, el domicilio, los teléfonos de contacto, la dirección electrónica, etc.
- Datos académicos: incluiríamos aquí toda la información referente al historial académico del alumno, donde constan, entre otros datos, las asignaturas que ha cursado y sus correspondientes calificaciones.
- Datos logísticos: en este apartado hallaríamos información que nos indique a qué grupo ha asistido dentro de una determinada asignatura, cuál era su horario de clases, qué profesores impartían los créditos a los que estaba matriculado, etc.

No consideramos que pertenezca al ámbito académico aquella información de naturaleza económica relacionada con los alumnos, como pueden ser los importes de matriculación y créditos cursados, los datos de la domiciliación bancaria para satisfacer dichos importes, el importe de las becas que le hayan sido concedidas, etc. Este tipo de datos del alumno los ubicamos dentro del entorno administrativo y no serán objeto de nuestro estudio.

Una vez especificado nuestro ámbito de trabajo podemos proceder al análisis del mismo y determinar qué leyes descritas anteriormente le afectan y en qué medida.

Los datos personales que se pueden encontrar en ficheros, informatizados o en soporte papel, referentes al entorno académico podemos concluir que son de nivel bajo. No se especifica en ninguno de los documentos en vigor nada referente a los datos académicos de una persona física por lo que debemos considerarlos estrictamente datos de carácter personal, tipificados estos de nivel básico. De este modo hemos de tener en cuenta que la información académica se halla afectada por la LOPD y también por el Reglamento 994/1999 en vigor sobre las medidas de seguridad.

Otro punto a analizar es la Ley 34/2002, más conocida como la LSSICE y su posible aplicación a la gestión académica. Parece lógico pensar que actualmente la gran mayoría de la información académica se almacena en soporte informático. Por lo que podemos intuir que su tratamiento irá más allá del mero almacenamiento en ficheros automatizados y, con toda probabilidad, se aplicarán las nuevas tecnologías de la información y comunicaciones (Internet) para dicha gestión académica. Pero aunque así sea y se usen los servicios de la sociedad de la información para agilizar y facilitar las actualizaciones y consultas de datos académicos, también es cierto que estos no se utilizan para generar comunicaciones comerciales ni para la contratación electrónica. Los servicios académicos que se suelen ofrecer a través de campus virtuales a los alumnos no pueden considerarse en modo alguno dentro del campo de aplicación de esta Ley y todos los datos de carácter personal que se gestionen deben regirse por las normas de la LOPD, que tienen como objetivo proteger el derecho a la intimidad y la privacidad de datos.

En resumen, la información académica y las operaciones que realicemos con ella deberán adecuarse a las normas establecidas por la LOPD y el Reglamento LORTAD vigente. Además, tendrán que adoptarse las medidas de seguridad especificadas para datos de nivel básico.

De todos modos, nos gustaría dejar constancia que una ley permite diferentes lecturas y, consecuentemente, distintas interpretaciones. Con ello pretendemos decir que si bien parece evidente que los datos académicos son, en sí mismos, de nivel básico, no es menos cierto que a través de un expediente académico se puede inducir un perfil de personalidad. ¿No es lógico pensar que si analizamos el historial académico de un alumno con calificaciones brillantes en su expediente y, de repente, encontramos un descenso drástico y global en sus notas, deduciremos que se encuentra en un momento de crisis personal y nos será más sencillo intuir que ese alumno tiene alguna problemática (ya sea laboral, sentimental o familiar) en su entorno? ¿No es verdad que los tutores utilizan los datos académicos de los alumnos para poder analizar su evolución, sus preferencias e inclinaciones profesionales? ¿Y de este modo poder evaluar múltiples aptitudes como pueden ser la tenacidad, capacidad de trabajo, constancia, extroversión, etc., que van más allá del mero perfil académico? Y, llegados a este punto, ¿podríamos concluir que estos datos podrían ser considerados de nivel alto?

3. Medidas de seguridad

Dado que los ficheros con datos académicos se ven afectados por la LOPD, estos deben ser declarados a la Agencia de Protección de Datos. Esta notificación puede hacerse por correo ordinario. También puede realizarse casi en su totalidad vía Internet a través de la página web https://www.agenciaprotecciondatos.org.

Seguidamente se procederá a la adopción de las medidas de seguridad de nivel básico para los ficheros afectados. Vamos a detallar en qué consiste cada una de ella y las acciones que deben llevarse a cabo en el caso que nos ocupa.

3.1. Documento de seguridad

Se ha de redactar un documento donde se detallen las normas a seguir por todo el personal que tenga acceso a los datos académicos con el fin de garantizar la protección de los mismos. Este documento también debe de contener la descripción de todos los procedimientos exigidos para las medidas de seguridad para el nivel básico. Algunos ejemplos serían: un procedimiento que especifique cómo, cuando y quién realiza las copias de seguridad; otro procedimiento que determine cómo se realiza la recuperación de datos si hay una caída del sistema, etc. Este documento debe estar actualizado, por lo que se ha de realizar una revisión del mismo con cierta periodicidad. La universidad también debe garantizar que el documento de seguridad sea del conocimiento de todo el personal involucrado en el tratamiento de datos académicos.

3.2. Registro de incidencias

Debe existir un formulario que ha de cumplimentarse en el caso que se produzca alguna incidencia que afecte a los ficheros con información académica. Así que cada vez que haya una interrupción en el suministro eléctrico que provoque una parada de los servidores de datos, o se produzca una avería en los soportes magnéticos o exista algún problema con las comunicaciones que no permita acceder a la información sensible (por poner tres ejemplos bastante habituales), dicha incidencia deberá quedar registrada en un formulario.

3.3. Identificación y autenticación de usuarios

El centro universitario debe asegurar que el acceso a los datos académicos sólo lo realizarán aquellas personas que estén habilitadas para ello. De este modo el acceso a los sistemas de información que permitan la consulta o actualización de información académica debe estar controlado. El mecanismo más común se basa en la existencia de nombres de usuario y contraseñas. Se acostumbra a adoptar un conjunto de normas que permitan garantizar la inequívoca identificación y autentificación de los usuarios en el sistema de información. Quizá alguna de las normas que citaremos conlleve un grado de protección más exigente que las estrictamente requeridas en el nivel básico, pero de todos modos aconsejamos que se implanten:

- no están autorizados usuarios genéricos que permitan accesos al sistema. Así pues, el usuario "profesor" no sería válido ya que permitiría el acceso al sistema a diversas personas y no se podría conocer qué persona en concreto está accediendo a la información protegida.
- activación de la caducidad de *passwords*: habitualmente con una periodicidad mensual o bimensual se fuerza que el usuario cambie su contraseña. De este modo limitamos el uso de contraseñas que hayan podido ser sustraídas de sus dueños.
- guardar un histórico de contraseñas, con el fin de evitar repeticiones en los cambios y obligar a los usuarios a cambiar realmente la palabra de paso.
- bloquear la cuenta de usuario a partir de un cierto número de intentos fallidos, con el objeto de limitar posibles accesos no autorizados de forma reiterada.
- No permitir *passwords* triviales: no se deben usar como contraseñas datos obvios del usuario como pueden ser sus iniciales, fecha de nacimiento, nombre de sus familiares cercanos, etc. Estas son las palabras habituales que se usan para intentar acceder al sistema.

3.4. Control de acceso

Esta medida determina que el personal sólo tendrá acceso a los datos académicos que le sean necesarios para desempeñar su trabajo. Del mismo modo únicamente se autorizarán las operaciones estrictamente requeridas sobre estos datos. Así pues, un profesor sólo debe tener acceso a los datos académicos de sus alumnos y, siendo extremadamente estrictos, a los referentes a su asignatura. Un profesor de la asignatura de Programación no debería tener acceso a las calificaciones de sus alumnos en la asignatura de Electrónica. En cambio un tutor debe tener acceso a todos los datos académicos de sus alumnos para poder desarrollar correctamente sus funciones. Y no sólo esto sino que el tutor de un alumno, evidentemente, podrá tener acceso a los datos de ese alumno pero en modo consulta y no actualización ya que no es el responsable de evaluar a ese alumno en las diferentes materias de las que este se haya matriculado.

Todas las acciones anteriores tienen como objetivo limitar el acceso lógico a los datos. En este sentido creemos necesario hacer notar que a veces controlamos correctamente los accesos lógicos a los datos y olvidamos el posible acceso físico. Por ello queremos insistir en el estricto control de acceso físico a la sala de servidores y también en un hábito que parece una nimiedad pero que acostumbra ya a aparecer como norma para los usuarios del sistema de información en las empresas: la obligatoriedad de bloqueo de la estación de trabajo en ausencia del trabajador y la activación del salvapantallas en un tiempo no superior a 5 minutos y su posterior desbloqueo con contraseña. De este modo evitaremos posibles descuidos de bloqueo del terminal y podremos garantizar la no vulnerabilidad física del sistema.

El control de acceso descrito hasta el momento es un control lógico.

3.5. Gestión de soportes

Los soportes que contengan información académica deberán estar correctamente identificados, tienen que estar inventariados y almacenados en un lugar de acceso restringido al personal autorizado. La salida de soportes informáticos con datos académicos fuera de los locales de ubicación de los ficheros debe quedar registrada y tiene que estar autorizada por el responsable del fichero. Si se pretende hacer una copia de las calificaciones de alumnos en un disquete o CD-ROM para poder trabajar con ella desde otro lugar, esta acción ha de estar autorizada explícitamente por el responsable de los datos y, además, ha de quedar constancia escrita de esta salida de información. Al ser información sensible, estos datos no han de ser accesibles por cualquier persona fuera del centro.

3.6. Copias de respaldo y recuperación

Es necesario realizar copias de seguridad de los datos académicos periódicamente. Esta operación es habitual hoy en día en la mayoría de centros. La periodicidad de las copias (diaria, semanal, etc.) variará según la volatilidad de la información. Muchos centros acostumbran a realizar copias de *backup* todos los días. Sin embargo no es tan frecuente verificar que estas copias permitan la recuperación de los datos en caso de pérdida de los mismos en el sistema. Esta medida de seguridad nos obliga a realizar pruebas de recuperación periódicamente. Las empresas que cumplen dicha medida hacen estas verificaciones trimestral o semestralmente.

4. Prácticas punibles

Una vez descritas las acciones necesarias para adoptar las medidas de seguridad exigidas por la LOPD, podríamos pensar que ya estamos cumpliendo correctamente las disposiciones de la Ley y también del Reglamento. Lo cierto es que hay prácticas habituales que se realizan en la gestión académica en entornos universitarios que son claras infracciones a la LOPD e, incluso, vulneran el artículo 18.4 de la Constitución Española, que no es otro que el derecho a la intimidad. Citamos textualmente: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

No pretendemos aquí realizar una persecución inquisidora de estas prácticas. Nuestro objetivo se limita a detectar y exponer ciertos hábitos que pueden ser constitutivos de infracción y proponer acciones alternativas que nos permitan actuar

dentro de las normas establecidas y evitar así posibles sanciones.

Empezaremos con una de las prácticas más habituales en el mundo académico como es la publicación de resultados de unos exámenes ya sean parciales o finales. El modo más usual de informar a los alumnos de sus calificaciones es que cada asignatura publique listas con sus notas. Si nos fijamos esta acción vulnera el principio de privacidad ya que se están haciendo públicos datos de carácter personal de los alumnos. Los artículos 6 y 11 de la LOPD informan que para comunicar datos personales a un tercero se necesita el consentimiento previo del afectado. De este modo todos los alumnos deberían hacer constar, o no, si permiten la notificación pública de calificaciones. Esto crearía un primer problema ya que ciertos alumnos aceptarían dicha publicación pero otros no. Un segundo problema viene dado por el derecho que tiene el alumno, según los mismos artículos, a revocar dicha autorización en cualquier momento. Creemos que este camino no lleva a ninguna solución viable. Se ha optado por soluciones intermedias como puede ser la publicación de listas de notas donde sólo existe el número de expediente de cada alumno y su nota. Esta solución tampoco cumple el objetivo de privacidad si existen sistemas accesibles al público que permitan a partir del nombre de un alumno obtener su expediente. La propuesta que parece más lógica es la de comunicar los resultados de las diferentes asignaturas personalmente a cada interesado. En este aspecto las tecnologías de la información nos facilitan dicha tarea ya que es relativamente sencillo diseñar un entorno donde permita el acceso personalizado al expediente de cada alumno según su nombre de usuario y contraseña. Nuestra experiencia de utilizar el campus virtual de nuestra escuela de ingeniería (*e-campus*), donde los alumnos pueden consultar sus notas de forma individualizada, ha tenido gran éxito, no tan solo por la privacidad de datos sino por la facilidad de acceso vía Internet desde cualquier punto geográfico. En resumen, hablando claramente podemos concluir que las listas de notas publicadas ya sea en los tablones de anuncios son una práctica ilegal según la LOPD. Y soluciones intermedias como la publicación de un documento pdf con la misma lista de notas en una intranet del campus universitario virtual al cual tienen acceso sólo los alumnos matriculados de esa asignatura continua infringiendo la Ley de Protección de Datos.

Otra práctica habitual, realizada sin ningún ánimo perverso, es la divulgación a través de la Red de imágenes personales. Sea a través de Internet o en una *intranet* de un centro universitario, la divulgación de fotografías personales está prohibida sin el consentimiento explícito de la persona.

Actualmente la mayoría de universidades, y en especial las que tienen estudios científico-técnicos, poseen desde una simple página web hasta un completo campus virtual donde el alumno encuentra multitud de servicios de gran utilidad para su vida académica. El problema está en que, pretendiendo ser una ayuda para el alumno, se ofrezcan servicios que difundan datos de carácter personal. Una utilidad habitual en los campus virtuales es el buscador. Esta herramienta permite a cualquier usuario de Internet realizar consultas de otros alumnos a partir de su nombre y apellidos o su número de expediente. La búsqueda nos permite obtener información de aquel alumno; nos facilita su dirección electrónica y su URL si esta existe. Este servicio nuevamente vulnera la Ley ya que permite la obtención a terceros de datos de carácter personal sin el consentimiento expreso del alumno.

La solución tecnológica para estos casos de consentimiento del alumno y derecho a una posible revocación de este sería poder implantar un pequeño aplicativo en la web, con acceso por *login* i *password*, que le permita al alumno la configuración de su perfil. De este modo podría actualizar sus datos personales, podría activar o no el consentimiento para la difusión de su fotografía, *e-mail* y URL a través de la web o a través de la *intraweb*.

5. Conclusiones

Se han presentado en esta ponencia las medidas de seguridad que deben adoptarse para los ficheros de datos académicos, dada su condición de datos de carácter personal de nivel básico. También se han descrito acciones habituales en la gestión de la información académica que constituyen una infracción a la LOPD y se han propuesto soluciones efectivas encaminadas a solucionar

este conflicto sin que por ello se deba renunciar a los objetivos que tenían dichas acciones.

Con todo, creemos que sería fácil de constatar que en muchos entornos universitarios las medidas de seguridad que hemos descrito no se han aplicado o si se han aplicado no están siendo seguidas. Adicionalmente, se siguen utilizando frecuentemente métodos en la gestión académica que son claras infracciones a la LOPD.

Llegados a este punto, creemos que es necesario hacerse la siguiente reflexión: ¿por qué no se han implantado las medidas de seguridad que marca la ley? ¿Por qué sigue siendo tan habitual la gestión académica mediante acciones que suponen infracciones tipificadas como graves por la LOPD? Sería ingenuo pensar que es debido a los altos costes que suponen la implantación de las medidas de seguridad exigidas y las soluciones alternativas a los métodos usados. Pensamos que ha quedado constancia que ni dichas medidas suponen un coste elevado para las universidades ni la adopción de nuevos métodos de trabajo tiene una complicación tecnológica excepcional.

La realidad es que convergen un conjunto de factores que hacen que nos encontremos en esta situación. Un primer factor determinante es la falta de información y formación: creemos que hay un gran desconocimiento en el sector informático, como en muchos otros, de las obligaciones y normas que afectan a los ficheros con datos de carácter personal. Para ello no hallamos otra solución que informar a los formadores y, posteriormente, informar y formar a los futuros profesionales del sector, nuestros alumnos. Existen diferentes sistemas para conseguir este objetivo. Una posibilidad que debería plantearse seriamente sería la incorporación de créditos obligatorios dentro de los planes de estudios que desarrollen esta temática que, por supuesto, afecta a todos los profesionales de la informática, sea cual sea su especialidad. De todos modos, nosotros abogamos más por una solución quizá más compleja de ejecutar pero más efectiva: creemos que la información sobre la legislación que afecta al sector debe darse con más continuidad e insistencia. La solución de añadir una asignatura, aunque no nos parece mal, no creemos que sea del todo efectiva. Evidentemente cumpliríamos el objetivo de informar pero no el de concienciar. Esta tarea es interdisciplinar y debe tener un pequeño hueco temporal reservado dentro de cada una de las asignaturas del plan de estudios. La manera de concienciar a futuros profesionales de la importancia de la protección de datos, que tiene su arraigo en el derecho constitucional a la intimidad, es informar desde distintas ópticas y eso sólo es posible hacerlo con la colaboración de todo el estamento académico. De hecho, existen iniciativas en ese aspecto (por ejemplo Créditos de Libre Configuración, cursos de postgrado, etc.) pero nos ha sido realmente difícil hallar propuestas que tengan un ámbito de aplicación transversal como proponemos en este artículo.

Un segundo factor que influye decisivamente es el aspecto cultural. Por naturaleza el ser humano es reticente al cambio. Así que el hecho de adoptar nuevos métodos de trabajo y adquirir nuevos hábitos siempre encuentra cierta oposición. Por experiencia propia sabemos que la implantación de nuevas metodologías de trabajo es costosa, aunque esta tenga las mismas funcionalidades que la anterior e incorpore mejoras considerables. Nadie duda hoy en día que tener las calificaciones de los alumnos en una hoja de cálculo o base de datos es infinitamente más cómodo y eficaz que mantenerlas en soporte papel: agilidad de cálculo de promedios, posibilidad de actualización de datos, rapidez en las consultas, etc. Así mismo, ¿alguien del sector tecnológico puede cuestionar que tener un entorno en Internet donde se puedan publicar, actualizar y consultar datos académicos tiene las mismas ventajas y adicionalmente otras como pueden ser la accesibilidad, movilidad y protección de datos?

Finalmente también querríamos hacer notar la falta de implicación de la dirección en este asunto. Argumentamos los mismos motivos que en los docentes: desconocimiento, falta de formación, etc. Esto nos llama la atención sobretodo si tenemos en cuenta las grandes sanciones económicas que suponen las infracciones de la LOPD. Mientras que, mayoritariamente, las directivas de las empresas ya han tomado las medidas adecuadas para cumplir la normas que se derivan de la LOPD, pensamos que los en centros universitarios no se ha llegado aún a ese punto. Hechos como que no existan cláusulas relativas al cumplimiento de la LOPD en los contratos de los profesores universitarios, que no se divulgue entre estos una Normativa de Seguridad Informática o que ni exista esta constatan esta situación.

Agradecimientos

Queríamos aprovechar la oportunidad para agradecer al jefe del Departamento de Informática de Ingeniería y Arquitectura La Salle (Universidad Ramon Llull), la motivación que nos ha dado para redactar la presente ponencia. Nos ha transmitido su denodado interés por estos temas, así como la preocupación por la falta de concienciación que existe por ellos.

Referencias

[1] "Ley Orgánica 15/1999, de 13 de diciembre", *BOE* nº 298, 14 de diciembre de 1999.
[2] "Ley 34/2002, de 11 de julio", *BOE* nº 166, 12 de julio de 2002.
[3] "Ley 5/1992, de 29 de octubre", *BOE,* de octubre de 1992.
[4] "Real Decreto 1332/1994, de 20 de junio", *BOE*.
[5] "Directiva 95/46/CE, de 24 de octubre", *DOCE*.
[6] "Real Decreto 994/1999, de 11 de junio", *BOE* nº 151, 25 de junio de 1999.
[7] "Real Decreto 195/2000, de 11 de febrero", *BOE* nº 49, 26 de febrero de 1999.
[8] "Resolución de 22 de junio de 2001", *BOE* nº 151, 15 de junio de 2001.