

UNIVERSIDAD COMPLUTENSE DE MADRID

Facultad de Ciencias de la Información

Dpto. Biblioteconomía y Documentación



**PROTECCION DE DATOS
EN LA BIBLIOTECA DE
LA UNIVERSIDAD COMPLUTENSE**

Presentada por Juan José Prieto Gutiérrez

DIPLOMA DE ESTUDIOS AVANZADOS

Director: Fernando Ramos Simón

Madrid 2006

ÍNDICE

Introducción	4
Objetivos y metodología	4

PRIMERA PARTE

Protección de Datos en España

- Introducción 5
- Orígenes 9
- Principios:
 - Relativos a los derechos del afectado 13
 - Relativos a los ficheros 20
- Datos especialmente protegidos 24
- Cesión de datos a terceros 26
- Ficheros de titularidad pública / privada 28
- Las Agencias de Protección de Datos 30

SEGUNDA PARTE

Protección de datos en la Biblioteca Universidad Complutense de Madrid

- Introducción. 36
- Protección de datos en la Biblioteca de la Universidad Complutense de Madrid. 40
- Inserción de datos en el Fichero.
- Mantenimiento del fichero. 47
- Comparación del fichero de la biblioteca de la Complutense con la Universidad Autónoma de Madrid 57
- Encuestas: 61
 - Usuarios
 - Personal de la BUC

Conclusiones 75

Bibliografía 76

Anexos 77

- Tablas
- Modelo de notificación de ficheros de la APDCM
- Legislación

Introducción

El propósito fundamental de la realización del estudio es dar a conocer la Protección de Datos de carácter personal, fundamentalmente en la Biblioteca de la Universidad Complutense y de una forma más general de la propia Universidad. Con éste fin se intenta mostrar los derechos y principios a los que se acoge la Comunidad Universitaria. Así se aspira a mejorar los conocimientos por parte del personal de la biblioteca como el de los propios usuarios de la misma.

A fecha de junio de 2006, el tema de Protección de Datos de Carácter Personal relacionado con las bibliotecas, suscita poco interés, pero día tras día, se escriben mas artículos en revistas, en foros de Internet, relacionados con la archivística y la documentación. En ellos se habla y se comenta acerca de si los datos personales de los usuarios de las bibliotecas y los historiales de préstamo de cada uno de ellos pueden ser o no objeto de consulta por parte de los trabajadores de las bibliotecas o de los propios usuarios. Existe variedad de opiniones fundamentalmente, por el desconocimiento de las leyes.

Metodología y objetivos

El estudio comprende dos partes bien diferenciadas, la primera trata el grueso teórico referente a la Protección de Datos de Carácter Personal de diferentes Leyes Orgánicas y los principios de los derechos de los afectados y los relativos a los ficheros. En este mismo bloque se incluye la diferente tipología de datos así como los ficheros. Este apartado nos da una visión general sobre la Protección de Datos en España.

La segunda parte del trabajo es práctica, se centra en el fichero de la Biblioteca de la Universidad Complutense de Madrid, llamado “Usuarios de la Biblioteca”.

Para llevar a cabo la investigación se ha realizado diferentes sondeos; por medio de una encuesta realizada a usuarios y a trabajadores de la biblioteca sobre una base de seis preguntas baremadas desde la unidad al seis. El resultado de las encuestas fue el esperado, ya que se llega a la conclusión del desconocimiento de la existencia del

fichero sobre protección de datos, por parte de la comunidad universitaria y la creencia por parte de los estudiantes de la limitación del acceso al fichero por parte de los trabajadores de la biblioteca. Con los diferentes resultados se recaba una información que nos lleva a conclusiones cuyo objetivo es el de ayudar a la comunidad universitaria.

Otro de los sondeos mencionados fue la comparativa entre la Protección de Datos en la Biblioteca de la Universidad Complutense con la de la Universidad Autónoma de Madrid. Existe una gran semejanza entre los ficheros, empezando por la existencia de un solo fichero en cada biblioteca, la formación de los mismos es pareja, a través de los respectivos programas de matriculación de primer, segundo y tercer ciclo provenientes de las respectivas Secretarías. Ambas bibliotecas dan cada vez mas importancia a la Protección de Datos de carácter personal.

La biblioteca de la Universidad Autónoma de Madrid está mas implicada en el ámbito de la Protección de Datos que la de la Universidad Complutense de Madrid, empezando por la nota informativa expuesta en los mostradores de préstamo y por la constancia de los procesos de modificación y supresión de los datos que forman su fichero. Sus objetivos futuros son comunes, como la creación y formación de unidades de Protección de Datos (la Universidad Complutense de Madrid ya ha creado la suya).

Otro apartado de la metodología está formado por la bibliografía aportada, tanto de monografías, de artículos en revistas, como de páginas visitadas en Internet, etc.

Finalmente se incluye un apartado de anexos, los cuales están formados por, las tablas de los resultados de las encuestas realizadas a los usuarios y trabajadores de la Biblioteca de la Universidad Complutense de Madrid, el modelo de notificación de los ficheros de la Agencia de Protección de Datos de la Comunidad de Madrid.

La Protección de Datos en España

Introducción:

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Etimológicamente la palabra persona proviene del verbo latino *sono, as, are* (sonar). Desde este punto de vista, persona es igual a hombre, a ser humano. Hoy en día nadie pone en duda que todos los seres humanos somos personas, esto es, sujetos portadores de valores que ha de reconocer y respetar la organización social, y especialmente al Estado como expresión del grupo social organizado en que nos movemos. La idea de que todo ser humano es persona, por encima e incluso antes de que la colectividad organizada constituya el eje del Derecho civil y del Derecho en general.

La información relativa a las personas, denominada «datos personales», se recoge y emplea en muchos ámbitos de la vida cotidiana. Una persona física ofrece datos personales cuando, por ejemplo, cumplimenta un formulario para obtener un carné de biblioteca, se apunta a un gimnasio, abre una cuenta corriente, etc. Los datos personales pueden proceder directamente del interesado o de un fichero existente. Posteriormente, estos datos pueden utilizarse para otros fines o comunicarse a terceros. Los datos personales pueden ser cualquier dato que permita identificar a una persona física, como un nombre, número de teléfono o fotografía.

El derecho a la intimidad deriva de los derechos fundamentales a la vida, libertad y propiedad. La intimidad constituye un derecho de la personalidad y como tal ha de ser considerado como irrenunciable. Se podría definir el derecho a la intimidad como el derecho del individuo de decidir por sí mismo en que medida compartirá con otros sus pensamientos, sentimientos y los hechos de su vida privada. Intimidad es la parte interior que solamente cada uno conoce de sí mismo. Lo íntimo está protegido por el sentido del pudor. La dignidad humana, dentro de la esfera de lo social, se garantiza en la medida en que tenga la posibilidad de conservar su privacidad, entendida como aquel fuero interno que sólo puede interesar al ser humano como individuo o dentro de

un contexto reducido de personas que en últimas está determinada por el consentimiento de quien es depositario de su existencia.

Para Hernán Alejandro Olano García ¹ la intimidad es “ un derecho que se proyecta en dos dimensiones, como secreto de la vida privada y como libertad. Concebida como secreto, atentan contra ella todas aquellas divulgaciones ilegítimas de hechos propios de la vida privada o familiar o las investigaciones también ilegítimas de hechos propios de la vida privada. Concebida como libertad individual, en cambio, trasciende y se realiza en el derecho de toda persona de tomar por si sola decisiones que conciernen a la esfera de su vida privada. Es claro que los atentados pueden provenir tanto de los particulares como del estado. Se ha creído necesario proteger la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas.

La lucha por los derechos humanos es por tanto una lucha permanente, para que todos nuestros hermanos, en todos los países del mundo, tengan condiciones de vida de seres realmente humanos, se realicen plenamente, vivan fraternalmente, en la paz efectiva entre las personas y entre las naciones. El «otro mundo posible» es aquel en el que la dignidad propia de todo ser humano, de cualquier ser humano, nunca será puesta en duda y será siempre defendida con toda la fuerza de nuestros corazones, en el amor, que es el único camino para la redención de la humanidad.

Existe una nueva óptica entre los problemas relacionados entre intimidad e informática. Esta libertad informática surge en España de los planteamientos vertidos en 1984, y aun antes, con vistas a reglamentar el artículo 18.4² de la CE, ya que

¹ Olano García, Hernán Alejandro en su texto de la Constitución Política de Colombia. Bogotá, *Doctrina y Ley*, 2002.

² El artículo 18.4 de la Constitución se inscribe dentro de un precepto dedicado a la protección de la intimidad en general. El artículo 18.4 se refiere a una dimensión de la intimidad, aquella que tiene que ver con las informaciones sobre la vida de una persona que, de tal modo determinen el ámbito de lo que propiamente podríamos llamar su personalidad, que podrían, manejados por terceros y, fundamentalmente, por los poderes públicos, violentar el principio de la dignidad de la persona, de los derechos inviolables que le son inherentes, del libre desarrollo de su personalidad, todos ellos valores establecidos en el artículo 10 de nuestra Constitución.

resultaba insuficiente la normativa anterior frente a algunos atentados y agresiones producidas por el fenómeno informático.

Los avances de la informática, junto con las nuevas redes de telecomunicaciones, permiten la transferencia transnacional de datos personales con mayor comodidad. A consecuencia de esto, los datos relativos a los ciudadanos de un Estado miembro a veces son tratados en otro Estado miembro de la Unión Europea (UE). Al aumentar la recogida e intercambio de datos personales, se hace necesaria una norma sobre transferencia de datos.

Por regla general, las leyes nacionales sobre protección de datos exigen unas prácticas adecuadas en materia de gestión de datos por parte de las entidades que los tratan, denominadas «responsables del tratamiento». Una de estas prácticas es la obligación de tratar los datos correctamente y de forma segura, y de emplear los datos personales con fines explícitos y legítimos. Las leyes nacionales también garantizan una serie de derechos de las personas físicas, tales como el derecho a ser informado de cuándo y por qué se ha realizado el tratamiento de datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a modificar o suprimir los datos.

Si bien las leyes nacionales sobre protección de datos buscaban, ya desde la Declaración de los Derechos Humanos de 1948 y desde el Comité de Ministros de 26 de septiembre de 1973 relativa a "La protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado", con alguna diferencia. Tales diferencias podían suponer obstáculos para la libre circulación de información y crear trabas adicionales para los operadores económicos y los ciudadanos. Entre estas figuraban tener que registrarse o ser autorizado a tratar datos por las autoridades de control de varios Estados miembros, la necesidad de ajustarse a distintas normas y la posibilidad de tener limitaciones para transferir datos a otros Estados miembros de la UE. Por añadidura, algunos Estados miembros no tenían leyes sobre protección de datos.

Por estos motivos, era necesaria una acción a escala europea, que tomara la forma de directivas comunitarias³.

El concepto de protección de datos nació como una mera contraposición a la interferencia en la vida privada de las personas facilitada por el avance tecnológico. Sin embargo, con el transcurso del tiempo, esa concepción fue evolucionando hasta llegar al momento actual en el que la doctrina internacional lo entiende como la protección jurídica de las personas en lo concerniente al tratamiento de sus datos personales, tanto en forma manual como automatizada.

Más allá de la reconocida evolución doctrinal de este concepto, es indudable que con el correr de los años la posibilidad de disponer de información sobre las personas ha ido paulatinamente en aumento. Si a ello se le suma el importante papel que las bases de datos desempeñan en el mundo tecnificado y globalizado de hoy, surge con pocas dudas el derecho de las personas a protegerse frente a la intromisión de los demás.

Como explica Pablo Lucas Murillo de la Cueva⁴ el bien jurídico subyacente es la autodeterminación informativa que consiste en el derecho que toda persona tiende a controlar toda la información que le concierne, sea íntima o no, para preservar de este modo y en el último extremo, la propia identidad, su dignidad y libertad. Este derecho a la autodeterminación informativa fue llamado por primera vez de esta manera⁵ en la Tribunal Constitucional Alemán del 15 de diciembre de 1983, que declaró inconstitucionales ciertos aspectos de la Ley del Censo de Población de 1982 de la República General Alemana.

La referida sentencia destacó como contenido del derecho a la personalidad la facultad de decidir por si mismo cuando y dentro de que límites procede revelar situaciones referentes a la propia vida. Reconoció además que esta facultad requiere de especiales medidas de protección ya que la interconexión de varias colecciones de datos puede converger en la elaboración de un perfil de la personalidad y puede influir en la autodeterminación del individuo y en su libertad de decisión. Haciendo un pequeño

³ Directiva 95/46/CE del Parlamento Europeo, Directiva 97/66/CE y la Directiva 2002/58/CE.

⁴ Murillo de la Cueva, Pablo Lucas. *“El derecho de la autodeterminación informativa”*. Editorial Tecnos. Madrid, España, 1990)

⁵ en alemán, Recht auf informationelle Selbstestimmung.

resumen, basado en la exigencia de consentimiento para que la recogida y el tratamiento de datos sean lícitos, el derecho a la autodeterminación informativa sobre el que se apoya el concepto de protección de datos personales, no solo entraña un específico instrumento de protección de los derechos del ciudadano, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona y decidir sobre la difusión y la utilización de sus datos. Así lo ha entendido el Tribunal Constitucional español⁶ al decir que el derecho fundamental a la protección de datos persigue garantizar a las personas el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

⁶ Véase T.C. *en la sentencia 30/11/2000, fundamento 6.*

Orígenes de la Protección de Datos:

La normativa actual sobre protección de datos tiene sus orígenes más remotos en el artículo 12 de la Declaración de derechos humanos de 1948 que establece la protección contra la injerencia arbitraria en la vida privada, así como el derecho a la libertad de opinión y expresión que incluye el derecho a no ser molestado a causa de las opiniones (art. 19). Además, el Consejo de Europa estableció unas directrices básicas, como son la resolución del Comité de Ministros de 26 de septiembre de 1973, sobre la protección de la vida privada de las personas físicas frente a los datos electrónicos en el sector privado, y la de 20 de septiembre de 1974, referente a los bancos de datos del sector público, recogidos en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado en España el 31 de enero de 1982.

El artículo 18 de la Constitución Española garantiza el derecho al honor a la intimidad personal y familiar y a la propia imagen estableciendo que 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. Por tanto en el momento de redactar la Constitución española empezó a hablarse de la materia de protección de datos sobre personas físicas, ya que en su artículo 18.4 se prevé que algún día deberá regularse el tratamiento automatizado de los datos de las personas.

En Europa, a principios de los ochenta comenzó un movimiento intelectual que planteaba la regulación y el control del uso de la información personal dentro de la Unión Europea. Los trabajos encaminados a fundamentar el nuevo derecho de los ciudadanos sobre sus datos personales se iniciaron en el Convenio del Consejo de Europa de 29 de enero de 1981.

En lo referente al caso español, las nuevas propuestas para regular el sistema de información sobre las personas había nacido en la Convención de Schengen⁷, julio de

⁷ Convenio cuyos orígenes se remontan a julio de 1984 y del que en la actualidad forman parte los siguientes países : Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Holanda, Islandia, Italia, Luxemburgo, Noruega, Portugal y Suecia. Todos ellos en busca de determinados objetivos que el Acuerdo desarrollan y que consisten en: - La supresión de fronteras entre estos países. - La seguridad. - La inmigración. - La libre circulación de personas por el territorio de estos países.

1984. El 29 de octubre de 1992 se aprueba la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal (LORTAD). El objetivo de la nueva Ley consistía en regular el uso de la informática cuando estaban implicados datos personales. Asimismo, intentaba garantizar el derecho a la privacidad. Al regular solo el tratamiento automatizado, quedaban fuera de su ámbito los tratamientos documentales y audiovisuales, con los que los derechos fundamentales de los ciudadanos quedaban garantizados solo si el infractor había cometido la infracción con un ordenador o con un soporte informático. Si la infracción se cometía con un listado papel, se entendía que quedaba fuera de la cobertura legal porque la ley sólo regulaba el tratamiento informatizado.

Poco a poco se fueron dictando Leyes, Reales Decretos y Directivas que desarrollaron la Ley, como la aprobada el 24 de octubre de 1995 la Directiva europea, 95/46, reguladora del tratamiento de datos de carácter personal y a la libre circulación de los mismos; en la que ya no se distinguía el soporte de tratamiento y reconocía un nuevo derecho: el de oposición, con lo que la normativa española quedaba totalmente fuera de servicio. De esta forma, el 11 de junio de 1999, el gobierno español dictó el reglamento de seguridad de la LORTAD⁸. En lugar de actualizar nuestra legislación y adecuarla a la Directiva 46/95, se publicó la nueva Ley Orgánica de Protección de Datos (L.O. 15/1999), dejando vigentes los reglamentos que desarrollaban la antigua LORTAD, con lo que los ciudadanos se encontraron con que para dar cumplimiento a la nueva Ley que entró en vigor el 13 de enero de 2000 tenían que aplicar los reglamentos reguladores del tratamiento automatizado; tema que ha quedado pendiente.

Desde el 13 de enero de 2002 la protección de datos se ha convertido en materia de derecho constitucional, porque esta nueva Ley regula la garantía de los derechos fundamentales de los ciudadanos a la intimidad, privacidad, dignidad y propia imagen prescindiendo de soporte.

⁸ BOE de 31 de Octubre de 1992, nº 262. Tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.

A continuación, y según la Ley Orgánica 15/1999⁹, se define un vocabulario básico para el entendimiento de la Protección de Datos en España:

Se habla de datos de carácter personal cuando nos referimos a cualquier información concerniente a personas físicas identificadas o identificables. Al conjunto organizado de datos de carácter personal se le llama **fichero**, independientemente de la forma o modalidad de su creación, almacenamiento, organización y acceso. Los datos de carácter personal sufren **tratamientos**, es decir, se producen operaciones y procedimientos técnicos de carácter automatizado o no, los cuales permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Es obligatorio que se produzca un procedimiento de disociación, de modo que la información que se obtenga no pueda asociarse a personas identificadas o identificables.

Todo fichero debe ser sostenido por un **responsable**¹⁰, se le define como toda persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad y contenido del fichero, así como de su tratamiento. A parte del responsable del fichero, existe la figura del **encargado del tratamiento** de los datos; es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros trate de los datos personales por cuenta del responsable del tratamiento.

⁹ BOE, núm. 298, 14 de Diciembre de 1999.

¹⁰ Cuando los datos dejan de pertenecernos en exclusiva para formar parte de un fichero y realizar las funciones necesarias en las sociedades actuales trasladamos nuestra confianza respecto de ellos al responsable del fichero o tratamiento, quien adquiere la responsabilidad de trabajar con nuestros datos para nuestro beneficio y para el de la sociedad en general pero también asume la responsabilidad de tratarlos con cautela y conservarlos en buen estado. Frente a nosotros aparece además como el órgano ante quien dirigimos para continuar haciendo un seguimiento de nuestras informaciones personales y así poder hacer efectivo el control y el dominio sobre ellas. Por todo ello la ley sitúa al responsable del fichero en un importante lugar en el tratamiento de datos de carácter personal.

La persona física titular de los datos que sean objeto del tratamiento se le llama **afectado o interesado**¹¹.

Los ficheros pueden ser objeto de **cesiones** a terceros, es decir, revelaciones de datos realizados a una persona física distinta al interesado. Las cesiones de datos deben ser comunicadas y autorizadas por el afectado, siempre y cuando no lo exija alguna Ley.

Los ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación, se le denomina fuentes accesibles al público. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los diarios y boletines oficiales y los medios de comunicación.

¹¹ El afectado o interesado tiene derecho, de conformidad con el artículo 5 de la Ley, a ser informado de modo expreso, preciso e inequívoco, previamente a la recogida de datos, de los siguientes extremos:

- a) Existencia del fichero al que van a ser incorporados los datos, finalidad del mismo y destinatarios de los datos.
- b) Carácter voluntario u obligatorio de su respuesta a las preguntas que le planteen en relación con sus datos.
- c) Consecuencias de proporcionar los datos o de negarse a ello.
- d) Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e) Identidad y dirección del responsable del fichero o de su representante.

Principios sobre los datos personales

A continuación se comentan los diferentes principios relativos a los derechos del afectado. Nos encontramos con siete principios o derechos¹².

a) Información previa al interesado.

El primer principio a comentar es el relativo a la información previa al interesado, se convierte en el derecho básico del afectado para poder ejercitar, con ciertas garantías, los controles que la ley articula en los diversos momentos del tratamiento de datos.

Como ya se ha dicho es uno de los principios fundamentales de la LOPD por tanto se debe informar al interesado en el momento de la recogida de los datos, es decir, explicarle al usuario para que sean necesarios esos datos y lo que se va a hacer con ellos. De esta forma, siempre que se soliciten datos a los usuarios se debe informar claramente de:

- 1) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
- 2) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
- 3) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente.;

¹² Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

- 4) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
- 5) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Esta información deberá aparecer en los todos los formularios que se utilicen para recoger datos de carácter personal¹³.

b) Información posterior a la recogida de datos.

El segundo principio es el concerniente a la posterior información a la recogida de datos y sus excepciones. En éste apartado se tratan los datos que llegan al fichero sin ser proporcionados directamente por el afectado; cuando ocurre esta situación el perjudicado debe ser informado en los tres meses posteriores al registro de los datos por el responsable del tratamiento o de su representante, del contenido del tratamiento, de la procedencia de los datos, de la existencia de un fichero o tratamiento, de la finalidad del tratamiento, los destinatarios de los mismos, la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición de la identidad y domicilio del encargado de tratamiento o de su representante.

En este segundo principio existen una serie de excepciones:

- Cuando una ley expresamente lo prevea.
- Cuando el tratamiento tenga fines históricos, estadísticos o científicos.

¹³ A modo de ejemplo, éste podría ser un formulario tipo, teniendo en cuenta tanto las diferencias de los ficheros como sus contenidos: “*De acuerdo con la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, le informamos de que sus datos serán incorporados en un fichero automatizado con una finalidad exclusivamente administrativa. El interesado podrá dirigirse a la UCM, para ejercer su derecho de acceso, rectificación, cancelación y oposición. El fichero se encuentra en el sistema informático de la Universidad Complutense de Madrid*”.

- Cuando dicha información posterior al interesado resulte imposible o exija esfuerzos desproporcionados a juicio de la Agencia u organismos autonómicos, teniendo en cuenta el número de interesados, la antigüedad de los datos.
- Cuando los datos proceden de fuentes accesibles al público y se destinen a actividades de publicidad o prospección comercial, en cuyo caso se informará al interesado del origen de los datos y de la identidad del responsable del tratamiento, así como los derechos que le asisten.

c) Necesidad de consentimiento inequívoco del afectado.

Para incluir datos de carácter personal en un fichero es necesario el consentimiento de la persona de la que se recaban los datos. Este consentimiento debe ser específico para el tratamiento de datos e informado, que implica que previamente a la recogida de datos debe suministrarse al afectado la información a la que nos referimos en el apartado de “información previa al interesado”.

Por excepción, no será necesario consentimiento del afectado cuando los datos los recoja la Administración Pública en ejercicio de sus funciones, cuando se refieran a las partes en un contrato comercial, laboral o administrativo, cuando se trate de proteger un interés vital del interesado o cuando los datos se encuentren en fuentes accesibles al público y haya un interés legítimo del responsable del fichero o del destinatario de los datos.

La exigencia del consentimiento previo también sufre excepciones en el caso de cesión a terceros.

d) Derecho de oposición al tratamiento de datos.

Toda persona puede oponerse a facilitar datos de carácter personal siempre y cuando no sea obligatorio hacerlo, deben de existir motivos fundados y legítimos relativos a su situación personal. En tal caso el responsable del fichero excluirá del tratamiento los datos relativos al afectado. A éste principio se le denomina derecho de oposición al tratamiento de datos.

e) Derecho de acceso o comprobación por el interesado de forma periódica de lo que se mantiene en el fichero.

Los interesados en conocer sus datos pueden ejercitar su derecho, éstos deben, mediante petición o solicitud dirigida al responsable del fichero, desempeñar su derecho de acceso o comprobación de forma periódica de los datos que se mantienen en el fichero. Éste es uno de los principios mas importantes, ya que el afectado puede consultar no solo los datos personales del mismo sino también cuales son. A su vez, siempre que la configuración del fichero lo permita, podrá optar a uno o varios de los siguientes medios a la hora de acceder a sus datos:

- ❖ Visualización en pantalla.
- ❖ Escrito, copia o fotocopia remitida por correo.
- ❖ Fax.
- ❖ Cualquier otro procedimiento ofrecido por el responsable del fichero.

El responsable del fichero deberá resolver en el plazo de un mes, transcurrido el plazo sin contestación, ésta podrá entenderse como desestimada.

Si la resolución fuera estimatoria el acceso se hará efectivo en el plazo de diez días siguientes a la notificación de la misma.

La información que se facilite se hará en forma legible y debe comprender:

- ❖ Todos los datos del afectado, incluidos los resultantes de cualquier elaboración o proceso informático.
- ❖ El origen de los datos.
- ❖ Los cesionarios de los mismos.
- ❖ Las finalidades y usos para los que se almacenaron los datos.

En caso del que no se contengan datos del solicitante el responsable del fichero deberá comunicárselo igualmente.

Al igual que ocurre con los principios de rectificación y cancelación el responsable del fichero mediante el Real Decreto 1332/1994¹⁴ puede denegar el acceso cuando la solicitud sea formulada por personas distintas del afectado. Podrá no obstante ejercitar este derecho el representante legal del afectado, cuando se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

La segunda limitación a este derecho esta regulado en el artículo 15 de la Ley 15/1999, al establecer que el derecho de acceso solo podrán ser ejercitados intervalos no inferiores a 12 meses, salvo que el interesado acredite un interés legítimo efecto, en cuyo caso podrá ejercitarlo antes.

El Tribunal Constitucional en sentencia 30/11/2000¹⁵ ha eliminado la limitación al derecho de acceso contenida en el apartado 2 del artículo 15 al declararlo nulo.

Manuel Heredero Higuera¹⁶ enseña que incluso antes de que se promulgaran las primeras leyes sobre Protección de Datos, este derecho había sido bautizado como

¹⁴ Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

¹⁵ La LO 15/1999 dedica sus artículos 20 a 24 a los ficheros de titularidad pública. Digna de destacar es la declaración de inconstitucionalidad que el Tribunal Constitucional ha dictado recientemente STC de 30.11.2000, mediante la cual, el legislador ha rechazado por ser contrario a derecho parte de los artículos 21 y 24, donde se otorgaban claros privilegios a las Administraciones Públicas. Dicha Sentencia del Tribunal Constitucional ha declarado inconstitucional ambos extremos y ha significado un paso hacia delante en la ardua tarea de poner freno a las amplísimas prerrogativas de que goza la Administración.

hábeas data, por considerarlo una modalidad de acción exhibitoria análoga a la del hábeas corpus.

f) Derecho de rectificación y cancelación, derecho a la impugnación de las valoraciones efectuadas por los responsables de los ficheros.

Uno de los principios más importantes para el Responsable del fichero y para el encargado del tratamiento de los datos es el relativo a la rectificación y cancelación, con la finalidad de que los datos incorporados al fichero sean exactos y respondan con veracidad a la situación actual del afectado.

Aunque el legislador habla simultáneamente de rectificación y cancelación, entendemos con Miguel López-Muñiz Goñi¹⁷ que nos encontramos ante derechos distintos. Éste entiende que la rectificación procede en los casos de datos erróneos e inexactos, mientras que la cancelación tiene lugar cuando los datos sean excesivos con relación a la finalidad perseguida por el tratamiento así como en los supuestos de revocación del consentimiento.

El derecho de cancelación permite eliminar del archivo o base de datos aquellos datos personales que, por diversas circunstancias, no deben figurar en el mismo. Es importante poner de manifiesto que el término "cancelación" debe ser entendido en forma amplia como la acción tendiente a hacer irreconocibles los datos archivados, ya sea anulando, destruyendo, borrando, tornando ilegibles o declarando su nulidad. La metodología empleada diferirá de acuerdo a las circunstancias. Demás está decir que existen casos en los que, por cuestiones de interés público, será imposible eliminar

¹⁶ Véase, Heredero Higuera, Manuel, *“La Directiva comunitaria de protección de datos de carácter personal” Pamplona : Aranzadi, D.L. 1997, pag.96*

¹⁷ López-Muñiz Goñi, Miguel, *‘La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal’*, Informática y Derecho, núms. 6-7, 1994, p. 93-116.

- *El derecho de la persona en la Ley de protección de datos personales*, Jornadas sobre Abogacía e Informática, Ilustre Colegio de Abogados de Barcelona, Barcelona, 7 y 8 de mayo de 1993.

Completamente una información. Prueba de ello es la excepción a la destrucción física de los datos que la ley contempla en diversos artículos al referirse al mecanismo de bloqueo de datos.

La rectificación no supone el borrado o destrucción física de los datos sino únicamente la sustitución de unos datos inexactos o incompletos por otros, pero en modo alguno llevan consigo una desvirtualización de la finalidad perseguida por el tratamiento ni una revocación del consentimiento prestado. A diferencia de lo dispuesto en la LORTAD en que la cancelación llevaba parejo necesariamente la destrucción física de los datos, y subsidiariamente el bloqueo, la nueva normativa establece que dicha destrucción tendrá lugar únicamente transcurrido el plazo establecido para la prescripción de las responsabilidades derivadas del tratamiento.

Los derechos de rectificación y cancelación se harán efectivos en el plazo de cinco días siguientes a la recepción de la solicitud de rectificación o cancelación acompañada de los documentos justificativos. Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud ésta podrá entenderse desestimada.

A parte de los conocidos derechos que confiere en relación con dichos ficheros, los anteriormente tratados, (acceso, rectificación o cancelación y el de oposición al tratamiento de los datos), la Ley Orgánica de Protección de Datos establece el derecho a la impugnación de valoraciones o decisiones *"cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad"*¹⁸. Este derecho, que tan poco ejerce el requerimiento de *único* es difícil de apreciar en la práctica, permite realizar la autodeterminación informativa en su plenitud, ya que, tan importante como conocer quién tiene nuestros datos, qué datos se gestionan o lo que se ha hecho con ellos, es poder intervenir en las decisiones que se tomen basándose en dicho tratamiento.

¹⁸ Art. 13 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

g) Derecho de indemnización de los daños y perjuicios que puedan ocasionarse por el uso indebido de la información.

Es el último principio a comentar, es el derecho a ser indemnizados como consecuencia del incumplimiento de lo dispuesto en la Ley por el responsable o encargado del tratamiento siempre que sufran un daño o lesión en sus bienes o derechos. Si el fichero es de titularidad pública, dicha indemnización se resolverá ante la jurisdicción administrativa, si por el contrario se trata de ficheros de titularidad privada la jurisdicción competente es la ordinaria.

Como consecuencia de cualquier procedimiento sancionador, la Agencia no tiene competencia para fijar la indemnización de los posibles daños y perjuicios, debiéndose plantear su reclamación tal y como se establece en el artículo 19 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal¹⁹

¹⁹ *Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria."*

Principios sobre los ficheros que contienen datos personales.

Al conjunto organizado de datos de carácter personal se le llama fichero, independientemente de la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tenemos seis principios²⁰ para analizar:

- Pertinencia
- Legalidad
- Finalidad.
- Caducidad.
- Exactitud.
- Principio de seguridad

a) Principio de pertinencia

De los seis principios a analizar, el referente a pertinencia es de los más importantes, coincidiendo con Carlos Lema Devesa²¹, considero que el primer principio que ha inspirado la Ley es el principio de pertinencia de los datos. También conocido como principio de proporcionalidad y calidad de los datos, este principio exige que los datos que se recaben y almacenen en una base de datos sean pertinentes y adecuados, es decir, que estén relacionados con el fin perseguido en el momento de creación de la base de datos.

Esto significa que la recolección y el tratamiento de los datos han de ser proporcionales con respecto a los fines que se persiguen, sin que en ningún caso se puedan utilizar los datos obtenidos para finalidades distintas de aquéllas para las que se

²⁰ Adoptados por la Asamblea General en su resolución 45/95, de 14 de diciembre de 1990.

²¹ Lema Devesa, Carlos, “*Protección de Datos y Publicidad*”, Ponencia presentada en la XX Conferencia Internacional de Autoridades de Protección de Datos. Santiago de Compostela, España, 16-18 de Septiembre de 1998.

hubieran recogido. Por tanto los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y finalidad para los que se hubieren obtenido.

El principio de pertinencia, por tanto, delimita las circunstancias personales sobre las que pueden indagar y recabar información quienes mantengan bases de datos que incluyan información personal.

De tal forma, como enseña Javier Aparicio Salom ²² este principio supone no obstante la posible autorización del titular de los datos o la habilitación legal para someter la información a tratamiento, no se permite que puedan incluirse más datos que aquellos que sirvan o puedan servir para la consecución de la finalidad que justifica dicho tratamiento, que debió determinarse en el momento de la obtención del consentimiento, o que sirve para presumir la concurrencia de éste en los supuestos en que se establecen presunciones legales de su otorgamiento.

b) Principio de legalidad.

A la hora de captar datos el principio de legalidad tiene suma importancia y se encuentra ligado al principio de necesidad de consentimiento inequívoco del afectado pudiéndose apreciar en la Ley 15/1999²³. El Título VII dedica sus artículos a tratar a los responsables, los tipos de infracciones, los tipos de sanciones, relacionados con la legalidad o no de la captación de datos. A modo de ejemplo, pueden mencionarse como métodos fraudulentos, ilegales o desleales de recolección de datos a las investigaciones privadas realizadas por detectives, el uso de instrumentos de grabación o escucha de conversaciones privadas, la violación de correspondencia o papeles privados, o cualquier otro en el que se oculte la verdadera finalidad de la recogida de datos y posterior tratamiento. Lo que pretende la ley es evitar actuaciones delictivas por intermedio de las cuales pueda vulnerarse el bien jurídico protegido.

²² Salom, Javier Aparicio, (*"Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal"*, Editorial Aranzadi. Pamplona, España, 2000, pág.95

²³ Artículo 4, párrafo 7. "Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos"

c) Principio de finalidad

Los datos de carácter personal que se recaudan o se obtienen para la creación de un fichero deben poseer un objetivo específico conocido antes de la creación del fichero. Por tanto deben responder al llamado principio de finalidad.

Los datos personales solo serán guardados en ficheros informatizados para unos fines concretos y legítimos. Por tanto el criterio general es que los datos van a ser tratados y difundidos en y desde el fichero para el cual han sido captados y autorizados, y sobre el que el interesado a prestado su consentimiento, y a recibido la información previa. Por ello se prohíbe la cesión de datos para que sean tratados, incorporados a otros ficheros o difundidos por diferentes medios para los que fueron captados.

Una vez conocida la finalidad del fichero, tenemos que tener en cuenta que los datos recogidos serán los pertinentes y no excesivos y cumplirán por tanto éste principio.

Los datos no podrán ser utilizados para finalidades incompatibles con aquellas para las que fueron solicitadas, “no considerándose incompatibles el tratamiento posterior con fines históricos, estadísticos o científicos”.

d) principio de caducidad

Una vez cumplido el objetivo del fichero, los datos de carácter personal contenidos en el mismo deben ser cancelados ya que han dejado de ser necesarios o pertinentes para el fin por el que fueron registrados. A éste propósito se le llama principio de caducidad. “No serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido registrados”. La Ley remite a un Reglamento posterior el desarrollo de los supuestos en que excepcionalmente y de acuerdo con lo dispuesto en su legislación específica, se decida su conservación atendiendo a los históricos, científicos o estadísticos.

e) principio de exactitud

Tanto los principios relativos a los derechos de los afectados, como los relativos a los ficheros, se encuentran ligados por objetivos comunes. Los datos de carácter personal deben ser exactos y puestos al día siempre y cuando sean necesarios y por el contrario, los datos totales o parcialmente inexactos, o que sean incompletos deben ser suprimidos y sustituidos o en su caso completados.

El responsable del fichero aplicará el principio de exactitud cuando tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

Los titulares de ficheros deben poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar su puesta al día. Este principio alcanza también a los supuestos de cesión. En estos casos el cedente debe notificar la rectificación o cancelación al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

Parece lógica la necesidad que los datos que se obtengan y se sometan a procesamiento sean exactos y estén actualizados. Cuando la información la aporte el titular de los datos se entiende que será completa y actualizada. Pero si los datos se obtienen por otros medios puede ocurrir que la información no se encuentre actualizada, no se corresponda con la realidad o sea errónea, circunstancias que menoscabarán el legítimo interés de su titular. Por ello, el cumplimiento de la exigencia de que los datos sean exactos y actualizados recae sobre los responsables de los archivos o bancos de datos, siendo ellos los obligados por la ley a cumplir con el principio de exactitud. En definitiva, lo que pretende este principio es que los datos respondan con veracidad a la situación real de su titular.

f) principio de seguridad

Para finalizar es de útil importancia, garantizar la conservación de los datos y la no revelación de los mismos, salvaguardando la confidencialidad de los semejantes. Este objetivo recibe el nombre de principio de seguridad.

Debemos tener en cuenta lo dispuesto en el Real Decreto 994/1999 de 11 de junio²⁴ por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Las medidas de seguridad exigibles se clasifican en tres niveles²⁵ estableciéndose que todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad de nivel básico, los que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito o ficheros del artículo 4.4 del Reglamento (aquellos que permitan obtener una evaluación o definición de la personalidad del individuo deberán reunir las del nivel medio). Por su parte los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán adoptar las de nivel alto.

Conviene tener en cuenta que cada uno de estos tres niveles actúa como base de partida, que deben respetarse, al ascender a un nivel superior, sin perjuicio de lo dispuesto en las disposiciones legales o reglamentarias vigentes.

La Ley Orgánica 15/1999 establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o en su caso con el responsable del fichero.

²⁴ Véase el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. (B.O.E. 151/1999, publicado el 25/06/1999)

²⁵ Véase en el artículo 3 del Real Decreto 994/1999, de 11 de junio.

Datos especialmente protegidos

El artículo 7 de la LOPD hace hincapié en esta tipología de datos, al hablar de ésta categoría de datos estamos aplicando los datos sensibles, ya que se atribuyen y se aplican normas muy estrictas al tratamiento de datos sensibles: los referentes al origen racial o étnico, ideología, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual. Como norma, estos datos no podrán tratarse. Se tolerarán excepciones en circunstancias muy concretas. Entre éstas, el tratamiento de datos con el consentimiento explícito del interesado, el tratamiento obligatorio de datos debido a la normativa laboral, en casos en los que el interesado no pueda dar su consentimiento (por ejemplo, análisis de sangre de la víctima de un accidente de circulación), tratamiento de datos anunciados públicamente o el tratamiento de datos sobre afiliados por parte de sindicatos, partidos políticos o iglesias. Los Estados miembros podrán disponer excepciones adicionales para determinados casos como, por ejemplo, la protección de intereses públicos vitales.

A continuación se citan las especialidades de datos especialmente protegidos mas relevantes:

- Prohibición de la creación y existencia de ficheros con finalidad exclusiva de almacenar datos relativos a los extremos anteriormente expuestos.
- Los datos relativos a ideologías, creencias, o religión requerirán el consentimiento expreso y por escrito del afectado, con la advertencia de su derecho a no prestarlo. Se exceptúa los ficheros mantenidos por partidos políticos, sindicatos, confesiones religiosas, asociaciones y otras entidades sin ánimo de lucro en cuanto a los datos relativos de sus asociados. En todo caso la cesión requerirá el previo consentimiento del afectado.
- Los datos relativos al origen racial, a la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando por razones de interés general así lo disponga una ley, o el afectado lo consienta expresamente.

- Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas solo podrán ser incluidos en los ficheros de las administraciones públicas competentes en los supuestos previos en sus normas reguladoras.
- No obstante, todos estos datos considerados especialmente protegidos, podrán ser objeto de tratamiento cuando resulte necesario para la prevención o para la prestación de asistencia sanitaria o tratamientos médicos, siempre que dicho tratamiento sea necesario para salvaguardar el interés vital del afectado, y que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

En relación al nivel de seguridad de los datos especialmente protegidos²⁶, el nivel de debe de ser alto, el máximo nivel de protección de los ficheros ha de tenerse presente cuando se tratan datos referentes a ideología, religión, creencias, afiliación sindical, origen racial o étnico, vida sexual y salud.

Todas las medidas de seguridad deben de constar por escrito en el denominado "documento de seguridad" de la empresa, tal y como se recogen el artículo 8 del Reglamento de Seguridad. El documento de seguridad debe contener todas aquellas medidas de seguridad, tanto técnicas como organizativas, que la empresa debe adoptar para recabar y tratar los datos de carácter personal contenidos en sus ficheros automatizados.

El responsable del fichero será la persona que debe elaborar dicho documento e implantarlo en la empresa. Será de obligado cumplimiento este escrito para todos los trabajadores de la compañía. Del mismo modo, el documento de seguridad deberá estar actualizado en todo momento, incorporando aquellos cambios que se produzcan en las medidas de seguridad técnicas y organizativas referentes a los sistemas informáticos.

²⁶ Santiago Battaner. "Datos personales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº. 18, 2005"

Cesión de datos

Solo se podrán comunicar datos de carácter personal a un tercero cuando estén directamente relacionados con las funciones legítimas del cedente y del cesionario, y el previo consentimiento del afectado.

Existen una serie de excepciones a la hora de ceder²⁷ datos sin previo aviso del afectado:

- Cuando la cesión este autorizada por ley.
- Cuando los datos hayan sido recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a una relación jurídica cuyo desarrollo cumplimiento y control implique necesariamente conexión de dicho tratamiento con ficheros de terceros.
- Cuando el destinatario de la cesión sea el Defensor del Pueblo, Tribunal de Cuantías (u otros organismos autonómicos equivalentes), Ministerio Fiscal, Jueces o Tribunales en el ejercicio de las funciones que le son propias.
- Cuando la cesión se realice a las administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos, o científicos.
- Respecto a los datos de carácter personal relativos a la salud, cuando sea necesario para solucionar una urgencia o para realizar estudios epidemiológicos. Conviene tener en cuenta que respecto a estos datos las instituciones y centros sanitarios tanto públicos como privados así como los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de aquellas personas que a ellos acudan de acuerdo con la legislación de sanidad.

²⁷ Comentada en el artículo 11 de la LOPDP si bien bajo el título de “comunicación de datos”

El consentimiento del interesado será revocable, siendo nulo cuando no se le haya comunicado la finalidad a que se destinaran los datos que hayan sido objeto de cesión o el tipo de actividad a que se dedique el cesionario.

No tendrá la consideración de cesión de datos a un tercero, cuando el acceso a dichos datos por el tercero sea necesario para la prestación del servicio al responsable del tratamiento.

Cesión de datos entre las Administraciones Públicas²⁸ los datos recogidos o elaborados por las Administraciones Públicas para el desempeño de sus cometidos no serán comunicados a otras Administraciones para el ejercicio de competencias diferentes salvo cuando la comunicación tenga por objetivo el tratamiento posterior de datos con fines históricos, estadísticos o científicos.

Existe un derecho a conocer la cesión de datos. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario salvo que la cesión venga impuesta por ley o se trate de las excepciones explicadas anteriormente.

Uno de los últimos pasos de la cesión de datos es el deber de información al cesionario, concretamente se produce cuando el responsable o usuario de los ficheros que se procedan a rectificar, cancelar o suprimir información de carácter personal previamente cedida a terceros, debe notificar dicha rectificación o supresión al cesionario dentro de unos días hábiles.

²⁸ Artículo 21. Comunicación de datos entre Administraciones públicas.

Ficheros de titularidad pública y privada

La Ley Orgánica de Protección de Datos no delimita de forma expresa definiciones concretas en lo referente a estos dos tipos de ficheros, si bien el Capítulo I del Título IV viene a identificar los ficheros de identidad pública como aquellos cuya responsabilidad corresponde a la Administraciones Públicas, estableciendo ciertas especialidades en su régimen jurídico en las restantes disposiciones de este capítulo y en el artículo 46 en lo que se refiere régimen sancionador.

Como se desprende de las disposiciones de la LOPD, el criterio que ha de prevalecer en este punto es el de naturaleza pública o privada del responsable, ya que la Ley no diferencia entre ambas categorías de ficheros con base en criterios relacionados con la actividad llevada a cabo por el responsable, sino con el criterio de titularidad del fichero.

Diversos colegios profesionales han formulado consultas a la Agencia española de Protección de Datos solicitando su parecer a cerca de la naturaleza de los ficheros colegiales, en el sentido de considerarlos de titularidad pública o privada. Debe señalarse, como hemos explicado anteriormente, en los criterios que determinan la naturaleza jurídico-pública y jurídico-privada del responsable del fichero. Por tanto, se considera que la delimitación del régimen aplicable a los ficheros de titularidad pública o privada deberá fundarse de dos maneras: por una parte, el responsable del fichero deberá ser una Administración Pública y por otra sería necesario que el fichero sea creado como consecuencia del ejercicio de potestades públicas.

Un estudioso norteamericano, el profesor Henry H. Perritt Jr.²⁹ sostiene que los datos originados en el ámbito estatal, provincial o municipal son una importante parte de la salud general del estado, siendo incompleta la infraestructura nacional de información si no se facilita el acceso a los ciudadanos.

²⁹ Perritt Jr, Henry H., *Jurisdiction in Cyberspace: the Role of Intermediaries* in Fitzgerald, B. and Fitzgerald, A. (2002) *Cyberlaw: Cases and materials on the Internet, digital Intellectual property and electronic commerce*, Australia: LexisNexis Butterworths.

En los EE.UU. la Freedom Of Information Act (FOIA) garantiza a la ciudadanía el acceso electrónico a la información. Pero como muchas oficinas gubernamentales han firmado convenios con proveedores privados de información (en particular relacionados con la información legislativa y judicial) se plantea el problema entre el referido derecho y el de los proveedores privados.

Por tanto el artículo 25 de la LOPDP señala que podrán crearse ficheros de titularidad privada cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que la Ley establece para la protección de las personas.

En la Agencia de Protección de Datos existe un modelo³⁰ normalizado aprobado por ésta, el cual contiene 10 campos de obligado cumplimiento, desde los datos personales, hasta la finalidad del fichero o las cesiones a terceros.

Todos los cambios que se produzcan en los ficheros deberán ser comunicados a la APD. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En la Agencia Española de Protección de Datos nos encontramos con que ficheros inscritos en el Registro General de Protección de Datos a la fecha de actualización del WEB, clasificados según la titularidad de sus responsables: privada o pública.

Dentro de la clasificación de ficheros de titularidad pública, se encuentran aquellos cuyos responsables son:

- Administración Central (Administración General del Estado, Entidades y Organismos de la Seguridad Social, Organismos Autónomos y Entes Públicos del Estado).
- Administración, Entes y Organismos Públicos de las Comunidades Autónomas.
- Administración Local, Entes y Organismos Públicos de Entidades Locales.
- Otras Personas Jurídico Públicas.

En titularidad privada aparecerán aquellos ficheros cuyo responsable sea una persona privada física o jurídica.

³⁰ Resolución del 30 de mayo de 2000, BOE de 27 de junio, pag. 22649

Las Agencias de Protección de Datos

Tienen como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales.

A nivel estatal, nos encontramos con la Agencia Española de Protección de Datos³¹, cuyo objetivo principal es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

En cuanto a lo referente en la Comunidad Autónoma nos encontramos con la Agencia de Protección de Datos de la Comunidad de Madrid³², tiene como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales. Sus competencias versan sobre los ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, entes que integran la Administración Local de su ámbito territorial, Universidades públicas y Corporaciones de derecho público representativas de intereses económicos y profesionales de la misma. Las Agencias Autonómicas envían periódicamente relaciones de ficheros a la Agencia Estatal.

El artículo 37 de la Ley Orgánica de Protección de Datos relata las funciones de la Agencia Estatal, algunas de éstas competencias no pueden ser realizadas por las Agencias Autonómicas, como por ejemplo redactar una memoria anual y remitirla al Ministerio de Justicia, ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las

³¹ Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

³² Véase en el Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid.

funciones de cooperación internacional en materia de protección de datos personales y el velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se le reconocen sobre los mismos. Cada una de ellas pueda ejercer algunas de las funciones de la Agencia de Protección de Datos. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

SEGUNDA PARTE

Protección de datos en la Universidad Complutense de Madrid

- Introducción.
- Protección de datos en la Biblioteca de la Universidad Complutense de Madrid.
- Inserción de datos en el Fichero.
- Mantenimiento del fichero.
- Comparación de los ficheros de la biblioteca ucm con la Universidad Autónoma de Madrid
- Encuestas:
 - Personal de la BUC
 - usuarios
- conclusiones
- bibliografía

1. Introducción

Protección de datos en la Universidad Complutense de Madrid

En Junta de Gobierno celebrada en marzo de 2006, se aprueba la creación de la Unidad de Protección de Datos. El miércoles 12 de abril de 2006, se publica en el Boletín Oficial de la Comunidad de Madrid la relación de puestos de trabajo del personal funcionario de la Administración de la Universidad Complutense de Madrid, en ella se incluye la creación del “Jefe sección gestión y tratamiento de datos”. Por tanto a partir de ahora el departamento se creará, suprimirá y actualizará los ficheros, se agilizará la gestión, se informará a los estudiantes, a los profesores y trabajadores de la Universidad sobre la finalidad y los objetivos de todo este tema así como los derechos de cada uno.

Hasta ahora, todo lo referente a la Protección de Datos se tramita en los Servicios Informáticos ubicados en el Rectorado. no existía ningún departamento ni unidad dedicada exclusivamente a la Protección de Datos, concretamente el Director del Área Informática de Gestión es la persona que desde hace varios años actualiza, da ideas y tramita la Protección de Datos en la Complutense.

Hasta marzo de 2006, la Universidad Complutense de Madrid disponía de diecisiete ficheros registrados en la Agencia de Protección de Datos de la Comunidad de Madrid.

Estos ficheros son:

1. Usuarios de la biblioteca.
2. Doctorado.
3. Títulos Propios.
4. Becas y ayudas al estudio.
5. Matriculación de primer y segundo ciclo.
6. Admisión distrito compartido.

7. Admisión en el distrito único de Madrid
8. Personal docente.
9. P.A.S. régimen laboral.
10. P.A.S. En régimen administrativo
11. Nómina.
12. Seguridad social derechos pasivos.
13. Proveedores
14. Gaceta Complutense.
15. Retrib. Asis. Trib. Y comisión de servicios
16. Doctorado
17. COU y pruebas de acceso

A partir de la Junta de Gobierno celebrada en marzo de 2006, se produce la creación, modificación y supresión de ficheros de protección de datos de carácter personal.

Ficheros creados:

- Control horario.
- Registro de documentos.
- Devoluciones de enseñanza reglada.
- Usuarios de actividades deportivas
- Servicio de publicaciones.
- Ayudas de matricula de títulos propios.
- Servicio de medicina del trabajo.
- Odontológico general.
- Tarjeta universitaria de alumnos.
- Centro de orientación e información de empleo.
- Master en odontopediatría.
- Encuesta sobre docencia y profesorado de la facultad de ciencias físicas.
- Cursos de formación del PAS.
- Personas con discapacidad en UCM.

- Antiguos alumnos de la E.U. de Óptica.
- Encuesta docente de F. Matemáticas.
- Acceso a la red UCM.
- Campus virtual.

Modificaciones de ficheros:

- Personal docente.
- Personal de administración y servicio régimen administrativo.
- Personal de administración y servicios en régimen laboral.
- Nomina.
- Seguridad social y derechos pasivos.
- Proveedores.
- Gaceta Complutense.
- Retribuciones por asistencia a tribunales y comisiones de servicio.
- Investigación.
- COU y pruebas de acceso.
- Admisión en el distrito único de Madrid.
- Matriculación primer y segundo ciclo.
- Becas y ayudas al estudio.
- Doctorado.
- Fichero automatizado de títulos.
- Usuarios de la biblioteca.

Supresión de ficheros:

- Admisión en distrito compartido.

Todos los ficheros registrados en la Agencia de Protección de Datos de la Comunidad de Madrid a su vez están registrados en la Agencia Española de Protección de Datos, ya que las Agencias autonómicas envían periódicamente la relación de los ficheros creados, cancelados y sus modificaciones.

Conforme al artículo 6 del mencionado Decreto 99/2002, de 13 de julio, las disposiciones de carácter general de creación de ficheros, deberán indicar en todo caso, para cada uno de ellos, los siguientes apartados:

1. El órgano, ente o autoridad administrativa responsable del fichero.
2. El órgano, servicio o unidad ante el que se deberán ejercitar los derechos de acceso, rectificación, cancelación y oposición (este apartado se cumplimentará sólo en el caso de que sea diferente al responsable del fichero).
3. El nombre y la descripción del fichero que se crea.
4. El carácter informatizado o manual estructurado del fichero.
5. El sistema de información al que pertenezca el fichero (si se trata de un fichero informatizado).
6. Las medidas de seguridad que se apliquen. Si el fichero es informatizado habrá que indicar si las medidas de seguridad son de nivel básico, medio o alto.
7. Los tipos de datos de carácter personal que se incluirán en el mismo.
8. La descripción detallada de la finalidad del fichero y los usos previstos del mismo.
9. Las personas o colectivos sobre los que se pretenda obtener datos o que resulten obligados a suministrarlos.
10. La procedencia o el procedimiento de recogida de los datos.
11. Los órganos y entidades destinatarios de las cesiones previstas, indicando de forma expresa las que constituyan transferencias internacionales.

Para cada uno de los ficheros que se modifiquen, el proyecto de disposición de carácter general deberá contener principalmente:

1. El nombre del fichero que se modifica y el número de registro con el que figura inscrito en el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid.
2. El apartado de la inscripción que se modifica, sea uno o varios de los once que se recogen en la disposición de carácter general de los ficheros.
3. El contenido íntegro de cada uno de los apartados que se modifiquen.

Para cada uno de los ficheros que se supriman, el proyecto de disposición de carácter general deberá contener:

1. El nombre del fichero que se suprime y el número de registro con el que figura inscrito en el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid.
2. El motivo por el que se suprime el fichero y el destino de los datos contenidos en el mismo.
3. Si se va a destruir el fichero, las previsiones que se adopten para su destrucción.

Parte de los ficheros registrados en la Agencia de Protección de Datos de la Comunidad de Madrid fueron registrados previamente en la Agencia Española de Protección de Datos, con sede en Jorge Juan número 6, debido a la inexistencia de la Agencia de la Comunidad de Madrid. Una vez creada esta agencia se traspasaron los ficheros de la Agencia Española.

2. Protección de Datos en la Biblioteca de la Universidad Complutense

Actualmente, a 15 de junio de 2005, la Biblioteca de la Universidad Complutense de Madrid posee un único fichero de datos de carácter personal, dicho fichero se encuentra registrado en la Agencia de Protección de Datos de la Comunidad de Madrid, el nombre del fichero es “Usuarios de la biblioteca”.

La ficha resumida³³ de éste fichero aportada por la Agencia es:

RESPONSABLE DEL FICHERO	OTRAS PERSONAS JURIDICO - PUBLICAS UNIVERSIDAD COMPLUTENSE DE MADRID
ÓRGANO DE ACCESO	CL ISAAC PERAL, S/N 28015 - MADRID
NOMBRE DEL FICHERO DESCRIPCIÓN	USUARIOS DE LA BIBLIOTECA TABLA DE LA BASE DE DATOS CON INFORMACION DE CARACTER IDENTIFICATIVO.
FINALIDAD	FUNCIONAMIENTO DEL SERVICIO DE PRESTAMO AUTOMATIZADO DE LA BIBLIOTECA: CONTROL DE USUARIOS Y CIRCULACION DE FONDOS BIBLIOGRAFICOS. USO: GESTION AUTOMATIZADA DEL SERVICIO DE PRESTAMO DE LA BIBLIOTECA.
DISPOSICIÓN	RESOLUCION DE 15/12/94 DE LA JUNTA DE GOBIERNO DE LA UNIV. COMPLUTENSE DE MADRID REGULADORA FICHEROS AUTOMATIZADOS CON DATOS PERSONALES
CÓDIGO	2013410583
TIPO	INFORMATIZADO

En dicha ficha podemos observar que el fichero se aprobó el quince de diciembre de mil novecientos noventa y cuatro por la Junta de Gobierno de la Universidad, es de tipo informatizado (actualmente todos los ficheros de la Complutense son de tipo informatizado), así mismo podemos ver que el responsable del

³³ Fichero de Datos de Carácter Personal ofrecido por la Agencia de Protección de Datos de la Comunidad de Madrid a través de su página de Internet (www.apdcm.es)

fichero es la propia Universidad, que el Órgano de acceso se encuentra en la calle Isaac Peral s/n (Servicios Centrales de la Biblioteca) y la finalidad de la creación del fichero.

En el modelo de notificación de ficheros creado por la Agencia de Protección de Datos de la Comunidad de Madrid nos encontramos que la hoja de solicitud realizada por la Universidad Complutense de Madrid para la creación del fichero de datos personales nos encontramos:

- La dirección a efectos de notificación se encuentra en la calle Isaac Peral s/n, concretamente en los Servicios Centrales de la Biblioteca.
- El responsable del fichero de la Biblioteca y del Archivo Histórico es la Universidad Complutense de Madrid con dirección en la Av. Séneca
- En los Servicios Centrales se pueden ejercitar los derechos de oposición, acceso, rectificación y cancelación.
- La Disposición general es publicada en el Boletín Oficial de la Comunidad de Madrid.
- El nombre exacto del Fichero o tratamiento es “Usuarios de la biblioteca” de carácter informatizado y la descripción del fichero anotada en la Agencia es que los datos son de carácter identificativos, académicos, profesionales y de detalles de empleo. La descripción general del sistema de información es la gestión centralizada de la biblioteca. La red empleada es de tipo Intranet.
- El encargado del tratamiento trata los datos personales por cuenta del responsable del fichero, concretamente es el Director de la Biblioteca y del Archivo Histórico.
- Las medidas de seguridad, son obligatorias en caso de que los ficheros sean informatizados, son de nivel básico.
- El tipo de datos contenidos en el fichero son de carácter identificativo, donde figuran el DNI/NIF, la dirección postal o electrónica, nombre y apellidos, teléfono; en cuanto a los datos académicos y profesionales el modelo de la Agencia tiene señalado la casilla “otros” e indicado Facultad a la que pertenece, demoras, como el área temática, el curso, la biblioteca a la que pertenece y los

préstamos actuales del usuario (no hay forma de acceder al historial de préstamo del alumno, ni el estudiante ni a través del fichero, ni del historial del estudiante (datos que si poseen los ficheros de primer y segundo ciclo)). En cuanto a los datos de detalles de empleo, igualmente se encuentra señalado la casilla “otros” indicando información del colectivo. El fichero carece de datos especialmente protegidos, como la ideología, creencias, religión, afiliación sindical, etc. Carece también de datos de características personales, de circunstancias sociales, de datos de detalles del empleo, datos de información comercial, datos económicos-financieros y de datos de transacciones.

- La finalidad y usos previstos del fichero son el control y gestión del préstamo de materiales bibliográficos y de otros materiales útiles para el estudio, investigación y docencia, uso de gestión automatizada del servicio de préstamo de la biblioteca y evaluación de la gestión de las colecciones. Encuadrado en la sección de educación y cultura, concretamente en “enseñanza superior”; otra tipificación correspondiente a la finalidad es la estadística y concretamente se encuentra señalada la casilla “función estadística pública” ; se excluyen finalidades como, sanidad, trabajo y bienestar social, seguridad pública y defensa, etc.
- Las personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos son los alumnos, docentes y Personal de la Administración y Servicios de la U.C.M., Antiguos Alumnos e investigadores.
- Sobre la procedencia de los datos, es el propio interesado o su representante legal el encargado de transmitirlos. El procedimiento de recogida se realiza a través de formularios o cupones y a través de la solicitud personal; el soporte utilizado para la obtención es papel y mediante vía oral.
- Las cesiones o comunicaciones de datos no están permitidas sin el consentimiento del afectado. Aun así no están previstas.
- Lo mismo ocurre con las transferencias internacionales de datos, no están previstas.

El último apartado del modelo está relacionado con la modificación del fichero y partir de las modificaciones aprobadas en la Junta de Gobierno de marzo de 2006 se encuentran señaladas las casillas relacionadas con la disposición de creación, modificación o supresión del fichero (concretamente éste fichero sólo se modifica), nombre y descripción del fichero o tratamiento de datos, las medidas de seguridad y la finalidad del fichero y usos previstos. Estos cuatro objetivos son los que se modificarán.

Creación del Fichero

Como he comentado anteriormente el fichero se crea en 1994, con el objetivo de preservar los datos personales de los usuarios de la biblioteca.

La formación de éste fichero se realiza principalmente de dos formas, una automatizada y otra manual. La forma automatizada se realiza mediante el volcado desde el soporte Meta, es un programa creado para la gestión de matrículas de Secretaría; éste soporte da forma a tres ficheros, “Matriculación de primer y segundo ciclo”, “Doctorado” y “Títulos propios”. Por tanto la mayor parte de los integrantes del fichero “Usuarios de la biblioteca” viene de la forma automatizada.

El volcado de datos de carácter personal se realiza aproximadamente cinco veces al año, no existe un periodo fijo temporal, normalmente se realiza después del periodo de matriculación, o sea junio y septiembre.

Aproximadamente hace cinco años se realizó un volcado desde el fichero “Personal Docente” al fichero “Usuarios de la Biblioteca”. Desde entonces, los nuevos profesores son incluidos en el fichero de una forma manual desde los mostradores de préstamo de las distintas bibliotecas.

Mediante la forma manual, desde la propia biblioteca (a partir del programa de préstamo Millennium), se realizan carnés nuevos, también se realizan las modificaciones y renovaciones de los existentes en el fichero, en los siguientes casos:

1. Alumnos de doctorado procedentes de otras Universidades que no hayan cursado 1º y 2º ciclo en la Complutense.
2. Estudiantes Erasmus y Séneca.
3. Estudiantes procedentes de programas de intercambio con universidades norteamericanas (Universidades Reunidas)
4. Alumnos de masteres de la Facultad
5. Colegiales que acrediten pertenecer a Colegios Mayores de Fundación directa U.C.M. concretamente son 6.
6. Alumnos de centros adscritos, actualmente hay doce, dependiendo del campo científico (humanidades, ciencias sociales, ciencias experimentales o ciencias de la salud), le corresponden sus respectivos centros dentro de la U.C.M.
7. Alumnos matriculados en el curso que imparte la UCM para el acceso a mayores de 25 años, se les hará el carne de la biblioteca. Se les deberá dar categoría 10, y el periodo de duración será por un año (renovable, en caso de que repitan). Estos alumnos deberán acreditar documentalmente que están realizando este curso, mediante un carne que les ha sido expedido por la UCM.
8. Becas de Colaboración y Apoyo a la Dirección.
9. Cualquier miembro de la comunidad universitaria (Institutos Universitarios de Investigación, Escuelas de especialización profesional, Colegios Mayores, Centros de la UCM en el extranjero, Centros de Asistencia a la Investigación, edificios del Rectorado y de los Servicios Centrales, Instalaciones Deportivas y otros centros como hospitales universitarios, centros de estudio y de investigación, editorial Complutense, Tribuna Complutense, etc.).

Las actualizaciones del fichero son principalmente llevadas a cabo por el personal de las bibliotecas ya que tienen acceso constantemente al fichero, tanto para introducir, modificar, como para borrar datos de los usuarios.

Cabe destacar que si se modifican datos de forma manual, al producirse volcados desde el soporte Meta, éstas modificaciones desaparecen y vuelven a aparecer los datos

anteriores; por tanto para realizar modificaciones se debe acudir a las secretarías de las diferentes Facultades.

Ante éstos hechos se deduce que el fichero “Usuarios de Biblioteca” es la fusión de los tres ficheros que forman el soporte Meta, “Matriculación de primer y segundo ciclo”, “Doctorado” y “Títulos propios” y todas las modificaciones realizadas en éstos tres ficheros repercuten en el fichero de la Biblioteca. Por tanto el fichero de la biblioteca carece de autonomía propia al depender en parte de los otros tres ficheros que además prevalecen sobre el de la biblioteca.

Como he comentado anteriormente, en los mostradores de préstamo se añaden y suprimen datos personales; en porcentajes, aproximadamente el 95% del volumen del fichero de la biblioteca viene del programa Meta y solamente el 5% o menos, de los usuarios son creados directamente en los mostradores de préstamo.

La cancelación de los datos del fichero de la biblioteca no se realiza de forma automática sino que se realiza cada varios años, dando opción a que usuarios no matriculados vuelvan a matricularse y puedan usar los servicios de las bibliotecas. Concretamente se realizó un expurgo hace 4 años.

Puntos de acceso al fichero “Usuarios de la biblioteca”

Es posible acceder al fichero desde tres ubicaciones diferentes, desde las bibliotecas y centros de documentación, desde las bibliotecas departamentales y desde los Servicios Centrales. El total de bibliotecas y centros de documentación suman treinta y cuatro y si contamos con los departamentos tenemos cincuenta y tres. Al no existir limitaciones, todo personal de la Biblioteca puede acceder al fichero, siempre que se entre en el programa Millennium módulo de Circulación. Si diferenciamos por contratos laborales tenemos que, pueden acceder al fichero tanto el personal de administración y servicios, contratados laborales fijos y temporales, becarios, administrativos y el personal contratado a través del INEM. Desde Servicios

Centrales no existen restricciones a la hora de entrar en el programa de Circulación cualquier trabajador o colaborador de la biblioteca tiene acceso al fichero.

Hay que tener en cuenta varias obligaciones y deberes, como el deber de guardar secreto³⁴. Esto puede llegar a ser un problema a la hora de limitar responsabilidades si se produjese una negligencia. Al no haber tales limitaciones todos tienen acceso a los ficheros tanto para poder modificarlos como para cancelarlos.

Existen bibliotecas universitarias y públicas que si tienen limitaciones, mediante contraseñas, para restringir el acceso a los ficheros.

Debido al volumen de muchas bibliotecas de la Universidad Complutense sería inviable la limitación de acceso a los ficheros ya que, se lentificaría el trabajo y se jerarquizaría al mismo tiempo. Sobre todo a la hora de problemas de personal, si se produjesen bajas por enfermedad, vacaciones, etc.

Existen cuatro perfiles de entrada al programa de Circulación Millennium, a continuación se ordenan de mayor a menor número de funciones a realizar:

1. Mantenimiento, llevado a cabo por una empresa estadounidense.
2. Administrador (exclusivamente desde los Servicios Centrales).
3. Jefe de sala (en cada biblioteca existe un jefe de sala y préstamo, éste puede realizar algunas funciones, mediante contraseñas, que no puede realizar el resto del personal de la biblioteca, tales funciones son, los avisos de retrasos de ejemplares, las reservas cursadas por los usuarios, estadísticas, etc).
4. Personal.

Los puntos de acceso al programa Millenium, están limitados a 864, dentro del programa hay diferentes módulos, el de circulación, el de catalogación, adquisiciones, publicaciones periódicas, cisne (catálogo de la Biblioteca), etc.

Simultáneamente solo puede haber abiertos trescientos registros de Millennium.

³⁴ El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. (Art. 10. L.O. 15/1999)

El módulo de Circulación, está fabricado por una empresa llamada “innovate interfaces inc”. (Al igual que el resto de los módulos) y el mantenimiento de todo lo concerniente al mismo lo realizan los mismos fabricantes a través de un contrato renovable.

Hasta ahora no se han producido notificaciones a terceros, cesiones, por parte de la empresa norteamericana encargada del mantenimiento de éste programa.

En los puntos donde se trate con los usuarios/cliente debe de existir una cláusula en la que se informe de la finalidad del fichero, el responsable del mismo así como los derechos que poseen los integrantes del fichero.

A mediados de junio de 2006, ésta cláusula todavía no está presente en los mostradores de las diferentes bibliotecas, pero los Servicios Centrales de la Biblioteca de la Universidad Complutense de Madrid se ha marcado el objetivo de difundirla en todos los puntos de atención al público.

La cláusula³⁵ presente en los mostradores de las bibliotecas es la siguiente:

“Según lo establecido en la L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los datos facilitados en este cuestionario van a ser incorporados al fichero informatizado “USUARIOS DE LA BIBLIOTECA”, cuya finalidad es el control de y gestión del préstamo de materiales bibliográficos y de otros materiales útiles para el estudio, la investigación y la docencia. La entrega de dichos datos es obligatoria por parte del interesado y la negativa a suministrarlos implica la no formalización de relación alguna entre las partes. El responsable del fichero será la Universidad Complutense de Madrid con domicilio en Av. Séneca nº2 Madrid 28040 y el interesado podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Dirección de la Biblioteca Complutense. C/ Isaac Peral s/n. Madrid. 28015.

³⁵ Tanto en los mostradores de préstamo como en aquellos lugares de la biblioteca donde se accede, rectifica y cancela datos de los registros de los usuarios de la biblioteca, hay y debería de haber una cláusula como la relatada.

Mantenimiento del fichero.

A través del programa de préstamo “Circulación Millenium” el personal de la biblioteca, tanto desde los mostradores de préstamo como desde los Servicios Centrales, ejecuta el mantenimiento del fichero “Usuarios de la Biblioteca”.

Como se ha explicado anteriormente, el fichero de la biblioteca de la Universidad Complutense está compuesto en su mayoría por registros volcados a través del fichero “Matriculación primer y segundo ciclo” y en menor medida a través del mostrador de préstamo por el personal de la biblioteca.

El registro de usuario se encuentra compuesto por muchas celdas que contienen información del usuario, varias de ellas se encuentran ocultas y son visibles si seleccionamos la pestaña “ver” o la pestaña “modificar” (la diferencia entre las dos pestañas no es otra que la posibilidad, pinchando la pestaña “modificar”, de rectificar los campos de longitud fija y los campos de longitud variable). A primera vista cuando seleccionamos a un usuario los datos visibles son los datos llamados de “longitud variable”, básicamente son los datos personales del usuario, si desplegamos la pestaña “ver” o “modificar” tenemos acceso a los campos de longitud fija. Estos, a su vez, están compuestos por campos que actualiza automáticamente el sistema y por otros que deben rellenarse en el momento de la creación del registro de usuario o en posteriores actualizaciones.

A la hora de crear un registro de usuario el programa de circulación Millenium nos muestra el siguiente asistente:

CADUCA	31-12-2005	PREST ACT	4	EJEM ACT A	3
CURSOS	-	BIBLIOTECA	280 Geografía e Ha.	EJEM ACT B	1
A TEMATICA	g BCA. GENERAL	UMENSAJE	- SIN MENSAJE	PERDIDO	0
ADSCRI UCM	0 Usuarios UCM	BLOQUEO	-	DEMERITOS	8
CATEGORIA	30 Personal no docente	AFIRMA DEV	3	PETIC ILL	0
TOT PREST	9	DEBE	EU 0,00	EJEM ACT C	0
TOT RENOV	6	BLOQ HASTA	- -	EJEM ACT D	0

NOMBRE PRIETO GUTIERREZ, JUAN JOSE
DIRECCION Calle Profesor Aranguren S/N.
 Facultad de Geografía e Historia. Biblioteca.
TLF 91 394 60 80
DPTO:ESTUD 15700
ID UNIV 51415141
 0531487910
COD BARRAS
PIN pxtUhs4XPkIM
E-MAIL juipriet@buc.ucm.es
 juipriet@buc.ucm.es
F. CREACION LIB. 5.DIC.95

A continuación se describen los campos modificables por el personal de la biblioteca, éstos se actualizan automáticamente con cada volcado de datos proveniente del fichero de secretaría.

La caducidad del carné viene reflejada a través de la celda llamada “CADUCA”, nos indica el periodo de vigencia del carné.

La situación académica del usuario viene reflejada por la celda “CURSO” en ella se puede observar si el usuario es de primer, segundo o tercer ciclo, si pertenece a la Asociación de Antiguos Alumnos o Amigos de la Complutense, si pertenece a algún convenio de universidades extranjeras, etc.

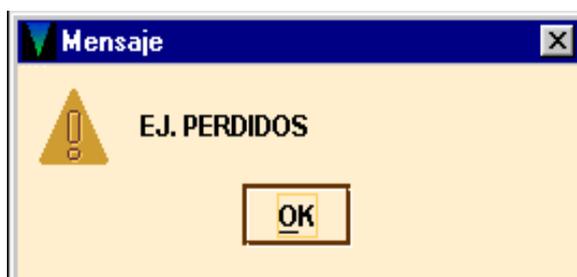
El área de conocimiento de la biblioteca viene dada por la celda “A. TEMATICA” en ella encontramos las diferentes áreas, como humanidades, ciencias médicas, ciencias, multidisciplinar, biblioteca general, etc.

Para conocer el centro al que pertenece el alumno nos introducimos en la celda “ADSCRI. UCM” en ella podemos ver la Universidad en la que cursa el usuario, bien sea la Universidad Complutense de Madrid, sus centros adscritos, las universidades públicas de la Comunidad de Madrid, la UNED, etc.

En la celda “CATEGORIA” se barema a los usuarios en función del vínculo a la Universidad, podemos encontrarnos a los estudiantes de primer y segundo ciclo definidos con la categoría 10, a los estudiantes de tercer ciclo (llamados investigadores) con la categoría 20, a los docentes con la 50, al personal de administración y servicios con la categoría 30, etc. Dependiendo de la categoría que tenga el usuario, el límite de préstamos a domicilio varía así como la fecha de devolución de los mismos.

Otra celda variable es la celda de “BIBLIOTECA” en ella podemos observar la biblioteca a la que pertenece el usuario y mediante ésta información deducimos la Facultad en la que estudia.

En la casilla “UMENSAJE” nos encontramos códigos que corresponden a mensajes en relación con el usuario definidos por la biblioteca. Los mensajes codificados en este campo se despliegan en el momento de la recuperación del registro de usuario. Por ejemplo:



En la celda “BLOQUEO” nos encontramos códigos correspondientes a causas definidas por la biblioteca que suponen un bloqueo del carné del usuario. La descripción del código introducido en este campo se despliega al recuperar el registro de usuario. La diferencia fundamental con el contenido del campo UMENSAJE es que éste no le genera ningún bloqueo al usuario y el del campo BLOQUEO sí.

Éstas dos últimas celdas a penas tienen uso ya que la causa fundamental de bloqueo en los usuarios es producida por el retraso en las devoluciones de los ejemplares prestados, ésta fecha vendría reflejada en la celda “BLOQ HASTA”.

La casilla “UMENSAJE” ha sido utilizada recientemente en la mayoría de las bibliotecas, a modo de mensaje masivo, con el objeto de la petición del email. Gracias a éste mensaje el fichero “Usuarios de la Biblioteca” dispone del correo electrónico de los usuarios, el cual se destina exclusivamente para la función de mensajes si el usuario se retrasa en la devolución de un libro; de éste modo el percance es percibido de forma instantánea y no cuando se recibe una carta vía postal (suele demorarse varios días) y el consecuente ahorro económico ya que el correo electrónico tiene coste cero.

El siguiente bloque de campos modificables desde el mostrador de préstamo por el personal de la biblioteca son los llamados campos de longitud variable.

El sistema permite crear registros de usuario etc. a partir de las plantillas definidas previamente. Si se han creado e instalado en el servidor diferentes plantillas de registros de usuario, el programa da a elegir entre una de ellas, pero si para el tipo de registro en cuestión (de usuario, en este caso), sólo existe una plantilla, el programa la abre directamente a través del Asistente para crear nuevos registros, que nos presentará una serie de cuadros de diálogo que ayudarán en la creación de registros. Para cada uno de los campos que aparecen en la plantilla seleccionada el programa pedirá la introducción de un valor.

A la hora de crear un registro nos aparece por defecto los siguientes campos, relativos a datos personales, nombre, dirección postal, teléfono, el número del documento nacional de identidad o en su defecto el número de pasaporte y si se trata de estudiantes extranjeros el número o célula que posean como identificación, y el código de barras asignado al carné de usuario.

La única forma de acceder al registro de usuario es a través del código de barras del carné, del número de identificación (D.N.I. o pasaporte) precedido por la letra “u” y de los datos personales precedidos por la letra “n”. Por tanto a través de los campos de longitud variable se accede a los Registros de Usuario.

En éste apartado pueden aparecer mas campos, exclusivamente si los introduce el personal de las bibliotecas de forma manual, tales son:

- La segunda dirección, definido como “DIRECCION 2” y la tercera dirección como “DIRECCION 3”, un segundo teléfono como “TLF2”. Se tiene la opción de rellenar, aunque no se suele realizar, la fecha de caducidad del D.N.I. del usuario. Otro campo sin uso es el reflejado como “DPTO/ESTUD”, es el nombre del departamento al que pertenece el usuario, en caso de ser profesores o investigadores.

- Un campo con bastante uso es el de “MENSAJE” se hace constar cualquier información útil sobre el usuario. Este mensaje se presentará en pantalla cuando se recupere el registro de usuario. Otra celda de longitud variable con información sobre el usuario es transcrita como “NOTA” En este campo el sistema añade automáticamente información sobre los días de bloqueo, sobre los ejemplares que el usuario afirma devueltos, etc. El contenido de este campo no aparece como un mensaje en el momento de recuperar el usuario, pero sí se muestra en la descripción abreviada del registro de usuario y en el registro completo. El uso de la celda mensaje es mas informativo para el trabajador que el de la celda nota y por tanto se representa en la pantalla cuando se recupera un registro de usuario.

La biblioteca da la opción de crearse un número pin para acceder al registro de usuario a través de la página de Internet de la biblioteca y para acceder a diferentes servicios como publicaciones electrónicas, bases de datos, etc. Éste número pin viene reflejado en los campos de longitud variable y tiene que ser creado desde la página de la biblioteca a través de Internet por el propio usuario. El personal de la biblioteca no tiene acceso al número pin, ya que aparece en el programa de Circulación Millenium de forma encriptada. Si el usuario olvida el pin, el personal de la biblioteca tiene que borrar éste campo para que el usuario cree uno nuevo, si lo que se desea es modificarlo, el usuario a través del pin que tiene lo modifica.

Otro campo muy usado es el del correo electrónico, transcrito como “EMAIL”, el sistema da la opción de incluir un segundo correo electrónico a través de “EMAIL2”. Los avisos de retraso en la devolución de los libros irán a la dirección de correo electrónico primera y si por el contrario el usuario desea tener otra dirección para otro tipo de notificaciones se usará la dirección segunda.

Dentro de los campos de longitud fija tenemos también celdas que no se pueden modificar de forma manual y que viene actualizadas a través de los Servicios Centrales, tales celdas son el total de préstamos y renovaciones del usuario desde la creación del registro, éstas celdas vienen representadas como “TOT PREST” “TOT RENOV” respectivamente.

El préstamo actual del usuario viene representado como “PREST ACT”. En ésta celda exclusivamente podemos apreciar el número de ejemplares prestados para comprobar el título, signatura, ubicación, código de barras y vencimiento de los mismos, tenemos que acceder a la pestaña “ejemplares prestados”.

La celda “AFIRMA DEV” nos indica los ejemplares que el usuario tiene prestados y que afirma haberlos devuelto pero que en el sistema aparece como que no los ha devuelto.

Nos encontramos con una celda que indica la cantidad adeudada por el usuario como consecuencia de las distintas multas. Este campo siempre estará a cero porque la biblioteca no utiliza las multas económicas como método de sanción a los usuarios.

El programa tiene cuatro celdas que nos indican el número de préstamos englobados en las distintas categorías A, B, C y D. El contenido de este campo determina el límite de ejemplares prestados al usuario.

El número de puntos de demérito que se le han acumulado a un usuario con motivo de la devolución de ejemplares con retraso, viene definido en la celda “DEMERITO”. Este número deberá ser muy alto para llegar a bloquear el carné del usuario.

Hay una celda que representa el total de ejemplares perdidos por el usuario desde la creación del registro.

Una vez analizados las celdas del programa de circulación, se concluye que el personal de la biblioteca posee información que nada tiene que ver con el ámbito de las bibliotecas, como por ejemplo lo relativo a los estudios del usuario, independientemente de la Facultad a la que se pertenezca el usuario debería de ser atendido de igual modo, actualmente los desajustes en los datos de cada usuario solo son tratados en la biblioteca a la que pertenece (si un usuario perteneciente a una Facultad del campus de Moncloa

necesita obtener en préstamo un ejemplar en el campus de Somosaguas y existe alguna anomalía en su registro de usuario debe volver a su campus, ralentizando uno de los servicios básicos de las bibliotecas, el préstamo de libros).

Los datos personales, como el teléfono, la segunda dirección postal, etc. de los usuarios es información no necesaria para prestar o devolver un ejemplar, solo debería tener acceso el responsable de préstamo de cada biblioteca. El problema viene cuando en las bibliotecas se prestan ejemplares sin el perceptivo carné de la biblioteca, aceptando por parte del personal de la biblioteca el D.N.I. o simplemente los datos personales de palabra (sin tener que presentar por parte del usuario ninguna acreditación física).

El programa de circulación permite realizar desde los Servicios Centrales, a través del Administrador todo tipo de estadísticas, dependiendo de los parámetros que se introduzcan, como por ejemplo el número de préstamos por Facultades, por bibliotecas, por franjas horarias.

El fichero “Usuario de la Biblioteca” al crearse mayoritariamente a través del programa de matriculaciones de la Universidad impide que se mantengan las modificaciones realizadas por el personal de la biblioteca, dichas actualizaciones deberían comunicarse a las respectivas Secretarías de alumnos o al Vicerrectorado de alumnos y deberían de ser invariables cuando se producen volcados de datos.

Comparativa con la Universidad Autónoma de Madrid

La Universidad Autónoma de Madrid, posee varios ficheros sobre protección de datos personales al igual que la Universidad Complutense y el resto de universidades ya sean públicas o privadas.

La totalidad de los ficheros en la Autónoma son dirigidos desde los Servicios Informáticos.

La Biblioteca de la Universidad Autónoma solo tiene un fichero de Protección de Datos, creado el 17 de diciembre de 2004, cuyo nombre es "Biblioteca" y la descripción del mismo es la de conocer los datos de las personas que utilizan el préstamo de las bibliotecas de la UAM. Es un fichero informatizado y se encuentra registrado en la Agencia de Protección de Datos de la Comunidad de Madrid.

La ficha resumida³⁶ de éste fichero aportada por la Agencia es:

RESPONSABLE DEL FICHERO	OTRAS PERSONAS JURIDICO - PUBLICAS UNIVERSIDAD AUTONOMA DE MADRID SECRETARIA GENERAL
ÓRGANO DE ACCESO	SECRETARIA GENERAL CR COLMENAR , KM15 28049 - MADRID
NOMBRE DEL FICHERO DESCRIPCIÓN	BIBLIOTECA DATOS DE LAS PERSONAS QUE UTILIZAN EL PRESTAMO DE LAS BIBLIOTECAS DE LA UAM
FINALIDAD	GESTION DEL PRESTAMO BIBLIOTECARIO DE LA UAM
DISPOSICIÓN	RESOLUCIÓN DE 17 DE DICIEMBRE DE 2004 DEL CONSEJO DE GOBIERNO
CÓDIGO	2051110015
TIPO	INFORMATIZADO

Al igual que el fichero de la biblioteca de la Complutense, el fichero de la Universidad Autónoma se forman a partir de los datos volcados de un programa

³⁶ Fichero de Datos de Carácter Personal ofrecido por la Agencia de Protección de Datos de la Comunidad de Madrid a través de su página de Internet (www.apdcm.es)

utilizado en matriculación llamado Sigma, programa utilizado en la gestión de matriculación de los alumnos de primer, segundo y tercer ciclo. La Autónoma utiliza otras aplicaciones y ficheros para dar forma al fichero de la biblioteca, como por ejemplo, la aplicación de nóminas, fichero de profesores, de PAS, etc.

La cancelación de datos personales se realiza anualmente, se borran los registros del programa de préstamo de los usuarios que no utilizan la biblioteca.

La finalidad es ofrecer los servicios del sistema de gestión automatizada Unicorn: préstamo, renovaciones, reservas, solicitud de préstamo interbibliotecario, etc. El fichero constituye la base de datos de usuarios del sistema.

El fichero de la Biblioteca carece, al igual que en la Complutense de datos especialmente protegidos como religión, ideología, creencias, etc.

La estructura del fichero contiene:

- nº de usuario asignado en la aplicación de origen (en el caso de la matrícula es un número asignado por la aplicación y que figura en el carné universitario)
- Nombre y apellidos
- DNI o pasaporte
- Facultad, estudios y curso en el que está matriculado
- Domicilio habitual y durante el curso
- dirección de correo electrónico institucional (del dominio...@estudiante.uam.es) que es asignada de forma automática en el momento de la matrícula.

Cuando el usuario llega por primera vez al mostrador de préstamo se le indican los datos que figuran en su registro de usuario (sobre todo la dirección de correo electrónico ya que a través de ella se le enviarán los avisos de reserva disponible, vencimiento de préstamo, etc.)

El responsable del fichero no es la propia Universidad Autónoma de Madrid, sino el responsable es el director de Tecnologías de la Información. Ellos son los que proporcionan los ficheros de los usuarios que son cargados mediante un proceso automático en el sistema de gestión automatizada de biblioteca.

Tienen acceso a los datos del fichero todo el personal de las bibliotecas. La modificación de determinados datos se realiza mediante contraseñas.

Al igual que ocurre en la Biblioteca de la Complutense, el sistema de gestión de bibliotecas está configurado de forma tal que se otorgan distintos privilegios en función del colectivo al que se pertenece; por ejemplo los/as directores/as de bibliotecas o responsables de préstamo de cada centro pueden ejecutar una serie de acciones que no pueden realizar las personas que están en los mostradores de préstamo. Como se ha comentado antes, éste colectivo tiene el acceso limitado por contraseñas.

El acceso a los datos sólo puede ser desde los distintos puntos de servicio de la biblioteca (bibliotecas de centros y servicios centrales); los departamentos no pueden acceder a los mismos salvo que tengan una biblioteca departamental informatizada, independientemente de que el personal bibliotecario, perteneciente a los Servicios Centrales de la Biblioteca.

En los mostradores de préstamo no suelen solicitarse datos, excepto para aquellos usuarios para los que no se ha realizado descarga y a los que se da de alta en el sistema de biblioteca la primera vez que acuden al mostrador de préstamo con su carné universitario (alumnos que aún no han realizado la matrícula pero que están asistiendo a clases, caso de los Erasmus, profesores visitantes, etc.,) en cuyo caso se les solicitan los datos, pero no se les entrega ningún documento informativo, ni tienen que rellenar un formulario, etc.

Existe una nota informativa en todos aquellos formularios que el usuario ha de cumplimentar introduciendo sus datos desde el acceso Web al catálogo, como por

ejemplo en el formulario de solicitud de préstamo interbibliotecario, en cuyo caso figura al final el texto siguiente:

“Sus datos personales son tratados por la Universidad Autónoma de Madrid, en el fichero Biblioteca. El titular podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición solicitándolo por escrito en la Secretaría General de la Universidad Autónoma de Madrid, Edificio rectorado, 4ª planta, Campus de Cantoblanco. 28049 Madrid”.

Encuesta trabajadores/ estudiantes

Se han realizado varias encuestas a estudiantes y trabajadores de la biblioteca, todos ellos pertenecientes a la Universidad Complutense. Las encuestas están realizadas a partir de seis preguntas y sobre una muestra de cien para estudiantes y cincuenta para trabajadores. No ha habido distinciones en el caso de la muestra de los trabajadores, se ha encuestado a personal laboral, funcionarios de carrera, personal proveniente del INEM y becarios de diferentes bibliotecas.

Las preguntas formuladas son:

1. Conocimiento de la existencia del fichero de datos de carácter personal de la biblioteca.
2. Información, de los derechos básicos de Protección de Datos, por parte del personal de la biblioteca hacia los usuarios a la hora de solicitar datos personales y añadirlos en el fichero.
3. Finalidad de la petición de los datos.
4. Opinión sobre el tratamiento de los datos.
5. Existencia del secreto profesional, confidencialidad, etc.
6. Acceso al fichero por parte de todos los trabajadores de la biblioteca.

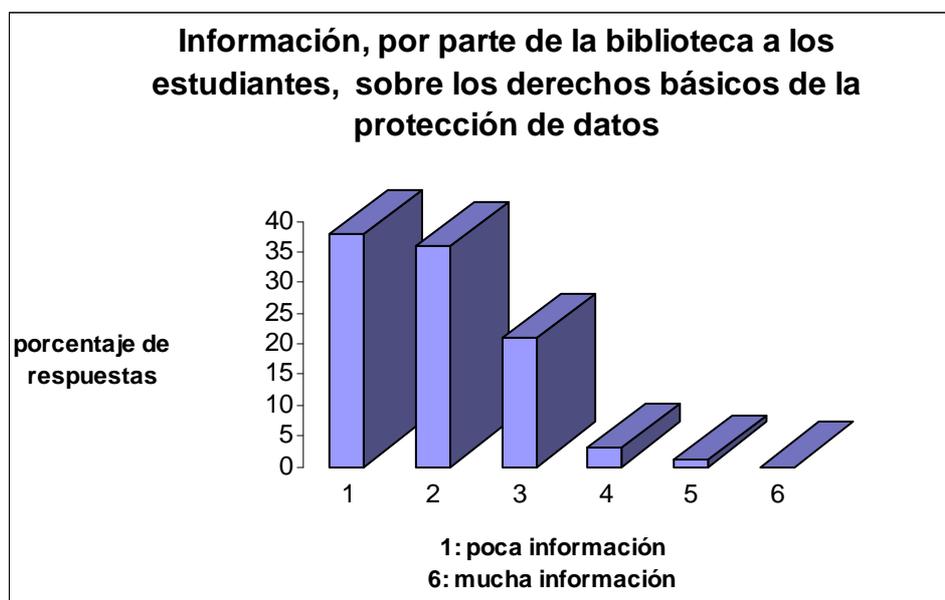
Las respuestas de las preguntas se encuentran graduadas de 1 a 6, siendo 1 poco, nada o desconocimiento y 6 mucho o conocimiento pleno. En el caso de la primera pregunta, la respuesta es si o no, por tanto no existe un baremo.

Encuesta a estudiantes

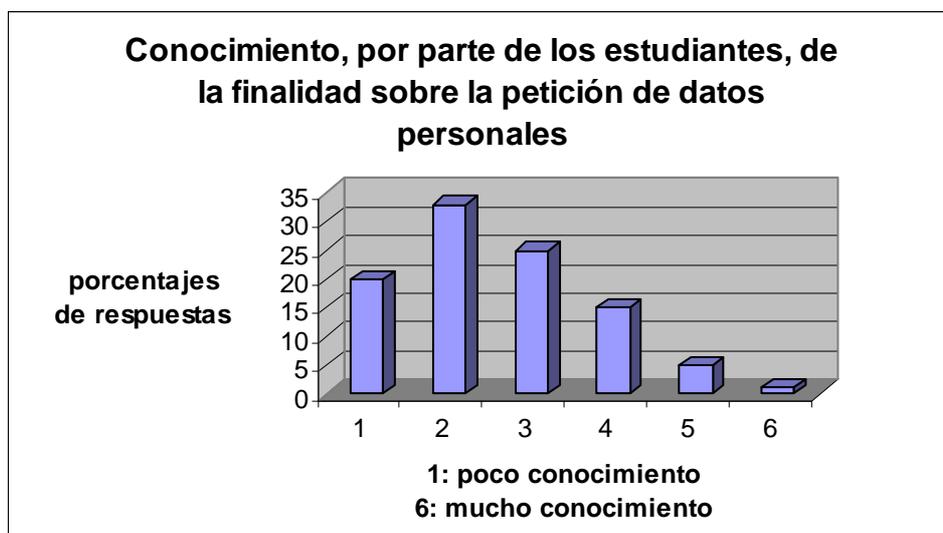
- En referencia a la primera pregunta dirigida a la comunidad estudiantil, de la Universidad Complutense de Madrid, el 32% afirma conocer la existencia de un fichero de datos en la biblioteca, dentro de éste grupo se ha introducido a los estudiantes que respondían que debería de haber un fichero pero que no conocían el nombre. Por tanto se incluyen a los que conocen el fichero y a los que tienen conocimientos en Protección de Datos y por tanto afirman de la existencia del fichero. Ninguno de ellos supo responder al nombre exacto del fichero. El 68% de los encuestados desconoce totalmente la existencia del fichero.



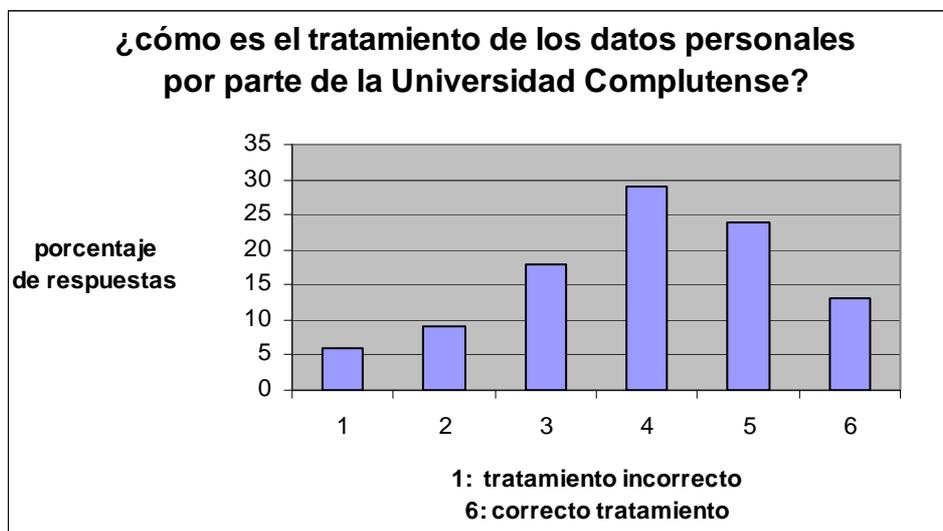
- En cuanto a la segunda pregunta, si el personal de la biblioteca informa de los derechos que tienen los usuarios sobre protección de datos hay una clara mayoría de estudiantes que afirma que no recibe información. Cerca del 80% de los encuestados respondió entre uno y dos, esto se transmite a la grafica concentrándose la mayor parte de la muestra cerca de la unidad. Algunos estudiantes afirman que existe información a cerca de la finalidad del fichero pero sobre los derechos muy poca. La mayor parte de los estudiantes desconoce que tienen derecho de acceso a sus datos personales, que pueden oponerse, el derecho a la rectificación, quien es el responsable del fichero, la dirección del mismo, etc.



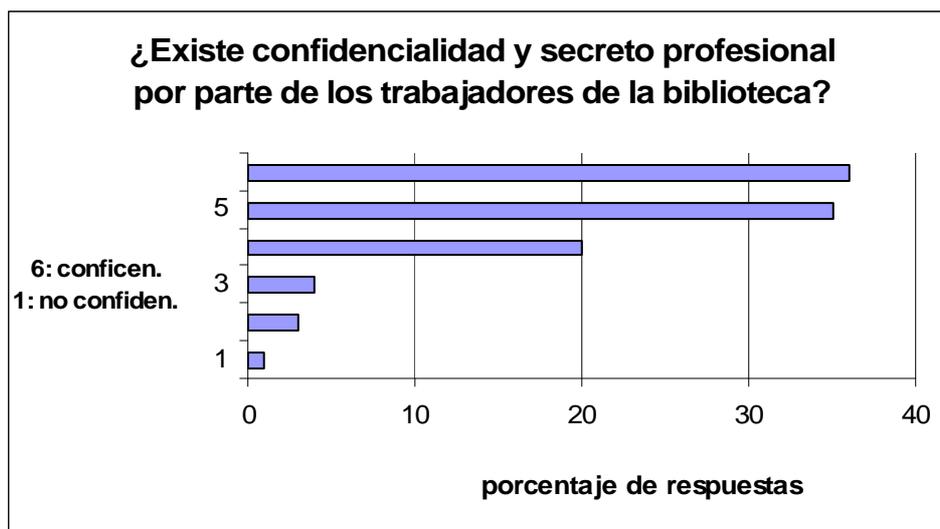
- Analizando la respuesta de la tercera pregunta, se puede comprobar como he comentado en el apartado anterior, que el porcentaje de estudiantes que conoce la finalidad de la petición de datos personales es mayor que el conocimiento de los derechos. Casi todos los estudiantes coincidían en que la petición de datos como el e-mail, la creación del PIN, etc, suponía una mejora en el servicio de la biblioteca. La concentración de respuestas se ha movido hacia el centro de la gráfica, concentrándose bastantes resultados de la estadística entre el dos, tres y cuatro.



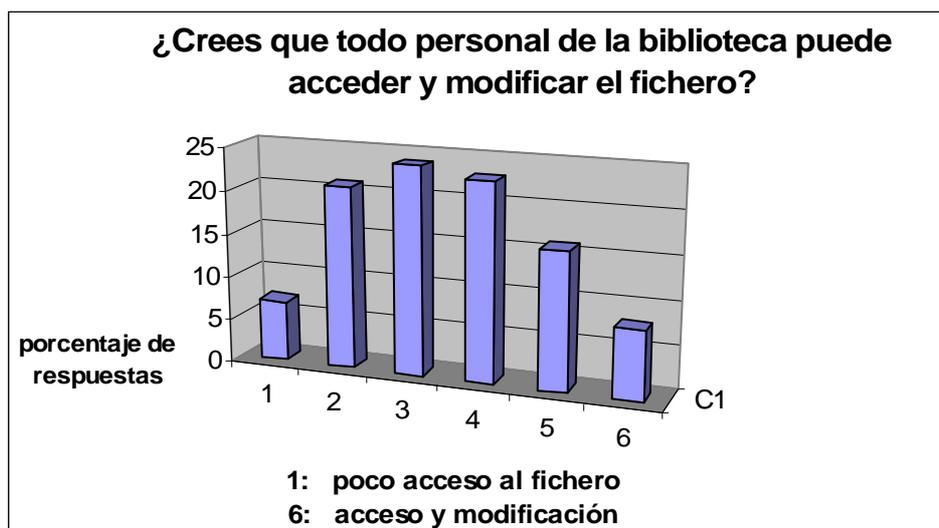
- Sobre el tratamiento de los datos personales por parte de la Universidad Complutense de Madrid, la inmensa mayoría de la muestra piensa que es correcto por parte de la Biblioteca y en particular por parte de la Complutense, ya que la mayor parte de los estudiantes no ha recibido informaciones extra universitarias ni han detectado movimientos de datos personales fuera del ámbito universitario. La cuarta pregunta está relacionada con la quinta, que trata sobre la cesión de datos, confidencialidad y secreto profesional. En la gráfica podemos ver como la mayor parte de las respuestas se concentran cerca del tres, cuatro y del cinco.



- La penúltima encuesta realizada a los estudiantes trata el secreto profesional, la confidencialidad y la cesión a terceros. El setenta por ciento de los estudiantes puntuaba la pregunta entre cuatro, cinco y seis, confiaban en la confidencialidad y ninguno de ellos había tenido repercusiones con sus datos personales ni había notado problemas de cesiones a terceros.



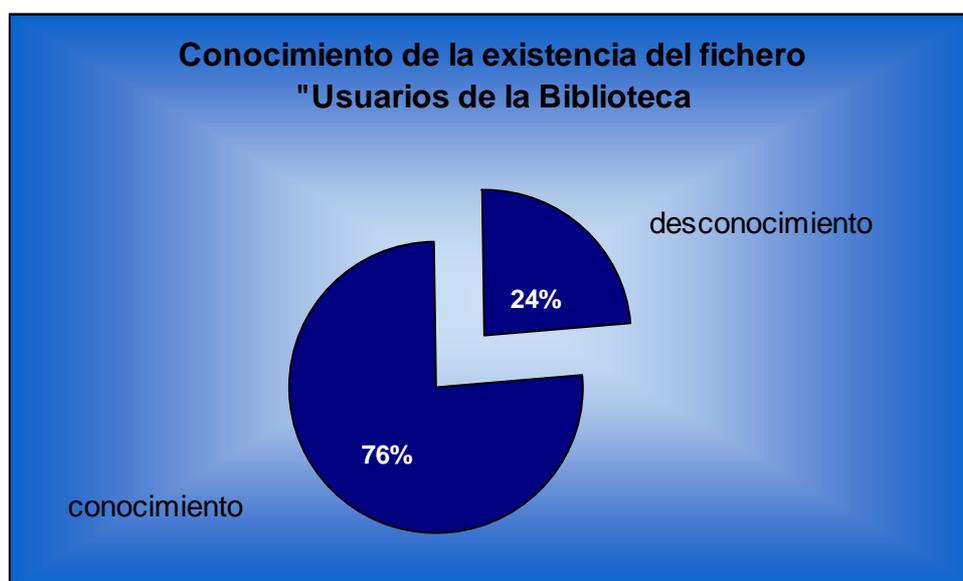
- La sexta y última pregunta realizada a la comunidad estudiantil es si creían que todo el personal de la biblioteca tenía acceso al fichero de datos personales. Un gran número de estudiantes respondió dos, tres y cuatro. Por las respuestas de los usuarios, éstos no conciben que todo el personal de la biblioteca tenga acceso a modificar el fichero de datos personales. Por el contrario un gran número de ellos comentó a modo de anécdota que en los mostradores de préstamo existía una rotación del personal y por tanto, todos los trabajadores trataban el programa de préstamo y accedían a la modificación y tratamiento de los datos. Aproximadamente un cinco por ciento de los estudiantes comentó sobre ésta última cuestión la imposibilidad, rotunda, de creer que todo el personal de la biblioteca accediese a los datos personales de los usuarios y sobre todo comentaron el tema de las modificaciones del fichero, creyendo que solo tenía acceso a la modificación el responsable de la biblioteca o alguna persona en concreto y con autoridad. Por contrapartida mucha gente que respondió a esta pregunta y, que usaba con frecuencia la biblioteca comentó que la modificación de los datos es preferible que la pueda realizar cualquier personal de la biblioteca reduciéndose así el tiempo de actualización del fichero.



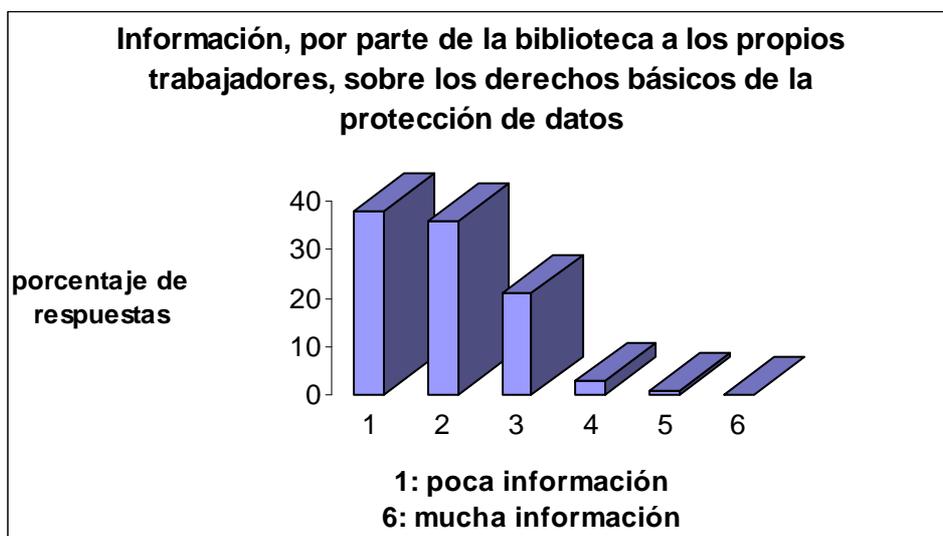
Encuestas trabajadores

La encuesta a los trabajadores se realizó sobre una muestra de cincuenta personas, el grupo de los trabajadores está compuesto por todos los colectivos, laborales, funcionarios, trabajadores provenientes del INEM y becarios.

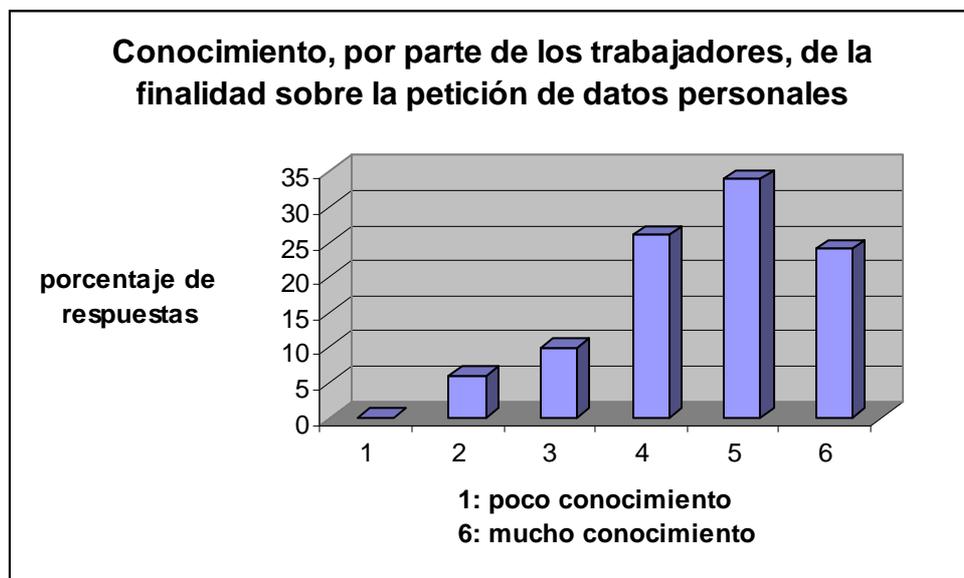
- La primera pregunta realizada a los trabajadores es a cerca del conocimiento o no del fichero de datos personales “usuarios de la biblioteca”, el 76% de los encuestados conocían la existencia del fichero, casi nadie conocía el nombre exacto del fichero, y solo un 24% desconocía la existencia del fichero y lo relacionado con el tema de la Protección de Datos.



- Las respuestas a la segunda pregunta, información por parte del personal de la biblioteca de los derechos que tienen los usuarios a cerca de la Protección de Datos, se centra en que un 80% de los trabajadores no ofrecen ninguna información sobre el tema de los derechos (fundamentalmente debido al desconocimiento) como veremos en el gráfico de la siguiente pregunta muchos de los trabajadores conocen la finalidad del fichero pero muy pocos informa a los usuarios sobre los derechos. La información se centra en los múltiples servicios que ofrece la biblioteca y sobre todo ahora, con las nuevas tecnologías.

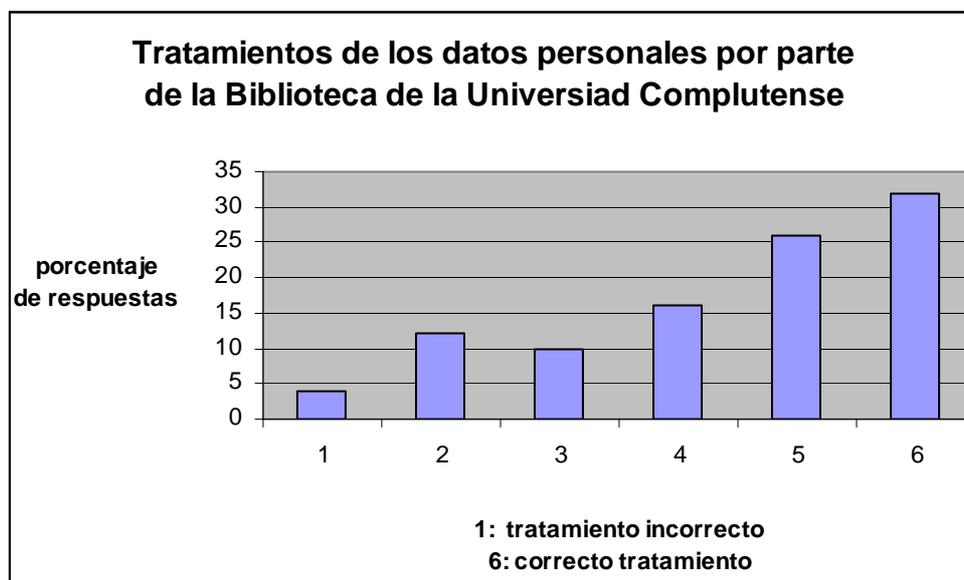


- Como se ha comentado anteriormente, la inmensa mayoría de los encuestados dice conocer la finalidad de la petición de datos personales dirigidos al fichero “Usuarios de la Biblioteca” dirigidos principalmente al ofrecimiento de los diferentes servicios de la biblioteca, como el préstamo, renovaciones y reservas. Al encontrarnos inmersos dentro de un sin fin de nuevas tecnologías, todos los servicios se encuentran informatizados y con la disposición de un pin podemos acceder a múltiples servicios de la biblioteca.
La finalidad sobre la petición de los datos es la de formar parte de un fichero protegido, al ser el fichero informatizado, el tratamiento de los datos es más factible y rápido.



- La siguiente pregunta formulada a los trabajadores de la biblioteca es, si creen que los datos de los usuarios se tratan correctamente, la mayor parte de contestaron que los datos se tratan correctamente.

Se tienen en cuenta las siguientes cuestiones, la calidad de los datos solicitados (tratados de manera leal y lícita), la legitimación del tratamiento, seguridad de los datos, acceso desde medios remotos como Internet, etc. El tratamiento de datos personales debe tener finalidades determinadas, explícitas y legítimas. Los datos que se pueden recoger y tratar han de ser adecuados, pertinentes y no excesivos en relación con la finalidad. Además, tienen que ser exactos y puestos al día por parte del responsable del fichero o del tratamiento.

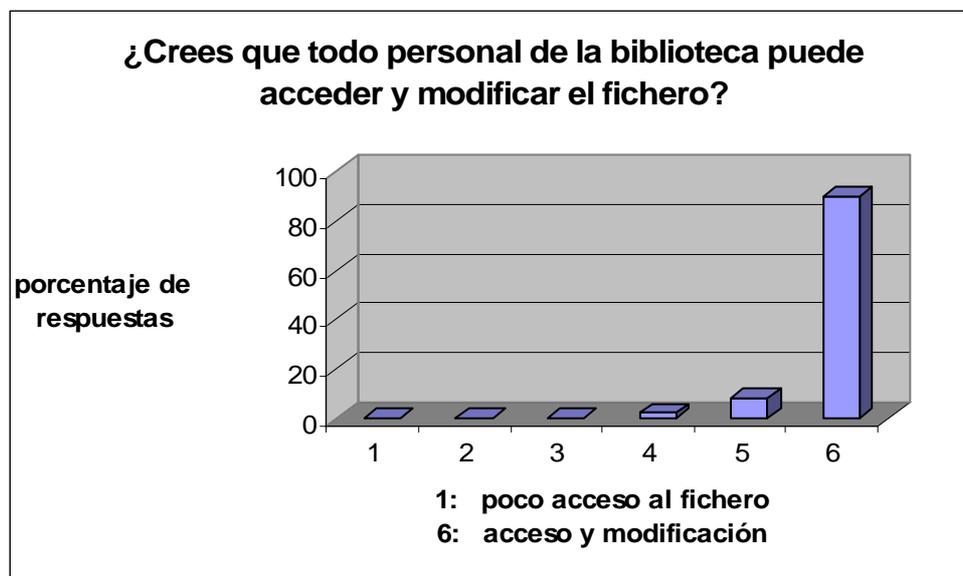


- Sobre el tema del secreto profesional y la confidencialidad por parte de los trabajadores de la biblioteca, aproximadamente el 95 por ciento de los encuestados afirmaban cumplir estos temas (se aprecia en el gráfico que la mayor parte de las respuestas se concentran entre 5 y 6 del baremo). Todo lo concerniente a estos temas son obligatorios dentro de la ley de Protección de Datos, los responsables del fichero y todos los participantes en el proceso de gestión de los datos personales están obligados al secreto profesional.



- La última pregunta de la encuesta es la limitación de acceso al fichero de la biblioteca por parte de los diferentes colectivos de la biblioteca. El 95% de los encuestados afirmaban que todo el personal de la biblioteca accede al fichero, que el personal que tiene acceso directo al fichero son los profesionales destinados de cara al público, a través del programa de préstamo, el resto podría tener acceso desde otro punto siempre que activasen el módulo de préstamo, o desplazándose al mostrador de préstamo. Como se comentó anteriormente, la Biblioteca de la Universidad Complutense no tiene perfiles a la hora de entrar en el módulo de préstamo (para tratar los datos de los usuarios). Este dato se ha visto contrastado con las opiniones de los diferentes encuestados.

Se puede ver la gráfica:



Conclusiones

- 1) Es necesario la creación de un Código de conducta sobre Protección de Datos. En este Código de Conducta se aportaría un gran conjunto de garantías adicionales para la protección de datos personales, como es la incorporación de una cláusula informativa en todos los formularios donde se recojan datos personales aunque no vayan a formar parte de ningún fichero. Es, por lo tanto, el código tipo que aporta mayores garantías. Actualmente la Universidad Complutense de Madrid posee algunos formularios pero faltan bastantes dependiendo del fichero.

- 2) Sería necesario la implantación de un decálogo de seguridad, que con la posesión de una única contraseña personal se pueda acceder a todos los servicios de la Universidad, actualmente se necesitan varias contraseñas (con diferentes configuraciones, porque para acceder a al registro del usuario en la biblioteca la contraseña tiene que tener de uno a treinta dígitos alfa-numéricos y por ejemplo para acceder a Metanet (es un Servicio de gestión académica en el que se pueden comprobar el expediente académico y la matrícula) tiene que tener cuatro dígitos. De igual modo sería conveniente una apuesta por la formación para que todos los miembros de la comunidad universitaria, especialmente los alumnos, conozcan el tratamiento de los ficheros de carácter personal, son algunas de las actuaciones que la Universidad podría adoptar.

- 3) La Universidad Complutense de Madrid ha mostrado siempre una especial sensibilidad por los temas relacionados con el soporte informática. Con la creación de la Unidad de Protección de Datos se consolida esta inquietud.

- 4) En las encuestas realizadas se ha comprobado que existe un gran desconocimiento en la materia por parte de los trabajadores de la Biblioteca. Muy pocos conocían el nombre exacto del fichero de Protección de Datos. Los principios relativos a los derechos del afectado no son empleados normalmente a la hora de crear, modificar o cancelar una parte de fichero. Por parte de los usuarios, se reduce mas aún el conocimiento de la Protección de Datos en la Biblioteca.

- 5) Los integrantes principales del fichero son los usuarios de la biblioteca, son los usuarios ligados a la Universidad Complutense de Madrid, y debemos evitar que se vean afectados o piensen que pueden llegar a serlo por un problema en la protección de datos.

- 6) Uno de los focos de actuación es el usuario, la persona, y a él debe orientarse fundamentalmente nuestra labor.

- 7) Los ficheros sobre Protección de Datos de la Complutense se encuentran registrados en la Agencia de Protección de Datos de la Comunidad de Madrid, dicha Agencia realiza sesiones informativas dirigidas al ámbito de las Universidades tanto las públicas como las privadas. Éstas sesiones son formativas y están dirigidas a toda clase de usuarios.

- 8) Uno de los problemas que se aprecia al fichero de la biblioteca, es el procedimiento de creación del fichero. Al depender directamente de los ficheros de primer, segundo y tercer ciclo, al producirse volcados de información, éstos sustituyen los datos modificados manualmente por el personal de la biblioteca. Por ejemplo, si algún trabajador de la biblioteca

decide matricularse en algún curso al volcarse los datos se le cambia la condición de préstamo, la dirección, el teléfono, etc. Lo mismo ocurre con los profesores que se encuentran matriculados en algún programa, o con los discapacitados que se les modifica la condición de préstamo.

- 9) Promover encuentros entre las distintas Agencias o Unidades de Protección de Datos de las Universidades de la Comunidad de Madrid y una vez que estén afianzadas procurar los encuentros a escala nacional, para fomentar el intercambio de conocimiento y experiencias.

- 10) Durante el proceso de investigación se ha podido comprobar un creciente interés por parte del gremio de la archivística, de la documentación y de los trabajadores de las bibliotecas en lo referente a la Protección de Datos de carácter personal. Las ponencias en foros, los artículos de revistas, son mas frecuentes y de mayor calidad.
Debido a problemas legales referidos a la Protección de Datos, ha ido en aumento la preocupación por el mismo. De hecho, se aprobó una Ley que lo regula en 1999.

- 11) Se debería promover una mayor colaboración con sector privado.
Favorecer el funcionamiento de expertos u oficiales de protección de datos.
Se debería incentivar la autorregulación de los propios agentes interesados, por ejemplo a través de códigos de conducta.

Bibliografía

- Pagina de Internet de la Universidad Complutense de Madrid. www.ucm.es
- Intranet de la Biblioteca de la Universidad Complutense.
- Agencia de Protección de Datos de la Comunidad de Madrid. www.apdcm.es
- Agencia española de Protección de Datos. www.agpd.es
- Revista digital de la Agencia de Protección de Datos de la Comunidad de Madrid. www.datospersonales.org
- Página de Internet de la Universidad Autónoma de Madrid. www.uam.es
- Romeo Casabona, Carlos M., “*La protección de datos personales: El tratamiento de datos de carácter*”. En: Telos : Cuadernos de Comunicación, Tecnología y Sociedad, 1994 MAR-MAY; (37).
- Terré Rull, C., “*El secreto profesional y la protección de datos de carácter personal*”. En: Matronas Profesión, 2002; 9
- Troncoso Reigada, Antonio, “Agencia de Protección de Datos de la Comunidad de Madrid”, En: Madri+d. Monografía: revista de investigación en gestión de la innovación y tecnología, 2003 MAY; (6).
- Hermoso, Carmelo, “*José Luis Piñar Maña, director de la Agencia Española de Protección de Datos. "En la AEPD somos conscientes de las preocupaciones del sector"*”. En: IPMARK: Información de publicidad y marketing: Guía de servicios y proveedores, 2004 MAY 16; (621).
- Almuzara Almáida, Cristina, “*Introducción y principios de la Ley Orgánica 15/1999, reguladora de la protección de datos de carácter personal*”. En: Lex Nova: la revista, 2004 ENE-MAR; (35).
- Ramírez Cruz, Rafael, “*El futuro reglamento de protección de datos*”. En: Byte España, 2005 NOV; (122).
- Agencia de Protección de Datos de la Comunidad de Madrid. “*Memoria 2004*”. Madrid, 2005.

- González Ballesteros, Teodoro. *“Los principios de la protección de datos personales: Garantías frente al poder político”*. En Telos: cuadernos de Comunicación, tecnología y sociedad, 1994 MAR-May (37).
- Garrido Gómez, M. Isabel. *“Datos personales y protección del ciudadano”*. Revista de la Facultad de Derecho de la Universidad Complutense, 1997; (87).
- Ull Pont, Eugenio. *“Protección de datos personales en ficheros de titularidad pública”*. Informática de derecho: revista iberoamericana de derecho informático 1998; T.1 (19-22) T. 2 (23-26).
- Olano García, Hernán Alejandro *en su texto de la Constitución Política de Colombia*. Bogotá, Doctrina y Ley, 2002.
- Murillo de la Cueva, Pablo Lucas. *“El derecho de la autodeterminación informativa”*. Editorial Tecnos. Madrid, España, 1990
- López-Muñiz Goñi, Miguel, *'La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal'*, Informática y Derecho, núms. 6-7, 1994, p. 93-116.
- Heredero Higuera, Manuel, *“La Directiva comunitaria de protección de datos de carácter personal”* Pamplona : Aranzadi, D.L. 1997, pag.96
- López-Muñiz Goñi, Miguel, *'La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal'*, Informática y Derecho, núms. 6-7, 1994, p. 93-116.
- Lema Devesa, Carlos, *“Protección de Datos y Publicidad”*, Ponencia presentada en la XX Conferencia Internacional de Autoridades de Protección de Datos. Santiago de Compostela, España, 16-18 de Septiembre de 1998.
- Salom, Javier Aparicio, (*"Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal"*), Editorial Aranzadi. Pamplona, España, 2000, pág.95
- Battaner, Santiago. *“Datos personales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid”*, Nº. 18, 2005
- Ramos Simón, Luis Fernando. *“Introducción a la administración de información”*, Madrid : Síntesis, D.L. 2003

Anexos

1 – Tablas de las encuestas a estudiantes y trabajadores.

2 – Formulario para la creación de un fichero en la APDCM.

3 – Legislación:

- LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- LEY 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

Encuesta trabajadores

	1	2	3	4	5	6
1	1	2	5	2	6	6
2	1	4	5	2	6	6
3	0	4	3	5	6	6
4	1	1	4	4	5	5
5	1	4	5	2	5	6
6	0	1	4	5	6	6
7	1	5	5	6	6	6
8	1	5	5	6	6	6
9	1	6	5	6	6	6
10	1	4	6	6	6	6
11	1	2	5	6	5	6
12	1	4	6	2	4	6
13	1	1	4	5	6	6
14	0	2	6	6	6	6
15	0	1	6	4	6	6
16	1	2	6	6	6	6
17	1	5	5	5	6	6
18	1	2	6	5	6	6
19	1	1	5	4	6	6
20	1	3	4	3	6	6

21	0	1	3	5	5	6
22	1	1	6	6	6	6
23	1	2	6	6	6	6
24	1	2	6	4	3	6
25	0	1	2	3	5	6
26	1	2	4	6	6	6
27	1	3	4	3	3	5
28	1	2	3	2	4	6
29	0	3	2	1	5	6
30	0	1	3	3	6	5
31	1	5	6	4	4	4
32	1	2	5	5	6	6
33	0	2	4	3	6	6
34	1	6	5	2	6	6
35	1	1	2	1	4	6
36	1	2	4	6	6	6
37	1	2	5	6	6	6
38	1	1	6	6	6	6
39	1	2	3	5	6	6
40	0	2	4	5	6	6
41	0	1	5	4	6	6
42	1	3	4	5	5	6
43	1	1	5	6	6	6
44	1	2	5	5	6	6
45	1	2	4	6	6	6
46	1	3	5	6	6	6
47	0	1	6	4	5	6
48	1	5	5	4	6	6
49	1	4	4	5	6	6
50	1	4	4	5	6	5

Encuesta estudiantes

	1	2	3	4	5	6
1	0	2	2	3	5	4
2	0	2	4	5	6	2
3	0	1	3	5	6	5
4	0	2	2	4	5	5
5	0	2	1	5	6	6
6	0	3	2	6	5	4
7	1	3	4	5	6	6
8	1	2	3	5	5	6
9	0	3	2	4	4	6
10	1	3	3	3	5	4
11	0	2	5	4	6	6
12	0	5	4	6	6	6
13	1	1	6	5	6	4
14	0	2	2	6	4	4
15	1	1	4	6	6	5
16	1	2	2	6	4	3
17	0	1	1	5	5	4
18	0	1	4	4	6	2
19	0	2	3	4	6	6
20	0	1	2	6	4	5
21	0	1	4	6	6	6
22	0	2	4	6	4	6
23	0	2	3	6	6	3
24	0	1	2	5	6	5
25	1	2	3	4	6	5
26	0	1	4	3	5	2
27	1	2	1	4	6	6
28	0	2	2	4	5	5
29	1	1	3	5	6	5
30	0	1	2	6	6	4
31	1	2	1	4	6	1
32	0	1	2	4	5	3
33	0	3	3	5	5	4
34	0	3	4	3	4	5
35	1	1	3	4	5	6
36	0	1	2	3	6	6
37	1	2	3	3	6	6
38	0	3	5	4	5	5
39	0	3	1	2	2	6

40	0	2	2	4	4	5
41	0	1	3	2	6	4
42	1	1	3	3	6	3
43	0	3	1	1	1	6
44	0	2	2	4	5	6
45	0	1	3	6	4	6
46	0	3	2	4	3	5
47	0	3	2	3	4	6
48	0	2	1	5	4	6
49	0	1	1	2	5	5
50	0	2	3	3	4	5
51	0	1	2	5	5	6
52	0	3	1	2	5	4
53	1	3	1	1	2	5
54	1	4	3	4	6	6
55	0	1	2	5	6	5
56	0	1	1	5	5	5
57	0	2	3	2	6	4
58	0	2	2	1	4	5
59	1	1	2	4	5	6
60	0	1	1	4	5	6
61	0	2	2	4	6	6
62	1	1	1	6	6	6
63	0	2	1	2	5	5
64	0	2	2	1	5	5
65	0	1	4	3	4	2
66	1	2	5	5	4	5
67	0	1	2	5	5	6
68	0	1	2	5	5	6
69	1	4	4	3	3	3
70	1	1	5	4	5	5
71	0	1	3	2	6	4
72	0	1	3	5	5	5
73	0	2	4	5	6	5
74	0	3	2	6	6	6
75	1	1	1	5	6	6
76	1	2	1	4	6	5
77	0	3	3	3	5	5
78	0	2	1	1	2	5
79	1	1	2	5	5	6
80	1	3	4	4	4	4
81	1	3	2	3	4	6
82	0	1	2	3	4	5
83	0	2	1	2	3	3
84	1	1	2	4	5	4
85	1	3	2	4	6	4
86	1	4	2	2	6	2
87	0	2	1	3	6	4

88	0	1	1	4	5	4
89	0	3	3	1	5	5
90	1	2	3	4	5	6
91	1	2	2	3	6	6
92	0	1	4	5	5	5
93	0	2	3	4	5	4
94	0	1	4	3	5	5
95	0	3	2	4	4	4
96	1	3	3	4	3	4
97	0	2	5	5	4	4
98	0	1	3	3	4	4
99	0	2	3	5	5	6
100	0	2	3	2	4	5