IX Encuentro Estatal de Defensores Univesitarios

MESA de TRABAJO nº 1 - Confidencialidad

Joan Miró Ametller (Universitat de Girona)

Purificación Fenoll Hach-Alí (universidad de Granada)

Artur Juncosa Carbonell (Universitat Ramón Llull)

Introducción

Entre les características principales de la figura del defensor universitario destacan su independencia y el carácter confidencial de su labor. Al introducir la figura del defensor universitario, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades establecía que su función consiste en velar por los derechos y las libertades de los miembros de la comunidad universitaria y que sus actuaciones, dirigidas a contribuir a la calidad del sistema universitario, no están sometidas a mandato imperativo de ninguna instancia universitaria y se rigen por los principios de independencia y autonomía. Así lo han recogido los Estatutos de las distintas universidades cuando han regulado la figura del defensor. Para desarrollar sus funciones en un clima de plena confianza de la comunidad universitaria, una de las condiciones inherentes a la figura del defensor es, muy frecuentemente, la confidencialidad en la comunicación entre quienes visitan la oficina del defensor y el propio defensor y, por lo tanto, la seguridad en el tratamiento y la conservación de los documentos generados en el curso de las actuaciones del defensor.

Las oficinas del defensor universitario manejan documentos escritos y ficheros informáticos que afectan a personas y que contienen nombres y datos confidenciales. Estos documentos, en principio, se guardan en el archivo de la propia oficina o en los ordenadores del defensor y de sus colaboradores administrativos.

Existe una legislación sobre datos personales, sobre el tratamiento y conservación de la documentación administrativa y sobre patrimonio histórico.

Son la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter

personal, la Ley 30/1992 de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, la Ley 16/1985 de 25 de junio, del Patrimonio Histórico Español, las orientaciones que pueda dar la Agencia española de protección de datos y la legislación propia de cada comunidad autónoma (que también pueden tener sus propias agencias de protección de datos o su equivalente).

Confidencialidad, intimidad y anonimato

La confidencialidad es uno de los principios básicos que inspiran la actuación de los defensores universitarios, mientras que la intimidad es un derecho fundamental reconocido expresamente como tal en el artículo 18.1 de la Constitución española. Una vulneración del principio de confidencialidad no tiene necesariamente que implicar una lesión del derecho a la intimidad, aunque puede llevarla aparejada. Lo dicho respecto del derecho a la intimidad es también aplicable al derecho fundamental a la protección de datos de carácter personal, reconocido por nuestra constitución en el artículo 18.4, y que puede resultar afectado con independencia o en concurrencia con los anteriores.

La confidencialidad no exige, por otra parte, el anonimato. De hecho, las quejas presentadas ante los Defensores Universitarios no pueden ser anónimas, aunque sí son confidenciales.

El concepto de interés legítimo y el principio de confidencialidad. Casos especiales

Para que el Defensor Universitario pueda intervenir, el quejoso ha de ser miembro de la comunidad universitaria y demostrar que tiene un interés legítimo en el asunto que presenta. No es infrecuente, no obstante, que se dirijan al Defensor padres, novios, amigos, etc.

La cuestión no parece en principio problemática, pero existen casos en que el Defensor no tiene más remedio que acceder a contactar con estas personas intermedias. Se trataría de identificar aquellos casos en que, siempre de manera excepcional, dicha actuación pudiese estar indicada (alumnos enfermos o que disfrutan de becas en el extranjero, etc.).

En ciertos casos, el desarrollo de las gestiones realizadas por el Defensor puede parecer contradictorio con el principio de confidencialidad. Son casos en que resulta

difícil, o incluso imposible, al Defensor Universitario defender los derechos de los miembros de la comunidad universitaria que a él se dirigen, sin que el órgano administrativo llegue a conocer la identidad de los quejosos (problemas relacionados con evaluación de exámenes, casos en que, antes de llegar el problema al Defensor, los quejosos se significaron sobremanera ante el órgano administrativo, etc.).

Por otra parte, la confidencialidad parece más vulnerable cuando la queja viene firmada por un colectivo de personas, ya que en la confección de esos escritos de adhesión, lo normal es que algunas personas se signifiquen más que otras y resulte difícil mantener la reserva.

Se trata, pues, como en los casos anteriores, de diseñar protocolos de actuación que permitan preservar en la medida de lo posible la confidencialidad en estos y otros supuestos, o al menos advertir a los quejosos de los posibles riesgos.

La confidencialidad puede quedar también expuesta a través de la correspondencia enviada por el Defensor Universitario, para lo que deben tomarse toda una serie de precauciones, tanto con relación al quejoso como respecto del órgano administrativo implicado.

Tipos de información

Típicamente, la oficina del defensor diversos tipos de documentos relacionados con las actuaciones del defensor: quejas, denuncias, solicitudes de mediación… Una buena parte de esta información tiene carácter confidencial. Se puede decir que las paredes de la oficina del defensor escuchan, pero no hablan. Sin embargo, de todos los casos se realiza un informe escrito.

Como se ha dicho, no toda la información es absolutamente confidencial. Si un investigador presenta una queja sobre un trabajo que conlleve una actuación cerca del responsable del grupo de investigación, será inevitable plantear el problema y aparecerán nombres, aunque todo, en principio, quede restringido entre dos personas o como máximo dentro del ámbito del grupo.

La información puede ser estrictamente individual o colectiva. Por ejemplo, si un grupo de alumnos o becarios presenta una reclamación deberán tenerse en cuenta los derechos de cada uno de los miembros del grupo.

Aunque confidencial, no es obvio que el tipo de información que llega a la oficina del defensor deba ser tratado como información secreta, excepto quizás ciertos aspectos de carácter muy personal que, generalmente y por razones de sentido común, probablemente no se recogen por escrito o es información que se destruye sin pasar al archivo. Sin embargo, un documento referido al funcionamiento de una entidad pública que se conserve no será para siempre inaccesible. Entre otras muchas posibilidades de petición de permiso para acceder a cierta documentación bastará citar la investigación histórica.

Por ello también deben considerarse en el marco de la confidencialidad, la seguridad de los archivos, los sistemas de destrucción de documentos y su conservación.

Tipos de documentos y tratamiento de ficheros

Una parte de la documentación en la oficina del defensor está escrita sobre papel. En algunos casos se trata de borradores, que se destruyen. Sin embargo, existen documentos definitivos que se archivan como si se tratara de un expediente.

También existe documentación sobre soporte informático en el ordenador del propio defensor y en los de su equipo administrativo.

Las universidades han empezado a adaptarse al reglamento de medidas de seguridad de ficheros automatizados que contienen datos de carácter personal, aprobado por real decreto (1999) y a la ley orgánica 15/1999 de protección de datos. Dicho reglamento define los usuarios de los archivos, los procedimientos que deben aplicarse, las responsabilidades de las personas que tienen archivos de este tipo a su cargo y establece niveles de seguridad para tratar dichos ficheros. Como se resume en el cuadro adjunto, cuando los ficheros contengan datos de carácter personal que permitieran evaluar la personalidad de un individuo, les corresponde el nivel medio. Si los datos se refieren a ideología, origen racial, salud, etc., les corresponde el nivel alto.

Características de los archivos según el tipo de datos

Tipos de datos - [Nivel / Autenticación / Confidencialidad / Integridad]

Datos no personales

[- / Baja / Libre / Baja]

Datos personales

[Básico / Normal / Restringida / Normal]

Infracciones, Hacienda, financieros, legislados, evaluadores

[Medio / Alta / Protegida / Alta]

Ideología, creencias, salud, raciales, sexuales, policiales

[Alto / Crítica / Confidencial / Crítica]

El responsable del fichero debe implantar una normativa de seguridad que contemplará aspectos como las normas que hay que respetar, las funciones y obligaciones del personal, el procedimiento de notificación de incidencias, de realización de copias, etc. Esto se aplica en los tres niveles.

Todo fichero que contenga datos personales deberá adoptar por lo menos las medidas de seguridad de nivel básico. Los ficheros de este nivel se destruirán cuando ya no sean necesarios para los fines que motivaron su creación.

Para el nivel medio de seguridad, los ficheros tendrán que someterse a auditoria. El responsable debe establecer un mecanismo de identificación de los usuarios que intenten acceder al fichero. Sólo el personal autorizado podrá acceder a los locales donde se encuentren los sistemas de información, deberá existir un registro de entrada y salida de soportes informáticos y se adoptarán medidas para evitar que se recupere la información cuando el soporte sea desechado o reutilizado.

En el caso del nivel alto, la información deberá estar cifrada si los soportes se distribuyen o los datos se transmiten telemáticamente.

Los ficheros y tratamientos de datos han de ser inscritos en un registro público de la Agencia de Protección de Datos (española o autonómica).

En el curso del proceso de adaptación al reglamento de medidas de seguridad, la universidad deberá identificar y analizar la tipología de ficheros sensibles con los que trabaja y los riesgos que pueden afectarlos. El defensor será el responsable directo de la gestión de los ficheros de su oficina (aunque el responsable general de los ficheros de la universidad será el secretario general). Entre otras cosas, la universidad deberá tener en cuenta ciertas cláusulas de confidencialidad al contratar personal y servicios.

Por último, la universidad redactará un documento de seguridad propio y aprobará y difundirá las instrucciones pertinentes para aplicar su normativa sobre protección de datos y sobre el uso de recursos y sistemas informáticos.

Será pues esencial que nuestras oficinas y su personal respondan a las exigencias de los niveles de seguridad de los documentos y ficheros con los que trabajan y que dispongan de equipos informáticos de alto nivel de seguridad, de criterios, orientaciones y normativas de distribución y de conservación de documentos, así como de maquinaria homologada para su destrucción.

Uno de los temas que deberá tener un tratamiento particularizado es el de la correspondencia. Por una parte, hay quien hace llegar sus escritos a la oficina del defensor utilizando el servicio del registro; entre la documentación que presenta puede haber información confidencial. Por otra parte, algunos documentos escritos que salen de la oficina del defensor pueden estar destinados a ser leídos por una única persona. Se trataría de estudiar un modelo de envío postal que acentúe en lo posible las garantías de todos los que se relacionan con el defensor (forma de utilización de los sellos “confidencial”, “abrir en destino”, utilización de los certificados, etc.). En este campo, las nuevas tecnologías – en particular, el correo electrónico – introducen todavía más la necesidad de tomar precauciones.

El deber de confidencialidad en el tiempo: la custodia de la documentación generada por las actuaciones del defensor universitario

El deber de confidencialidad, así como los derechos a la intimidad y protección de datos, no se extinguen una vez cerrado el expediente de queja, sino que se convierten en un deber de custodia, tratamiento informático, conservación y, en su caso, destrucción de datos y documentos obrantes en la oficina relacionados con el caso.

Tarde o temprano, la documentación que se conserve en una oficina pasará al archivo general de la institución. Los responsables de los archivos conocen bien su profesión y confiamos justificadamente en ellos. Una parte del archivo es confidencial y no se puede consultar… excepto si presenta una petición de consulta la persona afectada o un miembro del colectivo cuando el documento afecta a un colectivo.

Por otra parte, la legislación convierte en accesibles los documentos transcurridos 50 años del caso o 25 años de la muerte de la persona a la que se refiere.

Existe una experiencia acumulada que se puede calificar de secular en los profesionales de la archivística que transmite una vigorosa sensación de seguridad. Sin embargo, la seguridad de los archivos informáticos presenta características particulares que otorgan a este tipo de archivos ciertas debilidades para las que se precisan actuaciones especiales.

Las universidades han instalado cortafuegos, han reforzado sus sistemas de seguridad y han montado servicios informáticos que inspiran confianza. A pesar de todo, se pueden imaginar fácilmente situaciones en las que los ordenadores pueden correr serios peligros.

Seguridad informática

Ciertas prácticas, como abrir archivos sospechosos adjuntos a mensajes electrónicos o instalar programas no seguros, debilitan los sistemas de seguridad y permiten el acceso de usuarios no deseados a información privilegiada confidencial.

Además del propio usuario, en una red de ordenadores suelen existir permisos de grupo y permisos de acceso remoto para técnicos.

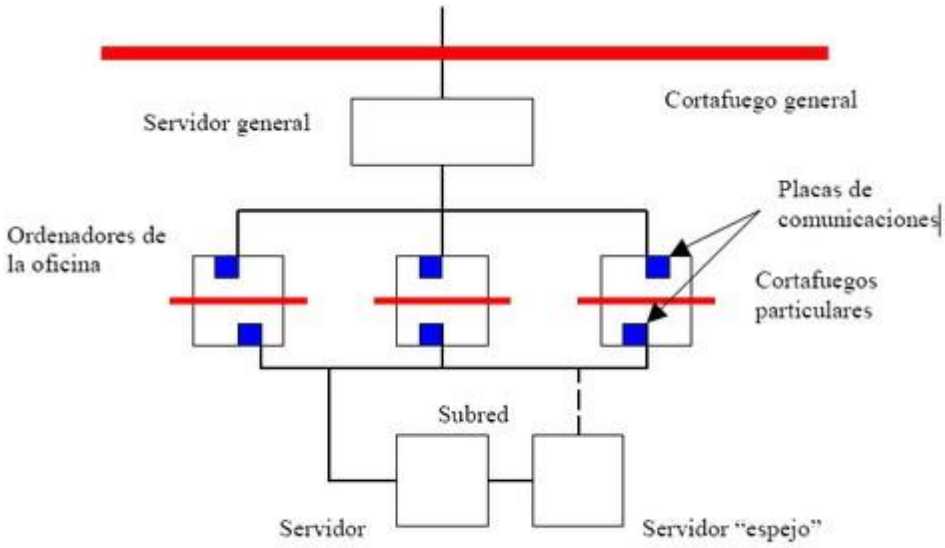
Hay otros escenarios: desprotección incidental o accidental de carpetas de usuarios, pérdida de memorias portátiles o de ordenadores portátiles que contienen información de nivel alto…

No se deben exagerar estos peligros; no es tampoco prudente dejar de tenerlos en consideración. Las instituciones como la universidad funcionan fundamentadas en la confianza. Sin embargo, siempre puede darse un incidente.

Generalmente, la solución a estos problemas se halla en el respeto estricto de los protocolos establecidos por los criterios de seguridad. Sin embargo, los incidentes pueden suceder inesperadamente. Aunque no exista la seguridad absoluta, puede obtenerse un ambiente informático de mayor confidencialidad incluyendo en los ordenadores cortafuegos particulares que permitan aislar una subred confidencial respecto la red general de la universidad, como aparece en el esquema adjunto. La subred consiste en un ordenador común para almacenar archivos (servidor) y un gemelo para las copias de seguridad (con posibilidad de conexión para prevenir accidentes).

Los cortafuegos particulares separan la placa de comunicaciones conectada a la red general de la placa conectada a la subred. Si técnicamente es posible, una partición del ordenador trabaja con la red general y otra, la confidencial, sólo con la subred.

Red de confidencialidad



Probablemente, otras secciones de una universidad –como el rectorado, la gerencia, el departamento de personal…– requieran también un tratamiento particular de acceso restringido del mismo tipo.

La difusión de la información. El equilibrio entre el deber de informar al Claustro y la obligación de preservar la confidencialidad.

Naturalmente, la información más confidencial no sale de la oficina del defensor. Los procedimientos que deben aplicarse a los archivos de nivel de confidencialidad alto restringen el traslado y el movimiento de los archivos, cuya salida de su ámbito de uso debe ser registrada.

Una de las obligaciones de los defensores es la presentación del informe anual ante el claustro universitario, que se complementa con la elaboración de una memoria de actividades La práctica de las memorias consiste en exponer los casos preservando el anonimato, aunque hay detalles que, inevitablemente, conducen a la identificación, si no de la persona, por lo menos del centro o departamento afectados. Quizá no es un inconveniente mayor, porque contribuye a reformar positivamente el funcionamiento de la universidad.

Distribución de espacios en la oficina del defensor y protección de la confidencialidad

La configuración arquitectónica y la distribución de los espacios de la Oficina del Defensor Universitario pueden incidir directa o indirectamente, positiva o negativamente, en la preservación del derecho a la confidencialidad de quienes al Defensor se dirigen.

Se trataría de confeccionar un diseño ideal de la distribución de los espacios y de los equipamientos mínimos que debe reunir la Oficina del Defensor Universitario, en orden a la protección de la confidencialidad: ubicación dentro del entorno universitario, disponibilidad de espacios idóneos para una atención reservada, impermeabilidad visual de ciertas dependencias y accesos, configuración de las salas de espera, etc.

Destrucción de documentos

Las universidades deben disponer de un servicio de destrucción de documentos que asegure que la eliminación es completa. La eliminación de datos y de información pública deba hacerse según las normas.

En la actualidad, parte de la documentación de la oficina es eliminada probablemente mediante un sistema rutinario. Si la destrucción de documentos se mecaniza, tendremos que organizarla y establecer de modo más preciso qué documentos, a medida que la documentación se acumule, deben ser destruidos para siempre. La historia de la institución no es sólo la historia de las oficinas ni mucho menos de sus intimidades.

Consulta de documentos

La política lógica de la oficina consiste en no permitir ninguna excepto la del afectado que pide acceso a sus propios documentos, por ejemplo si no se reservó una copia. No tiene acceso, sin embargo, a los restantes documentos que puedan formar parte del caso y que no le pertenece, aunque la conozca porque le ha sido comunicada durante las conversaciones que mantenido con el defensor.

El debate de la mesa uno

El debate sobre la confidencialidad en el seno de la mesa nº 1 fue sumamente enriquecedor. Los participantes aportaron numerosas ideas y experiencias personales de gran interés que contribuyeron a esclarecer los problemas que plantea la práctica de la confidencialidad en la actuación del defensor universitario. Así fue posible discutir los términos en los que se desarrolla la labor del defensor y se establecieron criterios de orientación para mejorar su trabajo.

Es posible que resulte conveniente que las oficinas del defensor se sometan a evaluación voluntaria, sin menoscabo de su independencia, con el fin de detectar sus puntos fuertes y débiles y realizar las operaciones oportunas para contribuir a la calidad del sistema universitario.

La seguridad en el tratamiento de archivos de datos personales es un tema de importancia suficientemente alta como para ser tratado con la ayuda de profesionales. En este sentido, puede ser conveniente cursar, en el próximo encuentro de defensores, una invitación a un experto de la Agencia Nacional de Protección de datos

para informar sobre este punto, así como para establecer criterios sobre la elaboración de la memoria anual e informar sobre el equilibrio que debe existir entre el deber de informar al Claustro y la obligación de preservar el principio de confidencialidad y los derechos intimidad y a la presunción de inocencia.

Conclusiones de la mesa nº 1: La confidencialidad

Primera:

La confidencialidad es un requisito esencial en la función del defensor como garante de los derechos y libertades de las personas de la comunidad universitaria.

La confidencialidad, en el sentido de secreto profesional, es el instrumento que asegura la independencia, la imparcialidad y la responsabilidad para inspirar confianza en la figura del defensor.

Segunda:

Los defensores deben instar a las universidades para que procedan a cumplir y completar la adaptación a las normas de protección de datos de carácter personal y a establecer criterios de seguridad.

Tercera:

La oficina del defensor universitario debe disponer de los elementos y mecanismos necesarios para desarrollar y asegurar su labor de acuerdo con el principio de confidencialidad.

Cuarta:

Las memorias e informes del defensor universitario, sin perjuicio de que se ajusten a las diversas tradiciones de las universidades, deberán respetar la confidencialidad y, en lo que sea posible, se pueden transformar en recomendaciones generales las características comunes que se infieran de los casos particulares.

Consultas

Ley orgánica 15/1999 [17 de octubre de 2005]

(Incluye la sentencia 292/2000 del Tribunal Constitucional de 30 de noviembre de 2000 que declaraba inconstitucionales determinados incisos)

Real decreto 994/1599, [5 de julio de 2006]

Agencia española de protección de datos, [5 de julio de 2006]