GUÍA PRÁCTICA

para la utilización de muestras biológicas en Investigación Biomédica

IV. GESTIÓN DE BASES DE DATOS

1. La creación de ficheros y su notificación
2. El responsable y el encargado del tratamiento
3. Las medidas de seguridad

IV. Gestión de bases de datos

1. LA CREACIÓN DE FICHEROS Y SU NOTIFICACIÓN

La creación de ficheros con datos de carácter personal debe ir acompañada de una notificación formal para su inscripción en el Registro General de Protección de Datos (RGPD) incardinado en la Agencia Española de Protección de Datos (AEPD).

El objeto de este registro es que cualquier persona pueda conocer la existencia de tratamientos de datos personales, sus finalidades, y la identidad y dirección del responsable de dichos tratamientos, lo que facilita que se puedan ejercer los derechos de acceso, rectificación, cancelación y oposición reconocidos en la normativa vigente.

Teniendo en cuenta este objeto del registro, la notificación tiene una naturaleza meramente declarativa y su inscripción no supone ningún tipo de autorización del fichero –que es innecesaria– ni la acreditación de que su funcionamiento real y efectivo cumpla con la normativa de protección de datos personales.

La notificación tampoco lleva aparejada la comunicación al registro de los datos personales incorporados en el fichero que se pretende inscribir, sino que se limita a declarar la existencia del fichero, con indicación de su responsable, la finalidad, la ubicación, el nivel de medidas de seguridad exigible –sin detallar el contenido de las mismas– y las cesiones de datos que se prevean, así como las transferencias de datos a terceros países que se vayan a producir, sin considerar terceros países a los Estados miembros de la Unión Europea ni a los que conforman el Espacio Económico Europeo.

Sin embargo, los requisitos para la creación de ficheros son distintos según los mismos sean de titularidad pública o privada. En el primer caso, la creación, la modificación o la supresión del fichero sólo se puede hacer mediante una disposición general previamente publicada en el *Boletín Oficial del Estado* o en el correspondiente diario oficial.

Las disposiciones de creación o modificación de los ficheros deben indicar su finalidad y usos previstos, las personas o colectivos de los que se pretende obtener datos personales o que estén obligados a suministrarlos, el procedimiento de recogida de los

datos, la estructura básica del fichero y los tipos de datos incluidos en el mismo, las cesiones o, en su caso, las transferencias que se prevean realizar a terceros países, los órganos de la Administración responsables del mismo, los servicios o unidades ante los que se pueden ejercer los derechos de acceso, rectificación o cancelación y oposición, así como la indicación del nivel de medidas de seguridad.

Por su parte, en las disposiciones de supresión de los ficheros se ha de establecer el destino de la información o, en su caso, las previsiones que se adopten para su destrucción.

En las comunidades autónomas en las que se haya creado una Autoridad de Protección de Datos y se haya previsto la existencia de registros de ficheros, será también necesario notificar para su inscripción los ficheros sobre los que tengan competencia. Así sucede en el caso de la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos. Entre ellas y la Agencia Española se están desarrollando procedimientos de colaboración que faciliten el cumplimiento de la obligación de notificar los ficheros en ambos registros.

En el caso de ficheros de titularidad privada su creación no precisa de una disposición previa de carácter general, aunque sí resulta exigible la notificación al RGPD de su inscripción.

Con independencia de la titularidad pública o privada de los ficheros, la notificación al Registro General de Protección de Datos de la AEPD se ha de realizar conforme a los modelos oficiales publicados en la página web de la Agencia: *www.agpd.es*.

Cuando sea necesario notificar un fichero de titularidad pública al registro de ficheros de una agencia autonómica, también se encuentran disponibles los modelos correspondientes en las páginas web de cada agencia.

Se debe resaltar que la obligación de notificar los ficheros para su inscripción es de naturaleza dinámica, de forma que la inscripción debe encontrarse actualizada en todo momento. De ahí que sea preciso notificar las modificaciones que se vayan produciendo, así como la supresión de los ficheros en el caso de que la misma tenga lugar.

2. EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

La normativa de protección de datos distingue varias figuras, como son el responsable del fichero o del tratamiento y el encargado del tratamiento.

El primero de ellos es la persona física o jurídica, de naturaleza pública o privada, o el órgano administrativo que decide sobre la finalidad, el contenido y el uso de los datos personales. Siempre que concurren estas circunstancias será responsable, incluso

aunque materialmente no sea el que trata la información. A él le corresponde la obligación de notificar.

El encargado del tratamiento es la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trata datos personales por cuenta del responsable al que se refiere el párrafo anterior, para la prestación de un servicio al mismo.

Esta figura del encargado del tratamiento, que puede prestar todo tipo de servicios, es particularmente importante en un momento en que, por las más diversas razones, es muy habitual la externalización de servicios.

La Ley Orgánica de Protección de Datos (LOPD) permite que el encargado del tratamiento pueda acceder a los datos personales para la prestación de servicios, sin necesidad de contar con el consentimiento de los afectados.

Pero esta posibilidad sólo podrá materializarse lícitamente si se cumplen las garantías exigidas por la Ley.

En este sentido, la Ley exige que la prestación de servicios esté regulada en un contrato que debe constar por escrito, de forma que se pueda acreditar su celebración y contenido.

En el contrato se deberá establecer, expresamente, que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con un fin distinto al que figure en el contrato y que no los comunicará, ni siquiera para su conservación, a otras personas.

Asimismo, en el contrato se deben estipular las medidas de seguridad exigibles, las cuales deberán ser implementadas por el encargado de tratamiento.

La prestación de servicios puede ser temporal o preverse con carácter indefinido pero, al término de la misma, los datos personales deben ser destruidos o devueltos al responsable, al igual que cualquier soporte o documento donde conste algún dato personal.

De preverse o producirse por parte del prestador del servicio una subcontratación que implique el tratamiento de datos personales, deberá reflejarse en el contrato haciendo constar, expresamente, además de los requisitos antes expuestos, que el contratista actúa en nombre y por cuenta del responsable o, alternativamente, se han de especificar en el contrato los siguientes requisitos acumulativos:

- Que los servicios subcontratados se hayan previsto, expresamente, en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento.
- Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato.
- Que el tratamiento de datos personales, por parte del subcontratista, se ajusta a las instrucciones del responsable del fichero.

3. LAS MEDIDAS DE SEGURIDAD

El tratamiento de los datos personales exige, en todo caso, la implantación efectiva de medidas de seguridad. Estas medidas tienen como finalidad garantizar la integridad, la confidencialidad y la disponibilidad de la información, evitando su pérdida o alteración; así como impedir los accesos no autorizados.

La adopción de las medidas de seguridad corresponde al responsable del fichero; es decir, a la persona o entidad que decide la finalidad, contenido y uso de los datos personales y, también, a los terceros que le presten servicios que permitan acceder a la información personal.

Las medidas de seguridad no sólo deben ser de naturaleza técnica, sino también organizativa, puesto que las deficiencias en estas últimas pueden producir debilidades o hacer ineficaces las primeras, como demuestra con frecuencia la experiencia práctica.

Las medidas de seguridad se clasifican en tres niveles: básico, medio y alto, atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

En particular, los tratamientos de los datos relacionados con la salud, como es el caso de la información genética, requieren, además de las medidas de seguridad de nivel básico y medio, las de nivel alto.

Las medidas de seguridad exigibles, conforme a la normativa de protección de datos de carácter personal, tienen la condición de mínimos exigibles, y se deben completar con las que puedan contemplar otras disposiciones legales específicas.

Antes de la implantación o de la modificación de los sistemas de información se pueden realizar pruebas. Estas pruebas no se deben realizar con datos reales pero, en el caso de que sí se utilicen, se deben cumplir todas las medidas de seguridad.

Asimismo, el tratamiento de los datos se realiza fuera de los locales donde está ubicado el fichero y deberá ser expresamente autorizado por el responsable del mismo y garantizarse el nivel de seguridad exigible a dicho fichero.

En cualquier caso, las necesidades de seguridad exigibles a un fichero, y en particular las relativas al control de acceso, se deben garantizar con independencia de que el acceso se esté realizando localmente desde las mismas instalaciones en las que se encuentra ubicado el fichero, o de que se realice remotamente a través de redes de telecomunicaciones.

También los ficheros temporales deben cumplir estas medidas de seguridad y borrarse cuando hayan dejado de ser necesarios para los fines que motivaron su creación.

Una de las medidas de seguridad fundamentales es la elaboración de un documento de seguridad. Este documento es de obligado cumplimiento para el personal que

accede a los datos personales y a los sistemas de información y constituye el eje de la política de seguridad de los datos.

El documento tiene un contenido mínimo que incluye su ámbito de aplicación, con especificación detallada de los recursos protegidos; las medidas, las normas, los procedimientos, las reglas y los estándares que garantizan la seguridad; la estructura de los ficheros con datos personales y la descripción de los sistemas que los tratan; el procedimiento de notificación, gestión y respuesta a las incidencias y los procedimientos de realización de copias de respaldo y de recuperación de la información.

El documento de seguridad debe identificar al responsable o responsables de la seguridad, contener los controles periódicos que se tengan que realizar para verificar el cumplimiento de lo dispuesto en el propio documento y qué medidas adoptar cuando un soporte vaya a ser desechado o reutilizado. Por soporte se entiende cualquier objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Los responsables de seguridad son las personas designadas por el responsable del fichero a los que se les encarga la coordinación y el control de las medidas establecidas en el documento de seguridad.

No obstante, el hecho de que se designen responsables de seguridad no supone una delegación de la responsabilidad que corresponde al responsable del fichero.

El documento de seguridad se debe mantener siempre actualizado, siendo necesaria su revisión cuando se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

Los usuarios, únicamente, pueden tener autorizado el acceso a los datos y recursos que precisen para el desarrollo de sus funciones, por lo que se deben establecer mecanismos que eviten que un usuario pueda realizar accesos distintos de los autorizados.

Por ello es imprescindible que el responsable del fichero no sólo documente dichas funciones y obligaciones, sino también que adopte las medidas necesarias para que cada persona conozca las medidas de seguridad que afectan al desarrollo de las funciones que tenga atribuidas, así como las consecuencias en que podría incurrir en el caso de incumplimiento.

Asimismo, es necesario que el documento de seguridad incluya una clara definición de las funciones y obligaciones del personal, ya que de ella dependerán las autorizaciones para acceder a la información o tratar los datos personales.

Con el fin de poder verificar los accesos realizados, de cada uno de ellos se ha de guardar la identificación del usuario, la fecha y la hora en que se realizó el acceso, el fichero al que se ha accedido, el tipo de acceso y si fue autorizado o denegado. En el caso de que los accesos hayan sido autorizados, será preciso guardar también la in-

formación que permita identificar el registro al que se accedió. Toda la información relativa al control de accesos se debe conservar durante un periodo mínimo de dos años.

Complementariamente debe existir una relación actualizada de los usuarios con acceso autorizado al sistema de información, así como procedimientos de identificación y autenticación para realizar dicho acceso.

La relación de usuarios ha de contener el acceso autorizado para cada uno de ellos.

La identificación es el procedimiento que permite reconocer la identidad del usuario autorizado y la autenticación tiene por objeto comprobar dicha identidad. Los mecanismos de identificación deben permitir que ésta se realice de forma unívoca y personalizada.

Los mecanismos de autenticación se pueden basar en la existencia de contraseñas, en cuyo caso los procedimientos para su asignación, distribución y almacenamiento deben garantizar la confidencialidad e integridad de las mismas.

Por otro lado, las contraseñas se deben cambiar cada cierto tiempo –según los periodos que determine el documento de seguridad– y mientras estén vigentes, se han de almacenar de forma no inteligible.

En todo caso se debe limitar la posibilidad de intentar, reiteradamente, el acceso no autorizado al sistema de información.

Los mecanismos que permiten el registro de los datos deben estar bajo el control directo del responsable de seguridad competente, y no se debe permitir, en ningún caso, su desactivación.

Dicho responsable de seguridad se ha de encargar de revisar periódicamente la información de control registrada, y elaborar un informe de las revisiones realizadas y de los problemas detectados, al menos, una vez al mes.

Las anomalías que afecten o puedan afectar a la seguridad de los datos se denominan incidencias.

El procedimiento de notificación y de gestión de las incidencias debe incluir, necesariamente, un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quien se le comunica y los efectos que se hayan derivado de la misma.

En dicho registro se deben consignar, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de restauración de los mismos.

Para la ejecución de los procedimientos de recuperación de los datos es necesaria la autorización por escrito del responsable del fichero.

La recuperación de los datos se debe posibilitar mediante una copia de los mismos en un soporte denominado copia de respaldo.

En relación con ella, el responsable del fichero se debe encargar de verificar la definición y la correcta aplicación de los procedimientos para realizar copias de respaldo y de recuperación de los datos.

Estos procedimientos han de garantizar la reconstrucción de los datos en el momento en que se encontraban, al tiempo de producirse su pérdida o destrucción.

Las copias de respaldo se deben realizar al menos semanalmente, salvo en el caso de que, en dicho periodo de tiempo, no se hubiera producido ninguna actualización de los datos.

Además, se deberá conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos. Esta obligación de conservación se debe realizar cumpliendo el resto de las medidas de seguridad.

En cuanto a los locales donde se encuentren ubicados los sistemas de información, exclusivamente podrá tener acceso a ellos el personal autorizado en el documento de seguridad.

El tratamiento de la información puede exigir su utilización en distintos lugares. Desde el punto de vista de la seguridad, ello obliga a que se exijan medidas específicas para la gestión de los soportes en que consta aquella.

Los soportes informáticos que contengan datos personales deben permitir identificar el tipo de información que contienen, estar inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La salida de estos soportes informáticos, fuera de los locales en los que está ubicado el fichero, sólo puede ser autorizada por el responsable del fichero.

Además, es necesario establecer un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y la hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, la cual deberá estar debidamente autorizada al efecto.

Del mismo modo, se debe disponer de un sistema de registro de salida de soportes informáticos con la misma información que se ha detallado, excepto la relativa al emisor y a la persona responsable de la recepción, que debe ser sustituida por la correspondiente al destinatario, y a la persona responsable de la entrega.

Cuando los soportes vayan a ser desechados o reutilizados se han de adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información al-

macenada en elllos. Todo ello con carácter previo a que se proceda a darlo de baja en el inventario.

Las operaciones de mantenimiento también pueden dar lugar a que los soportes salgan fuera de los locales donde se encuentran ubicados los ficheros. En tal caso será preciso, asimismo, adoptar las medidas necesarias para impedir la recuperación indebida de la información almacenada en ellos.

La distribución de los soportes que contengan datos personales relativos a la salud se ha de realizar bien cifrando los datos, bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Si la transmisión de dichos datos se realiza a través de redes de telecomunicaciones, se debe cumplir igualmente lo expuesto en el párrafo anterior.

Con el fin de evaluar las medidas de seguridad implantadas, los sistemas de información e instalaciones de tratamiento de datos se han de someter a una auditoría que verifique su cumplimiento y los procedimientos e instrucciones vigentes en materia de seguridad.

A tal efecto, el informe de auditoría debe dictaminar las medidas y controles exigibles, identificar las deficiencias y proponer las medidas correctoras o complementarias que resulten necesarias. Asimismo habrá de incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas. Estos informes de auditoría tienen que ser analizados por el responsable de seguridad, quien, a su vez, elevará al responsable del fichero las conclusiones pertinentes. El responsable del fichero tiene la obligación de adoptar las medidas correctoras adecuadas.

Los informes de auditoría se han de conservar, además, quedando a disposición de la AEPD o de las agencias autonómicas cuando éstas sean competentes. La auditoría puede ser interna o externa y se debe realizar, al menos, cada dos años.