Expediente Nº: E/00978/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad DIRECTOR INSTITUTO UNIVERSITARIO DE OFTALMOBIOLOGIA APLICADA, FUNDACIÓN GENERAL DE LA UNIVERSIDAD DE VALLADOLID (IOBA), en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 3 de febrero de 2015, tuvo entrada en esta Agencia Española de Protección de Datos (AEPD) un escrito remitido por Don ***A.A.A.,*** en el que denuncia al Instituto Universitario de Oftalmobiología Aplicada (IOBA), indicando que la gestión del mismo recae en la Fundación General de la Universidad de Valladolid, poniendo en conocimiento los siguientes hechos:

Que trabaja como médico especialista en anatomía patológica y actúa como responsable del laboratorio de patología ocular del lOBA y que tienen problemas con el sistema operativo instalado en los ordenadores, ya que se trata de windows, no dan soporte técnico y no admite el antivirus instalado.

Que el Departamento de Informática no realiza copias de seguridad de las imágenes histológicas de las muestras obtenidas desde el año 2008 que están guardadas en el ordenador conectado al fotomicroscopio con el que se toman las mismas y que se podrían perder.

Que no se le facilita una llave para poder acceder al archivo donde se encuentran custodiados los estudios e informes de diagnóstico del laboratorio.

Se adjunta con el escrito de denuncia Informe de Situación sobre el Cumplimiento de la Ley de Protección de Datos en el ámbito de actividad específica del IOBA (Datos específicos sobre pacientes), realizado el 3 de julio de 2014, en el que se expone las posibles carencias y propuestas de acción a llevar a cabo.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. En el Registro General de Protección de Datos figura inscrito el fichero denominado "PACIENTES", con el código ***B.B.B.***, siendo responsable la Fundación General de la Universidad de Valladolid.
2. El Gerente de la Fundación General de la Universidad de Valladolid, ha informado a la Inspección de Datos en relación con los hechos comunicados por el denunciante lo siguiente:

   En los últimos meses se han puesto en marcha diferentes acciones para solventar las deficiencias que el centro detectó en el cumplimiento de la Ley

Orgánica de Protección de Datos (LOPD). Dichas deficiencias fueron plasmadas en el *Informe de Situación sobre el Cumplimiento de la LOPD en el ámbito de actividad específica del IOBA,* informe de auditoría aportado por el denunciante, que el propio Centro puso en conocimiento de sus trabajadores, empleados y colaboradores externos, con el fin de que, entre todos, pudieran mejorar y colaborar en el cumplimiento de la LOPD, acto que demuestra la buena fe y el buen hacer de la entidad.

Actualmente disponen del Documento de Seguridad, del Informe de situación sobre el cumplimiento de la LOPD, de agosto de 2015, y de Fichas de Inventario de los sistemas de información en las que se recoge: responsable, ubicación, descripción, tipo de datos que se tratan, usuarios, copias de seguridad y recuperación y registro de accesos. Adjuntan copia de los citados documentos.

Así mismo, en marzo de 2015, entre otras de las acciones encaminadas a cumplir con las medidas de seguridad, tanto de carácter técnico como organizativo de la entidad, se contrataron los servicios de una consultora especializada en la aplicación de la norma en centros sanitarios.

Con respecto a las deficiencias detectadas en el **Informe de situación sobre el cumplimiento de la LOPD**, de fecha 3 de julio de 2014, aportado por el denunciante manifiestan lo siguiente:

- Identificación y autentificación: mediante nombre de usuario y contraseña, que se obliga a cambiar cada 45 días, no permitiendo contraseñas anteriores y se bloquean por tres intentos fallidos.
- El Responsable de Seguridad, Gerente del IOBA, es el encargado de asignar los usuarios y se debe proceder al cambio de contraseña por parte del usuario la primera vez que se accede al sistema, deberá tener al menos cinco caracteres y se guardarán de forma ininteligible.

En el Documento de Seguridad se relaciona los usuarios así como el perfil de cada uno de ellos.

- En el registro de incidencias se recoge cualquier vulnerabilidad del sistema de seguridad, el intento de acceso no autorizado a la aplicación, así como las posibles suplantaciones de identidad y se detallan las acciones correctivas y preventivas tomadas al respecto.
- Las funciones y obligaciones del personal sobre la información que gestionan, el uso de la red y la confidencialidad se detallan en el en el apartado 10 del Documento de Seguridad y los empleados deben firmar el recibí de dicha información.
- Copias de respaldo y recuperación: en las fichas de inventario de los sistemas de información consta un apartado sobre copias de seguridad en el que se detalla el procedimiento y la periodicidad.
- En el registro de accesos se recoge cada usuario que accede al sistema, la fecha y hora, el registro accedido, el tipo de acceso y si ha sido autorizado o denegado, la información se guardara durante dos años.
- Con respecto al acceso físico a los dispositivos de almacenamiento de documentos, que contengan datos de carácter personal, disponen de mecanismos que obstaculizan su apertura, así como laboratorios, despachos y sala de servidores. El acceso al Centro dispone de cámaras

de seguridad y puertas internas bajo control de acceso digital.

- La gestión de Historias Clínicas se encuentra automatizada por lo que se puede conocer la situación de cada historia clínica, quién la ha solicitado y para qué, si está en tránsito o en el archivo, así como el histórico de peticiones de la misma.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 9 de la LOPD, referido a la seguridad de los datos, dispone lo siguiente:

"*1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Para poder delimitar cuáles son los accesos que la Ley pretende evitar, exigiendo las pertinentes medidas de seguridad, es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta al concepto de "*fichero*" el artículo 3.b) de la LOPD lo define como *"todo conjunto organizado de datos de carácter personal",* con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son

automatizados o no.

Así, el IOBA está obligado a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros.

III

Los ficheros que contienen datos de salud, que son datos especialmente protegidos, deben tener incorporadas las medidas de seguridad de nivel alto. Estas medidas están especificadas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

El artículo 96 del mencionado Reglamento establece la obligación de realizar auditorías:

"1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas."

El denunciante acompaña la auditoría que se realizó en el mes de julio de 2014, en la que se indicaban las deficiencias encontradas. Todas y cada una de ellas han sido revisadas y corregidas, como han expuesto detalladamente los representantes del IOBA y se ha pormenorizado en los Antecedentes de esta Resolución.

IV

El artículo 97 determina la gestión de soportes y documentos

"1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción

que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada."

La gestión de Historias Clínicas se encuentra automatizada por lo que se puede conocer la situación de cada historia clínica, quién la ha solicitado y para qué, si está en tránsito o en el archivo, así como el histórico de peticiones de la misma.

V

El artículo 93 y el 98 establecen la obligación de identificación y autenticación

"1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

El artículo 98 indica:

"El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."

Se implementa la identificación y autentificación mediante nombre de usuario y contraseña, que se obliga a cambiar cada 45 días, no permitiendo contraseñas anteriores y se bloquean por tres intentos fallidos.

VI

En referencia al control de acceso físico, los artículos 99 y 111 del Real Decreto 1720/2007, establecen lo siguiente:

"Artículo 99: Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 111 Almacenamiento de la información

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad."

Según han indicado los representantes del IOBA, con respecto al acceso físico a los dispositivos de almacenamiento de documentos, que contengan datos de carácter personal, disponen de mecanismos que obstaculizan su apertura, así como laboratorios, despachos y sala de servidores. El acceso al Centro dispone de cámaras de seguridad y puertas internas bajo control de acceso digital.

VII

El artículo 100 del Reglamento indica respecto al registro de incidencias:

"1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos."

En el registro de incidencias se recoge cualquier vulnerabilidad del sistema de seguridad, el intento de acceso no autorizado a la aplicación, así como las posibles suplantaciones de identidad y se detallan las acciones correctivas y preventivas tomadas al respecto.

El artículo 103 se refiere al registro de accesos, señalando:

"1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al

mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

Tras las correcciones realizadas con posterioridad a la auditoría, en el registro de accesos se recoge cada usuario que accede al sistema, la fecha y hora, el registro accedido, el tipo de acceso y si ha sido autorizado o denegado, la información se guardara durante dos años.

VIII

En referencia a las copias de respaldo y recuperación, el artículo 94 del Real Decreto 1720/2007, indica:

"1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad."

El IOBA ha establecido copias de respaldo y recuperación: en las fichas de inventario de los sistemas de información consta un apartado sobre copias de seguridad

en el que se detalla el procedimiento y la periodicidad.

Por último, el Responsable de Seguridad, Gerente del IOBA, es el encargado de asignar los usuarios y se debe proceder al cambio de contraseña por parte del usuario la primera vez que se accede al sistema, deberá tener al menos cinco caracteres y se guardarán de forma ininteligible. Asimismo, en el Documento de Seguridad se relaciona los usuarios así como el perfil de cada uno de ellos.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución al DIRECTOR INSTITUTO UNIVERSITARIO DE OFTALMOBIOLOGIA APLICADA, FUNDACIÓN GENERAL DE LA UNIVERSIDAD DE VALLADOLID (IOBA) y a Don ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos